VERSION 4.4

MODULE 3
SUPPLY CHAIN IMPROVEMENT AND BEST PRACTICES

Section B: Manage Risk in the Supply Chain

Section B: Manage Risk in the Supply Chain

This section covers the basic process of risk identification, assessment, and classification to show how to devise a cost-effective response strategy for each risk, develop a risk response plan, and execute the plan as well as keep it up to date. It also elaborates on a number of common and emerging supply chain risks. The primary focus in this section is on risk associated with suppliers and procurement; risk associated with production, demand, and other logistics activities is discussed in greater detail in the APICS CLTD and CPIM Learning Systems.

Risk is generally defined as an uncertainty that could positively or negatively affect the accomplishment of business objectives—for example, it could be an uncertainty related to delivery dates, quality, or revenue/cost. Negative risks also include hazards, sources of danger, lawsuits, or the possibility of incurring loss, misfortune, or injury.

The above definition of risk includes uncertainties that could have a positive impact. Risks are not always bad things, but they are always uncertain. Why does risk include things that could be positive? Because an uncertain investment might not produce the benefits that are desired, thus wasting the time and money put in up front. When a risk describes a positive uncertainty, it is called an opportunity. A threat is more precise term for just the negative types of risk. These are the opportunities and threats of a SWOT analysis, for example.

Risk is often defined only from a negative perspective, such as in the *APICS Dictionary,* 16th edition, definition of **supply chain risk** as

> the variety of possible events and their outcomes that could have a negative effect on the flow of goods, services, funds, or information resulting in some level of quantitative or qualitative loss for the supply chain.

All investment involves uncertainty, including investing in a supply chain. Even a street food vendor's operations can illustrate the threats and opportunities of managing a supply chain.

Imagine some of the possibilities. The vendor could have car trouble or an accident going to work. The vendor's wife who serves as an at-home cook could fall ill and fail to prepare some of the items to be sold that day. Customers could get sick from eating spoiled product and sue. Regulators could shut the stand down for noncompliance with health regulations. The wholesale supplier or a nearby business that provides a great deal of foot traffic (customers) could go out of business. Bad weather could keep customers away, drive up the price of raw materials (food products or fuel), or destroy the stand. Police could cite the stand for lack of a license. Thieves could steal inventory while the vendor is busy. A regular customer might move out of the neighborhood. Street gangs might try to knock the stand down, cover it with graffiti, or intimidate the vendor or customers. A competitor could set up a cart nearby.

From an opportunities perspective, perhaps the vendor wants to expand to a new neighborhood. It may be that a vendor who worked that area has gone out of business and is offering his cart for sale at a bargain. Of course opportunities are still uncertain, so it may be that after purchasing the cart and more inventory and hiring a worker, due to different cultural backgrounds, no one buys the products.

The problems in this microcosm imply all the dangers that lie in wait for larger enterprises. And so do the solutions. In brief, a little redundancy might be in order as a buffer against most of these difficulties: availability of a second car, a neighbor who can help out in the kitchen, or a second or third source for supplies besides that wholesaler. The ability to sense and respond to issues can also help, such as moving the stand to where police are usually nearby to scare off thieves and vandals or establishing a personal relationship with customers to keep them from turning to that competitor's stand. Finally, building an adaptable business and supply chain can make the organization resilient: A bit of research and contingency planning could help avoid disruptions caused by weather or inadvertent violations of the law. The vendor could reduce the uncertainty of the opportunity by finding out what people in a different neighborhood like to eat before purchasing and setting up a new stand. Redundancies, system visibility and responsiveness, and system adaptability can go quite a ways toward ensuring the steady operation of the food stand—or any organization—in the face of some potential disruptions or failed opportunities.

The potential issues with a street food vendor, though it is a very small business to be sure, mirror many of the risks that threaten real-world supply chains in the global marketplace. Consider the following examples of risks for global enterprises.

> **Example:** A Canadian company that manufactures electric motors established new relationships with global vendors to accommodate booming international demand. A few seemingly justified shortcuts were taken in the initial site inspections to expedite the selection process. Subsequently, poor-quality issues have skyrocketed and external failure costs due to defective products being shipped to customers are eroding profits and damaging the company's reputation.
>
> **Example:** A multinational medical device manufacturer experiences many service problems caused by technology incompatibilities with business partners and third parties. The root cause—a lack of open standards and problems with business process integration.
>
> **Example:** Shipping seasonal textile goods made in Southeast Asia to a global retailer involves multiple parties, transportation modes, and port calls. Along the way, a political uprising paralyzes air freight and a labor dispute disrupts operations at a major port of call.
>
> **Example:** A 2013 World Economic Forum report, "Building Resilience in Supply Chains," indicated that cyber risk could have huge implications for supply chains. Indeed, a major U.S. retailer was the first of several retailers to have its customer's personal data stolen by hackers. In that case, the credit and debit card account information of 70 million customers was stolen using malware introduced at the point of sale. The store's sales and reputation suffered and it spent money repairing the damage, offering zero liability for fraudulent charges and a year's free credit monitoring and protection.

Chapter 1: Risk Identification

This chapter is designed to

- Define risk, threat, and opportunity, and discuss some common supply chain risks
- Discuss risk management and proactively addressing risks to reduce their impact or likelihood and preplanning a response if they occur anyway
- Understand that some areas of supply chain risk are have more mature response systems than others at most organizations
- Describe the importance of developing a strategy and plan for risk management, including specifying the organization's risk tolerance
- List some common tools for identifying risk
- Show how to document risks in a risk register
- Elaborate on some common supply chain risks.

Processes for managing risk in the supply chain

The key processes that supply chain managers need to be able to perform related to managing risk in the supply chain are

- Identifying the risks
- Assessing and classifying the risks
- Developing a risk response plan
- Executing the risk response plan.

Each of these processes is introduced next. Note that these are general overviews. The information required to plan and execute these processes is presented in later topics.

Prerequisites to these processes involve strategizing and planning:

- Developing a risk strategy by discovering the organization's predisposition toward risk taking and the maturity level of its risk management processes
- Developing a plan for how you will identify and assess risks and plan and execute risk responses

Identifying the risks

The process of identifying risks involves the following steps:

- Brainstorming all of the possible risks (threats and opportunities) related to the business process or project
- Assigning attributes to each risk, such as who it may affect, what causes might make the risk occur, and other details
- Entering the risks and their attributes in a risk register, which is usually a spreadsheet with risks in rows and attributes in columns

Assessing and classifying the risks

The process of assessing and classifying the risks involves the following steps:

- Performing a qualitative risk assessment, which involves discussions with subject matter experts and persons closest to a given process to perform the steps shown in Exhibit 3-8
- Performing an optional quantitative risk assessment, which involves doing further analysis for

significant risks, as shown in Exhibit 3-9.

Developing a risk response plan

The process of developing a risk response plan involves the following steps:

- Selecting the best type of response for each risk given the organization's attitude toward risk
- Developing a risk response plan showing what to do for each risk and when to do it, including what events might trigger action if applicable
- Clearly assigning one person to be accountable for each risk response
- Getting approval and funding for responses
- Adding the risk responses and response owners to the risk register

Executing the risk response plan

The process of executing a risk response plan involves the following steps:

- Implementing planned risk responses either on a schedule or as a contingent response to specified triggering events
- Analyzing trends and variances from expected results to see how effective risk responses are and identify new risks or triggering events
- Analyzing the risk budget to determine if reserve amounts are sufficient to address ongoing and planned risk responses
- Regularly meeting to review the risk register:
  - Adding new risks and reassessing existing risks
  - Determining the results of responses
  - Generating new planned responses
  - Retiring risks that are no longer relevant

Exhibit 3-8: Qualitative Analysis Steps

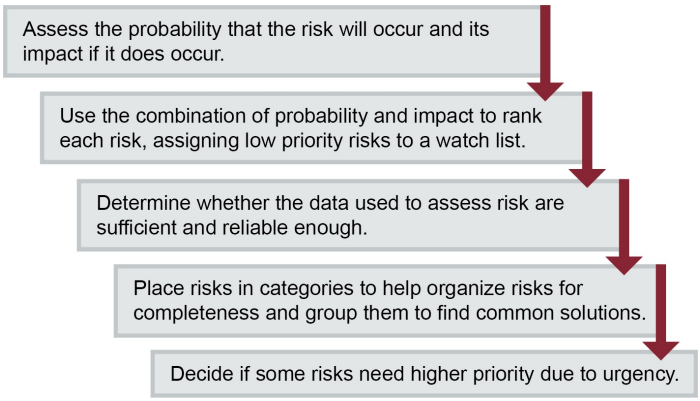
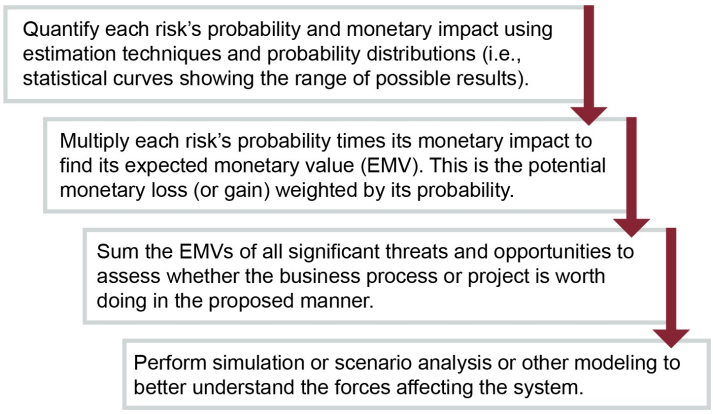


Exhibit 3-9: Quantitative Analysis Steps (Optional)



Topic 1: Risk Management

Prior to delving in and identifying the risks related to a particular business operation or project, like anything else, determining how to manage risk in the supply chain starts with a strategy and a plan. Therefore, the concepts of risk management, a risk management strategy, and a risk management plan are discussed first. Then the process of risk identification is discussed, concluding with a discussion of some common risks in a supply chain.

Risk management

How do organizations manage the numerous risks to a supply chain? They engage in risk management. The *APICS Dictionary,* 16th edition, defines **risk management** as

> the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate event or to maximize the realization of opportunities.

In supply chains, risk management is a complex end-to-end concern. A supply chain presents many opportunities in terms of resource availability, technology, market access, and the like. But it also substantially increases dependence on critical resources (human expertise and materials), transport capability, and other considerations. And, as witnessed in the examples presented in the introduction, globalization poses myriad additional risks that can expose a supply chain to upheaval.

Supply chain risk management

The APICS Supply Chain Council (SCC) defines **supply chain risk management** as

> the systematic identification, assessment, and quantification of potential supply chain disruptions with the objective to control exposure to risk or reduce its negative impact on supply chain performance.

In 2011, Accenture produced a set of principles that would help establish supply chain risk management as a discipline, here paraphrased as follows:

- **Integrate:** Align the risk management systems across the organization.
- **Model:** Develop a model of end-to-end risks and their priorities.
- **Diversify and add flexibility:** Create a diverse supplier portfolio, be flexible, and develop global visibility.
- **Quantify:** Develop contingency plans and identify unknown risks using probability modeling.
- **Perform due diligence:** Research suppliers and ensure they are performing their own due diligence on their suppliers.
- **Insure:** Make prudent decisions to insure against hazards and business disruptions.

In addition to integrating risk management with internal departments, supply chain risk management must be conducted by both the channel master and all the individual players, who each create their own risk management plans and risk response plans (a list of planned responses, discussed later in this section). The intent is to address all the events that could affect that associate's ability to continue the relationship and conduct business.

Developing an end-to-end risk model, what Accenture called understanding the supply chain ecosystem, might involve using a variety of tools and information sources to understand the environment in which the organization is operating. A 2011 AMR report cited meetings and discussions with suppliers and associates, use of predictive analytic tools, reviewing suppliers' business continuity plans, third-party reports, and performance risk dashboards as the most common methods executives used to develop a holistic understanding of supply chain risk.

In regards to diversification and flexibility, a 2012 Aberdeen group report discussed how businesses that used risk-adjusted strategies and had processes to clearly see risks and risk events and react quickly to them were also more likely to have more effective budgeting and profitability.

One example of how supply chain risk is getting better quantified is the emergence of new metrics such as time-to-recovery, which is how long it takes a supply chain to recover from an adverse event such as an earthquake or severe weather. Benchmarking against competitors using metrics like these can provide a better idea of the organization's actual levels of flexibility and supply chain visibility.

The need for multi-tier due diligence is evidenced by a 2012 report by Zurich, a global insurer. Part of the report stated that 40 percent of all disruptions had a root cause from below the tier 1 supplier level. Performing due diligence only with direct suppliers would not catch a large number of potential failures.

The same report published statistics to show what areas of the supply chain needed insuring the most. It stated that 50 percent of supply chain disruptions were weather-related. Many losses related to weather disruptions are often not covered by insurance. Lloyds of London reported in 2013 that only US$47 billion of the US$240 billion in losses from the 2011 Japanese earthquake and tsunami and the Thailand floods were covered by insurance. Much of these losses were for business disruptions, while much of what was insured was assets like plants and equipment. The second largest area—40 percent of disruptions according to Zurich—were IT/telecommunications outage–related. Types of insurance are discussed later in this section.

Risk managers

Risk managers have a critical role in supply chain risk management. They must examine the supply chain to:

- Map the entire supply chain and understand interdependencies
- Identify potential failure points along the supply chain
- Create risk awareness throughout the supply chain.

In addition, key duties of risk managers include the following:

- Devise methods to lessen risks before they become a costly problem
- Prioritize funds allocated for risk management to address critical risks and minimize overall system risk
- Implement risk prevention plans as projects and prepare and practice contingency plans
- Collect, analyze, and implement feedback to improve future plans
- Chair regular risk review meetings to keep plans current

Risk management maturity level

Risk management maturity level refers to how well developed the organization's risk management processes are relative to benchmarked competition.

What evidence is there that more mature risk management processes matter? According to an RIMS.org article, AON Insurance and the Wharton School of Business developed a risk maturity index showing that organizations with the highest level of risk maturity had 50 percent lower stock price volatility than those at lower maturity ratings. Furthermore, from 2010 to 2012, only organizations with the highest risk maturity ratings had positive returns during the most volatile parts of those years. Conversely, organizations with lower risk management maturity levels experienced losses between 17 and 30 percent during the same periods.

An organization's supply chain management team may have more advanced risk management processes in some areas than in others. According to Gregory Schlegel and Robert Trent, authors of *Supply Chain Risk Management,* most supply chain functions are fairly advanced in how they manage risk related to supply issues and are moderately advanced in terms of demand risks but are frequently lacking in the areas of process risk and environmental risk. What they mean by each of these broad categories of risk and why they feel the supply chain in general is at these levels is shown in Exhibit 3-10.

Exhibit 3-10: Supply Chain Function Risk Management Maturity Levels by Type of Risk

Type of Risk Defined	General Maturity Level and Rationale
Supply risk: Risks related to strategic sourcing, supplier communications, viability, quality, and capability, logistics, supplier due diligence, and malfeasance (e.g., counterfeiting, corruption, and fraud).	• Most mature category. • Many years of development and many tools such as SRM, spend management, credit management. • Advancements like supplier risk assessment and cloud-based software tools to detect malfeasance.
Demand risk: Risks related to customer acquisition and retention, demand management and forecasting, market and consumer trends, distribution requirements planning, competitor actions, reputation, and	• Moderately mature. • Sales forecasting is well established but doesn't incorporate risk in models. • However, collaborative planning, forecasting and replenishment (CPFR)

customer service.	does consider risk. • Sales and operations planning (S&OP) includes what-if analysis capabilities.
Process risk: Risks related to supply chain strategy and implementation, manufacturing and quality processes, IT processes, as well as organizational issues such as mergers.	• Middle low maturity. • Multiple tools for inventory planning and scheduling, etc., but most don't incorporate risk.
Environmental risk: Risks related to government regulation and compliance, tax, the economy, currency fluctuation, security, and natural disasters.	• Low maturity. • New area for risk management. • Regulations continue to change rapidly and processes and tools have trouble keeping up.

Note that these are generalizations; individual organizations may be more or less mature in each of these areas.

Risk management strategy

A risk management strategy describes how an organization plans to address the vulnerabilities it has identified throughout the supply chain by controlling, mitigating, reducing, or eliminating risk and mitigating or reducing the impact of risk events—the materialization of a seen or unforeseen adverse event. It also captures the organization's overall attitude toward risk, such as risk seeking or risk averse. These issues are discussed next.

Known versus unknown risks

Organizations will set different strategies for addressing known risks versus unknown risks. A known risk is one that has been identified and analyzed. These risks can be planned for using the processes discussed in this section. An unknown risk is one that exists but no one knows about it currently. These unforeseen risks can be addressed by putting funds in a reserve account to deal with the unknown. The size of this account, who authorizes expenditures, and the conditions under which it can be accessed are part of an organization's risk management strategy.

Risk management attitude

Organizations differ in how much risk is too much risk in exchange for the envisioned benefits, but for all individuals and organizations, risks and rewards are interrelated. Investors in general require a higher reward when there is higher risk, and this is as true for business decisions as it is for financial investments. That being said, an organization may be risk seeking while others are risk averse. To understand the continuum, contrast a risk-tolerant organization that manufactures a basic commodity such as gravel or lumber (where the benefits of accepting risk outweigh the potential harm) with a risk-averse pharmaceutical company (where a risk like contaminated raw ingredients or improperly certified suppliers could lead to deaths, lawsuits, substantial negative publicity, or a drop in share value).

Three ways of expressing an organization's attitude toward risk are risk appetite, risk tolerance, and risk threshold. The *APICS Dictionary,* 16th edition, defines the first two of these terms:

> **Risk appetite:** Amount and type of risk that an organization is willing to pursue or retain.
>
> **Risk tolerance:** An organization's or stakeholder's readiness to accept a threat or potential negative

outcome in order to achieve its objectives.

Risk threshold is a cutoff point below which a risk will be accepted and above which some type of proactive response is required.

Risk appetite refers to overall attitudes like risk seeking or risk averse. A risk seeking organization will take measured risks if the return seems worth it while a risk averse organization may want to find ways to minimize uncertainty to the highest degree possible. These attitudes may lead to different business strategies with different payoff profiles (e.g., cutting edge for the risk seeker and low, steady returns for the risk averse). Other ways that risk tolerance play out in organizational decisions include flexible supply chain strategies, diversification, and redundancy, such as the ability to produce the same part at all plants rather than specializing at each plant.

Risk tolerance and threshold are ways of expressing this appetite at the level of specific risks. These levels can be customized for different types of risk. An organization may specify that it has a low tolerance for quality risks, a moderate tolerance for delivery time risks, and a higher tolerance for cost-related risks. The organization's risk tolerance level will then play a role in which response is chosen for each identified risk.

Other organizations and individuals will also have their own risk appetite levels that need to be discovered and taken into account when developing a supply chain risk management plan. One impediment to getting risk management practices adopted across the supply chain is that many small and midsize organizations have yet to develop policies on risk tolerance in the first place. They may need to be motivated to devote sufficient time and funding to risk management.

Risk management plan

A risk management plan is a way to ensure risk is dealt with proactively and consistently. A supply chain risk management plan may be integrated with an overall organizational risk management plan or even an interorganizational risk management plan.

The plan says how risks will be identified, grouped, and assessed. It provides standardized tools to help various team members arrive at consistent definitions of risk levels. It identifies appropriate internal and external data sources for making risk assessments. Some tools specified in this plan, such as risk categories or tables to help consistently define probability and impact, are discussed in later topics.

A risk management plan also has controls to ensure risk plans and responses are appropriate to the degree of risk being faced and the importance of the business objectives or project being conducted. It ensures that risk planning and responses are cost effective, meaning they provide more benefit than they cost. Therefore, the agreed-upon risk thresholds and tolerances will be set down in the risk management plan along with required response types for various risk levels. To provide decision makers with visibility on risk issues, it will address how to track and report on risks on an ongoing basis.

A risk management plan contains a budget for a given period of time or a project duration. It should include a reserve fund for unknown risks.

When a formal plan is generated, it can be used as a tool to get buy-in and sign off/funding for the plan. Furthermore, it will specify who will be responsible for implementing the plan, who is accountable for

success, and who has authority to approve funding for specific risk responses or release funds from a reserve fund.

Topic 2: Risk Identification and Documentation

Recognition and identification of different forms of risk

Risk in a supply chain can take many forms, and supply chain risk managers need to take a systemwide perspective on risk. Risk managers determine risks to the supply chain using a number of analytical tools. For each risk identified, they define certain parameters for each risk in a risk register.

While a large number of risks may be identified in the first pass, risk identification is iterative, meaning that new rounds of identification need to occur. During these rounds, some known risks might become better understood and new risks might be identified.

A number of tools might be used to identify risks, including the following:

- **Documentation and assumptions reviews:** Reviewing supply chain documents, existing analytical tools, variance analyses, and the like can reveal risks. Reviewing assumptions made about a process or project can help consider what might happen if these assumptions are wrong.
- **Brainstorming:** Brainstorming is a group meeting where a wide range of experts are gathered to discuss risks. A facilitator sets down some rules in advance such as all ideas are welcome and none criticized. If risk categories exist, they can be used to promote completeness. Brainstorming can also be done remotely as a distributed survey.
- **Delphi technique:** Anonymous questionnaires are collected and compiled in multiple rounds until the group reaches consensus.
- **Interviews:** Formally or informally talking to experts and stakeholders can reveal new perspectives on risk.
- **Root-cause analysis:** Searching for the underlying causes of a risk can help focus on the actual problem rather than the symptoms.
- **Risk checklists:** Since risk analysis has been conducted in the past at the organization and other organizations, a list of risks from other processes or projects can be reviewed to see what applies.
- **Risk diagramming:** Flowcharts or other relationship diagrams can be used to show a process. Analysis of such charts can reveal weaknesses. Also, various tools from the quality discipline such as a cause-and-effect or Ishikawa diagram can be leveraged for risk analysis.
- **SWOT analysis:** A strengths, weaknesses, opportunities, and threats analysis starts by looking at the organization’s capabilities and areas that need work, then looks at external opportunities and threats. This strategic-level analysis is good at seeing the big picture, in other words, what opportunities or strengths might offset threats or vice versa.

One starting point for supply chain managers may be to list each raw material used, identify which materials are of strategic value, and invest time in understanding the organizational and financial structures of each strategic material supplier. This process can help with defining the relative vulnerabilities of the supply chain

and the implications of doing nothing.

Risk identification

Risks need to be described in a consistent manner and at a level of detail that will allow them to be understood and evaluated against one another. When identifying risks, specify

- **Cause(s):** The root causes, if applicable and known.
- **Event(s):** The triggering events, if applicable and known.
- **Impact:** The internal and external threats (or opportunities) for each critical asset or process. This includes an assessment of criticality. For threats, this is the critical assets or processes of the organization that, if not operating effectively, would prohibit the company from fulfilling its mission, such as providing its key products or services.
- **Effect:** Areas within the organization or up and down the supply chain that would be impacted as a result.

The final task is to combine these into a definitive statement of each risk. For a company that ships most of its products by train, an example statement might be “Derailment of multiple cars due to sabotage or disrepair of train tracks resulting in destruction of products onboard, possible injuries to train personnel, and delays of future shipments while track is repaired.” An automotive original equipment manufacturer that produces gas supply lines using a patented raw material from a single source might identify the risk as, “Nylon-12 is only available from one supplier, Corporation ABC, and is produced in just one plant in Germany. A disruption or accident at this plant could critically disrupt the supply of this raw material for Product Lines A and B.”

Risk definition

The scope and time frame of each risk must be well understood before organizations can decide what would be an appropriate response. The APICS SCC notes that each identified risk must also have a time dimension or a specific time horizon (e.g., day, month, year) and a specific perspective or view that defines the scope (e.g., boundaries, what is not included, etc.). Some risks will exist for only a given time period, such as risks of warranty returns in the warranty return period. Other types of risk are ongoing but can be defined further; for example, risks of delivery truck hijacking could be subdivided into risks as cargo is transported through specific countries or at particular times of the day. Risks of piracy (and resulting insurance costs) for container ships is defined by the countries the trade routes pass nearby.

Risk register

As defined in the *APICS Dictionary,* 16th edition, a **risk register** is a useful summary report

> on qualitative risk analysis, quantitative risk analysis, and risk response planning. The register contains all identified risks and associated details.

A risk register is often a spreadsheet with a row for each risk and a column for each risk attribute. More attributes can be added whenever they are desired. The register contains the risk identification information and risk definition information, along with all other information related to that risk. Since much of this information is determined during later steps in the risk management process, these fields would remain blank until those steps are completed. This can include a list of potential responses or references to planned responses. Exhibit 3-11 shows an example of a risk register.

Before moving on to how to categorize and assess the risks that have been identified, we will first examine some specific supply chain risks.

Exhibit 3-11: Risk Register Example

Risk ID	Category	Identified Risk	Cause(s)	Probability	Impact	Rating
7.2.1	Supply disruptions	Nylon-12 supply could be disrupted for Product Lines A and B.	Single sourcing with Supplier ABC. Also, Nylon 545 only made one plant in Germany.	50% Moderate x	80% Very high =	40% **High**
7.2.2	Supply partnership opportunities	Partner with Corporation ABC to build a second plant elsewhere.	See 7.2.1.	30% Low x	80% Very high =	24% **High**

Risk ID	Triggering Event/Red Flags	Response	Budget/ Reserve	Responsible	Expiration Date	Status
7.2.1	No triggering event. Red flags: Severe weather in plant region or plant calamity.	Mitigate: Order safety stock. Avoid: Search for substitute materials. See response plan #7.2.1.	US$50k for search. US$200k for safety stock.	J. Rodriguez	Ongoing (Search project finish 11/2018)	Project 40% complete, no substitutes found yet.
7.2.2	Trigger: Supplier ABC interest in offer.	Share. Generate interest and develop detailed business plan. See response plan #7.2.2.	US$10k for travel and proposals.	R. Russell	12/2018	Supplier reluctant but still in talks.

Topic 3: Supply Chain Risks

Risk of loss of tangible and intangible assets

Risk of loss involves risks to tangible and intangible assets (property, inventory, or intellectual property) from internal or external threats. Internal threats include employee theft, collusion (working with a person or group outside the organization), fraud, misplacement, damage or destruction from accidents, or improper handling. External threats include theft by unknown parties or by external business partners, abduction, hijacking of modes of transportation and their cargoes, counterfeiting, computer hacking, or damage or destruction from a host of threats.

Who bears the risk of loss during transfer of goods is not ruled by who currently holds the title to those goods. International Commercial Terms 2010 (Incoterms® 2010, discussed in the section on "Procure and Deliver Goods and Services"), outlines that the risk of loss or damage to the goods, as well as the obligation to bear the costs relating to the goods, passes from the seller to the buyer when the seller has fulfilled his or her obligation to deliver the goods. For example, in an FOB (Free on Board) transaction in which the terms of sale identify where title passes to the buyer, as soon as the goods are "on board" the main vessel the risk of loss transfers to the buyer or importer. The buyer must pay for all transportation and insurance costs from that point and must clear customs in the country of import.

In North America, two FOB terms (very often shown as F.O.B. and followed by Origin or Destination, and meaning either free on board or freight on board) are used (not to be confused with the FOB Incoterm® for sea and inland waterways) for domestic shipping via various modes of transport. The U.S. Uniform Commercial Code (UCC), Section 2-509, states that the risk of loss in a *FOB Origin* contract passes to the buyer when the inventory is duly delivered to the carrier. The risk of loss in a *FOB Destination* contract (where the seller is responsible for the goods until the buyer takes possession) passes to the buyer only when the goods reach the destination point. However, parties are free to allocate the risk of loss in any way the two parties can agree upon.

Loss of goods, money and reputation, and intellectual property are discussed next. Afterward, risk of loss from lawsuits is also mentioned.

Loss of goods

Keeping shipments secure from loss, damage, theft, and vandalism has always been a concern for businesses, whether strictly domestic or in the export-import area. The growing threat of terrorism has added a new sense of urgency to these long-standing security worries.

Losses from other forms of malfeasance

Organizations can face significant losses from various other types of malfeasance (wrongdoing), including bribery, fraud, corruption, abduction, and counterfeiting. Losses can take the form of fines, enforced shutdowns of operations, and seizure of goods. Illegal activities—even without the knowledge or consent of the organization's leaders—place a great risk on the organization's reputation. In the case of bribery, fraud, or corruption, the negative press from government or criminal investigations can cause loss of sales. Abductions can result in loss of key persons and require payment of large ransoms. Counterfeiting can

reduce the organization's reputation for quality or counterfeit goods could compete unfairly with the organization's products.

Fraud, corruption, and bribery are discussed next. Since counterfeiting is also a type of loss of intellectual property, it is discussed more in the next subsection.

Fraud and corruption

Fraud and corruption can take many forms. For a supply chain, it often has to do with attempting to make an unfair profit by avoiding laws and regulations. In an example of risks related to fraud and corruption, a U.S. honey importer was caught passing off Chinese honey as honey from other sources. The organization's incentive was to avoid the large tariffs that could triple the cost of the honey, so two executives produced fake documents and subsidiaries shipped the honey to multiple countries, where it was relabeled and filtered to hide its origin. The organization fired the executives and paid a $2 million fine, had to destroy and replace the inventory, and then faced lawsuits from its competitors. It was eventually forced into bankruptcy when it went into default on a loan.

Bribery

A bribe is when a person gives another individual a gift, money, or a favor intending to influence his or her decision, judgment, or conduct. The bribe can be in the form of anything the recipient considers to be valuable. According to Bowersox, Closs, and Cooper, although bribes are unethical and illegal in most developed nations, these types of payments may be necessary in the sale and movement of product through customs in developing countries.

There are three types of criminal bribery: commercial bribery, bribery of public officials, and bribery of foreign representatives.

Commercial bribes are usually aimed at covering up for an inferior product or obtaining new business or proprietary information. They can also involve industrial espionage, where sensitive information is stolen or kickbacks or payoffs are made for trade secrets or price schedules.

When it comes to public officials, any attempt to influence that individual in a manner that serves a private interest is considered a crime. The crime of bribery occurs when the bribe is offered even if the potential recipient does not accept it. Legally, a second separate crime occurs when a bribe has been accepted.

In 1977, the U.S. implemented the Foreign Corrupt Practices Act to discourage bribing of foreign officials in order to secure favorable business contracts. Since then, U.S. laws have been established that criminalize that bribery.

An example of risks related to bribery involves a large clothing retailer. An Argentinian subsidiary admitted to bribing officials to get customs clearance for goods and to avoid inspections. The company was also accused of creating fake invoices to hide the payoffs. The company had to pay a fine of $1.6 million to the U.S. SEC, which was less than it could have been since the organization cooperated fully and there was no evidence the practice occurred in other subsidiaries.

Abduction

In 2009, the *New York Times* reported that worldwide kidnappings soared as the global economy stalled. The risks for executives of North American companies traveling abroad is on the increase. According to a June 2009 article by Parker, Smith, and Feek, a Bellevue, Washington, international risk management and consulting firm, high risk areas include Mexico, Colombia, Brazil, and Venezuela, which have seen a significant increase in abductions of business professionals for ransom. In Colombia alone, there have been more than 3,000 kidnappings each year, and about US$250 million has been paid in ransom for Americans and other foreigners. Other risk experts agree that the Middle East and Southeast Asia are also higher-risk countries.

Abduction is not occurring solely on foreign soil. In 2010, the chairwoman of Columbia Sportswear was a victim of an attempted abduction while in her own U.S. home. Luckily for her, she knew how to respond and protect herself, and the criminal fled after she triggered a silent alarm that was sent to police.

Loss of intellectual property

Intellectual property losses can include the threat of counterfeit goods or services using the organization's designs and patents and possibly the organization's name and brand (or a close approximation of it). Counterfeits can be actual goods, replacement parts, or copyrighted digitized materials. The counterfeiters can be operating for profit or be freely distributing the materials (in the case of digital property). Counterfeit goods are often introduced into a legitimate supply chain when a supplier faces a shortage. Rather than turn down the sale, they turn to what are called "grey markets." These are markets selling legal goods but are produced by unknown third parties and thus become counterfeit goods when the supplier passes them off as their own manufacture.

Working with global suppliers creates intellectual property risk. If global suppliers have access to proprietary designs and already perform the manufacturing, they could go into business for themselves and become a competitor. A way to mitigate this risk is to source materials that involve trade secrets either domestically or only in countries with robust trade secret protections. Another solution is to divide up parts of a trade secret and have different suppliers work only on a small portion of the overall requirements.

Just doing business in some countries with less intellectual property enforcement also create risks. As organizations search for lower cost suppliers, the culture in many of these countries is more permissive of intellectual property theft, so organizations need to invest more time and money in protecting their trademarks and patents. In some cases, corporations or even governments of some countries engage in active corporate espionage, for example, stealing data from visitor's computers or other devices when they leave them in their hotel rooms.

Losses from lawsuits

Organizations also need to protect themselves from potential lawsuit losses.

Chapter 2: Risk Assessment and Classification

This chapter is designed to

- Explain the risk management process, including identification and categorization of risks, analysis of the risk level, evaluation, and formulation of a cost-effective risk response
- Differentiate between qualitative and quantitative risk analysis techniques and when to apply each
- Categorize common supply chain risks and provide instigating factors and possible related root causes or red flags
- Assess risk probability and impact and interpret risk rating on a probability and impact matrix
- Assess the quality of data used in risk assessments
- Understand how to represent risk on a probability distribution so it is clear a range of results could occur
- Calculate the expected monetary value of a risk with or without an up-front cost
- Understand the basic uses of sensitivity analyses and simulations.

Topic 1: Qualitative Risk Analysis

Organizations use risk assessment and classification processes to prepare for uncertainty by prioritizing scarce time and money toward risks with the greatest probability and impact. Risk assessment and classification thus includes prioritization.

Classification and prioritization occur first, which involves a qualitative, or subjective, analysis of risks using expert judgment and some helpful tools described in this topic. Risks can then be further assessed using quantitative risk analysis, which uses mathematical formulas or models to better quantify the monetary impact of certain risks, weighted by their probabilities.

Risk assessment and classification is influenced by the organization's tolerance for risk, the specific risk level for each risk, the basic responses to each risk that are possible, and the cost of the risk response. These were all discussed earlier and are part of the risk management plan.

Classification and prioritization: qualitative risk analysis

Classification and prioritization of risks uses qualitative risk analysis to understand, categorize, and rank risks quickly and efficiently. Qualitative risk analysis is an analysis of the various qualities that make up each risk. The analysis can take into account many factors and thus can be nuanced while being cost effective. The primary factors are probability and impact, but other factors such as urgency are accounted for.

Analysts also may need to compensate for data quality or completeness and potential estimator bias. Another factor is the risk tolerance for the specific business constraint, such as time or cost, which may differ by constraint. The various factors are weighed and the result is a risk rating that can be used to rank the risks in order of importance.

Methods and tools used in qualitative risk analysis discussed next include the following:

- Risk categorization
- Probability and impact assessment
- Risk urgency assessment

- Data quality assessment

Risk categorization

Different conventions exist for categorizing supply chain risks. The *APICS Dictionary,* 16th edition, defines a **risk category** as "a cluster of risk causes with a label such as external, environmental, technical, or organizational."

The Global Association of Risk Professionals classifies risk in operational categories:

- Personnel risk (e.g., internal fraud, human error)
- Physical assets (e.g., loss of business environments/assets)
- Technology (e.g., virus damage, system failures)
- Relationships (e.g., liabilities, lawsuits, loss of reputation)
- External/regulatory (e.g., external fraud, government incentives/ restrictions)

Each organization will define categories of risks in such a way that it helps the organization cluster planned risk responses, perhaps finding actions that can address more than one risk simultaneously. Exhibit 3-12 lists categories of internal and external risks to the supply chain.

Exhibit 3-12: Internal and External Supply Chain Risks

Internal Risks to the Supply Chain	External Risks to the Supply Chain
• Poor quality • Unreliable suppliers (lead time, capacity) • Supply shortages • Equipment breakdowns, lack of equipment • Incompatible/inflexible technology or technology disruptions • Uncertain demand or poor forecasting • Too frequent production schedule changes (system "nervousness") • Communication across different cultures • Service failures • Compliance risks • Poor labor relations, work slowdowns, or strikes • Poorly trained labor, high labor turnover or illness, or morale issues	• Labor shortages • Political instability (e.g., riots, government business appropriation) • Transportation delays due to weather, etc. • Financial risks from currency instability/fluctuations • Natural disasters, wars, or terrorism • Poor infrastructure in developing countries (e.g., unreliable electricity) • Large variability in demand caused by economy, competitor actions, etc. • Legal/regulatory changes • Taxation changes • Customs risks • Customer or consumer pressures

There are many other ways to categorize supply chain risks, for example:

- Strategic supply chain risks
- Supply risks
- Demand risks
- Process risks
- Environmental risks
- Hazard risks
- Financial risks
- Malfeasance risks
- Litigation risks

Each of these categories is discussed next. Note that supply risks, demand risks, process risks, and environmental risks might be grouped together in a larger category of operational risks, which together comprise the core risks facing most supply chains.

Strategic supply chain risks

Strategic supply chain risks are those risks that endanger the success of the organization's long-term supply chain strategy. Risks in this category include those that have strong potential to impact business continuity, brand image, reputation, and market share.

Supply risks

Supply risks include the following types of risk discussed in Exhibit 3-13 along with some examples of root causes or red flags that could be recorded for each risk. Some other supply-related risks mentioned in later categories, such as supplier insolvency or counterfeiting, might instead be located in this category.

Exhibit 3-13: Supply Risks and Common Root Causes/Red Flags

Supplier/subcontractor availability	• Failure of initial source/supplier.
Supplier pricing	• Poor performance may lead to price increases. • Contract changes or violations.
Supplier quality	• Suppliers may be using lower quality raw materials. • Supplier manufacturing processes allow variability.
Supplier lead time	• Suppliers may not have sufficient capacity. • Suppliers may not have sufficient raw materials.
Transportation lead time	• Fleet may have high rate of breakdowns. • Other risks may play a factor, e.g., hazards, customs.
Customs/import delays	• Paperwork errors or customs paperwork delays. • Port strikes or other labor issues.
Labor disruption	• Union contracts require renegotiation. • Country-specific general labor unrest.

Demand risks

Exhibit 3-14 lists some examples of demand risks and possible root causes or red flags. A key risk in this area is forecasting errors. Most organizations use a mix of statistical forecasting tools and expert judgment, but the error at the level of aggregated product lines (aggregating to reduce forecast error is called risk pooling) is still around 10 percent, and forecasting error at the stock keeping unit (SKU) level is 40 percent or more, according to Schlegel and Trent, authors of *Supply Chain Risk Management.*

Exhibit 3-14: Demand Risks and Common Root Causes/Red Flags

Forecasting error or bias	• Seasonality, bad data, or inadequate model/modeler. • Poor communications or assumptions (e.g., optimism).
Inter-organizational communications	• Separate forecasts cause bullwhip effect/variability. • Attitudes that forecasts are trade secrets.
Outbound shipping delays	• Capacity, information system, or product issues. • Customer order changes.
Outbound transportation delays	• Carriers experience capacity issues or instability. • Other risks may play a factor, e.g., hazards, customs.

Customer price changes/promotions	• Unannounced prices/promotions create demand surge and upstream stockout/capacity issues.
Quality issues	• Poor quality auditing (process audits)/quality control. • Poorly communicated requirements/specifications.
Warranties/recalls	• Poor integration of business units/subsidiaries. • Poor product portfolio or specification management.
Lost customers	• Inability to fulfill expectations due to failures in other risk areas.
Unprofitable customers	• Services offered are not tailored to customer profitability or longevity.
Customer's requirements change	• Poor communications and change control.
Customer product launches	• Failure to get involved early, which the customer may not be allowing, leading to poor planning/execution.

Process risks

Exhibit 3-15 lists some examples of process risks and possible root causes or red flags.

Environmental risks

Exhibit 3-16 lists some examples of environmental risks and possible root causes or red flags. The definition of what counts as an environmental risk might be expanded to include the political environment, currency exchange rates, and weather related events, but these are here addressed in other categories.

Exhibit 3-15: Process Risks and Common Root Causes/Red Flags

Capacity and flexibility	• Too reliant on certain equipment, persons, or places. • Poor planning, visibility, or communications.
Manufacturing yield	• Material shortages. • Human or equipment failure.
Inventory	• Poor life cycle planning (obsolescence). • Poor inventory planning or forecast error.
Information delays	• Union contracts require renegotiation. • Country-specific general labor unrest.
IT/Telecommunications	• Power or service outages in a region or at the host. • Hackers, malware, and human or internal errors.
Poor payables processing	• In-house cash flow shortages. • Deteriorating relationship with suppliers.
Poor receivables processing	• Customer financial difficulty. • Poor organizational follow up or contract enforcement.
Intellectual property	• Outsourcing/contractor due diligence failures. • Failure to compensate for country risk/espionage.
Poor planning	• Poor systems, processes, and infrastructure for planning. • Poor management oversight (e.g., no S&OP) or training.
Mismanagement	• Failure to develop strategy or execute strategy and tactics. • Poor measurement, management, and

	communications.

Exhibit 3-16: Environmental Risks and Common Root Causes/Red Flags

Environmental legislation/regulation	• Poor commitment or management. • Failure to use due diligence or audit self/suppliers.
Industry regulations	• Same as above plus new entry into industry (e.g., mergers or operating in many industries).
Country regulations	• Same as above plus lack of or failure to acquire cultural understanding/sensitivity.
Shifts in cultural expectations	• Evolving societal expectations go unheeded. • Competitors using stricter environmental practices.
Conflict minerals	• Failure to use due diligence with suppliers' suppliers. • Willful indifference or active obfuscation of conflict region sourcing.
Customs regulations	• Packaging poorly balances goods protection, custom's access, and packaging minimization.
Interest group attention	• Unwelcome negative press. • Pressure to adopt less profitable methods for sustainability.
Voluntary reporting	• Voluntary sustainability reporting used to highlight negatives. • Peer group comparisons don't favor the organization.

Hazard risks

Hazard risks are called force majeure in legal terms or acts of God colloquially. These are primarily the natural disasters that cause property damage and business disruptions, but hazards can also include political turmoil, war, government appropriations, product tampering, acts of terrorism, and similar events beyond the organization's control.

Financial risks

Financial risks relate primarily to the financial solvency and credit issues of the organization and of others up and down the supply chain. Financial risks also include risks related to volatility of the overall financial market or of commodity or foreign exchange markets.

Risks of insolvency or financial difficulty need to be monitored not only for suppliers and customers, but also for service organizations such as third-party logistics providers, third-party payment vendors, and so on. Financial metrics are discussed in detail in another section, but here are some other red flags to watch for that can show when a supplier is in financial distress:

- Supplier changes its early payment incentives or needs payment first.
- Supplier is paying its suppliers late (payables period is going up).
- Quality or grade is decreasing.
- Unusual early shipments may indicate lack of business.
- Longer lead times may mean they must order their materials late.
- Investments in R&D, equipment, resources, or IT are falling off.
- Supplier invested heavily in personnel, R&D, or equipment but there are delays getting these new products to market.

- Supplier's customers are industries in distress.
- Unusual executive turnover or stock sales occur.
- Supplier must restate financial statements.
- Supplier is laying off workers, closing plants, and denying rumors.

Organizations in financial distress may make unwise and selfish choices that they would otherwise not be motivated to make.

The great recession of 2008 is a clear example of a market risk that impacted many areas, not the least of which was a severe tightening in credit availability. Commodity market volatility is another large area of risk for supply chains. According to the IMF, commodity prices since 2005 have had three times as great of fluctuations in comparison to the period of 1980 to 2005.

Currency exchange risk exists because most (but not all) currencies are free floating, meaning that their value can go up or down relative to market forces. If you must pay for inventory or equipment in a different currency, even though the price is fixed, you might need to pay more or less in your own currency after the exchange is factored in.

Malfeasance risks
Risks of supply chain theft (or other types of loss), fraud, corruption, bribery, abduction, and counterfeiting can be placed in a category such as malfeasance (wrongdoing) risks.

Litigation risks
Risks of lawsuits include product liability, breach of contract, and many others.

Probability and impact assessment

A probability and impact assessment involves estimating the following attributes for each risk:

- **Impact.** This is the magnitude of the loss (or gain). It considers the importance of the process or asset at risk to the organization. Evaluate and rank the impact of potential worst-case scenarios, for example, from insignificant (5 percent), to minor (10 percent), to moderate (20 percent), to major (40 percent), to extreme (80 percent) consequences. The organization can decide on how to label the categories and assign percentages to these labels, as shown above. Percentages help estimators come to a common idea of the value of each category.
- **Probability.** This is the probability of occurrence. Evaluate and rank the probability of the scenario occurring, for example, from rare (10 percent), to unlikely (30 percent), to possible (50 percent), to likely (70 percent), to almost certain (90 percent). Once again the organization can decide on percentages and labels.

The final task in this step to create a matrix where the consequence levels and likelihood are identified for each scenario. This reveals each scenario's overall risk rating. An example from a packaged food company might be "Employees planning to strike over poor working conditions threaten to deface product packaging as it's being loaded into work trucks bound for a distribution center." This would probably be ranked as possible in likelihood with minor consequences, since the company has been informed about the threat in

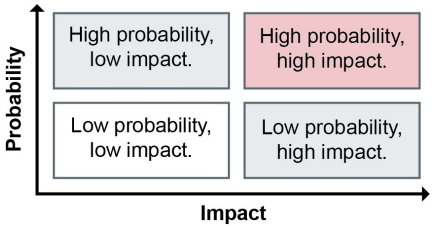
advance and can take the necessary precautions.

The *APICS ECM Supplemental Glossary* defines **supplier's/customer's/ product's risk rating** as "the numerical risk rating for supplier, customer or product. Normalized and used for comparison purposes." Risk rating is commonly described using the following equation:

$$\text{Risk Rating} = \text{Probability} \times \text{Impact}$$

The combination of probability of occurrence and magnitude of loss creates at least four basic categories of risk levels, as shown in Exhibit 3-17. Organizations can use risk level categories to decide on a risk response.

Exhibit 3-17: Categories of Risk Levels



Obviously, risk levels may occupy a spectrum rather than fitting neatly into categories. To provide risk assessors with more guidance on how to deal with risks, a full probability and impact matrix can be developed.

Exhibit 3-18 uses the percentage-based probability and impact percentages defined earlier to create a full matrix.

Exhibit 3-18: Probability and Impact Matrix

		Impact				
		Insignificant	Minor	Moderate	Major	Extreme
Probability		**5%**	**10%**	**20%**	**40%**	**80%**
Almost certain	**90%**	5%	9%	**18%**	**36%**	**72%**
Likely	**70%**	4%	7%	14%	**28%**	**56%**
Possible	**50%**	3%	5%	10%	**20%**	**40%**
Unlikely	**30%**	2%	3%	6%	12%	**24%**
Rare	**10%**	1%	1%	2%	4%	8%

In Exhibit 3-18, each box in the matrix is simply the probability percentage times the impact percentage, such as 90% × 80% = 72%. (The exhibit rounds to the nearest percent.) This chart is an elaboration of Exhibit 3-17, as a spreadsheet. The risks can then be placed in categories such as low (no shading), medium (grey shading), and high (black shading) as above. The organization will specify in the risk management plan how each category should be addressed, for example:

- Accept all low risks (do nothing but monitor them on a watch list).
- Use expert judgment to decide how to handle medium risks.
- Make a proactive plan to address all high risks.

Note that when an organization's risk tolerances differ by business objective, the risk management plan may specify how to rate risks differently by objective, such as placing delay related risks at a higher impact than cost related risks, and so on.

Risk urgency assessment

Organizations need to increase the priority of risks that will require further action based on their urgency. If action is required quickly for a response to be effective at all, then this analysis might move the response higher in priority and earlier in the schedule. Similarly, other factors may also be used to adjust a risk's priority, such as whether the risk impacts safety, the organization's reputation, or legal obligations.

Data quality assessment

A data quality assessment is used to determine how well the given risk is understood. It also assesses the reliability, accuracy, and integrity of the underlying data used to make the assessment. Low quality data can lead to inaccurate risk ratings. When a risk is rated incorrectly, it can lead to very poor decision making. For example, a major bank's US$6 billion trading loss was due in part to spreadsheet errors. A weakness included error prone manual copying and pasting between spreadsheets. Also there was an error in a value-at-risk (VaR) spreadsheet model. In one place, it divided by the sum of an old rate and new rate rather than by their average (i.e., failed to divide by two) which lowered the VaR and made the stock trades seem far less volatile.

If the data for the risk assessment is hard to come by, it is important to indicate how tentative the risk rating is and that the risk is not well understood. Flagging such risks for later analysis can help because many risks become easier to assess as relevant events grow nearer.

In the context of data quality, reliability refers to whether the same result would be obtained if the same measurement procedure is used multiple times. Reliability may be affected by bias on the part of estimators, such as preconceived notions or different assumptions about a process or environment. This is one reason why it is important to provide as much guidance as possible to estimators on shared assumptions and give them clear tools like a probability and impact matrix, perhaps along with supporting examples at each risk level.

Accuracy is the "degree of freedom from error or the degree of conformity to a standard" (*APICS Dictionary,* 16th edition). Accuracy can be verified by checking the data for math errors and so on. Accuracy may also involve checking risk levels against external sources to see if they conform to available external standards such as risk databases. Insurance specialists might also check them against actuarial tables.

For example, in Victoria, Australia, the Security and Emergency Management Division of the Victorian Department of Transport has prepared a report that includes a tool to be used by small and medium-size organizations to help them objectively and effectively evaluate security risks. This report is available in the Resource Center.

The *APICS Dictionary,* 16th edition defines **data integrity** as “assurance that data accurately reflects the environment it is representing.” For risk data, this may be determining the predictive quality of risk assessments or responses over time by comparing them to actual results.

Circling back

Once all of the various assessments are complete, supply chain managers circle back to reevaluate each risk. This follow-up step involves

- Reevaluating the organization’s risk priorities, determining if each is at an acceptable level or if there needs to be further action taken
- Verifying that the recommended actions are in accordance with the organization’s risk tolerance levels
- Adding the results of the analysis to the risk register.

In many cases, risk categorization and analysis is complete at this point. Some organizations choose to quantify certain significant risks or create risk models. These practices are discussed next.

Topic 2: Quantitative Risk Analysis

A quantitative risk analysis is a numerical analysis of the effect of risk on business objectives. Because these types of analyses produce quantifiable results, they can further reduce uncertainty and provide clear information for assessing the benefits and costs of doing nothing versus developing a proactive risk response. After individual risks have been assessed, they can be re-ranked in priority.

While individual risk analysis is useful, the real power of a quantitative risk analysis is the ability to assess the aggregate level of risk in a business endeavor. This is sometimes called a risk and opportunity analysis or as SCOR calls it, overall value at risk. This text introduces expected monetary value (EMV) below as one way to calculate individual VaRs as well as overall VaR when the individual values are summed.

Aggregating all of the uncertainties facing a particular operation or project can show when there is a likely net positive or negative impact when the various threats and opportunities are weighted by probability and then summed.

Quantitative risk analysis should only be performed for those risks that have sufficiently high data quality. Performing this analysis on less well understood risks can lead to worse decision making than if the mathematical analysis had never been done. In those cases it is best to rely on the qualitative risk analysis.

Data gathering

When more reliable data on risks needs to be gathered but the best source available is still interviews with those persons closest to the process, a good way to get better results is to ask each person for three estimates: a most likely estimate as well as an optimistic and a pessimistic estimate. These three estimates can then be averaged by adding them and dividing by three. For example, if the estimates for a cost were $40,000 as most likely but as high as $75,000 or as low as $30,000, the simple average would be ($30,000 + $40,000 + $75,000)/3 = $48,334.

Another method of averaging is to use a weighted average. A commonly used weighted average method is the one developed for PERT (program evaluation and review technique), which is a project management methodology used to develop budgets and schedules when significant uncertainty as to estimates exists. The PERT method uses a weighted average, placing four times more weight on the most likely estimate (it then divides by six because there are effectively six things to average). The formula for the PERT weighted average follows with a continuation of the prior example:

$$\begin{aligned}\text{Weighted Average} &= \frac{\text{Optimistic} + (4 \times \text{Most Likely}) + \text{Pessimistic}}{6} \\ &= \frac{\$30,000 + (4 \times \$40,000) + \$75,000}{6} \\ &= \$44,167\end{aligned}$$

Probability distributions

A continuous probability distribution is a way of showing how results could differ from an expected result (a well-known example is a bell curve). When shown on a graph with probability on the vertical axis and the possible results on the horizontal axis, the statistically most likely occurrence would be at the peak of the

graphed data. Using the simple average estimation example above, the peak is at the average of $48,334. The low end would be at $30,000 and the high end would be at $75,000.

The usefulness of such graphs is that they illustrate that an estimate could fall within a certain range rather than looking more certain than it is. A tall and narrow curve would show that the results are fairly predictable, while a fat and low curve would show that the results are more likely to be off a significant amount. A curve could also fall off more steeply in one direction than the other, as would be the case with the estimate above: The results are more likely to be on the $48,334 to $75,000 end of the scale, so this side would be a little wider than the $30,000 to $48,334 side (called skewed in the direction that is wider).

Expected monetary value (EMV): Risk response cost versus benefit

Prior to deciding on an appropriate response for each identified risk, the organization must balance the cost of the risk response against the risk level. That is, the cost of a preventive action and/or contingent action must be balanced against the benefits the action provides in terms of reduced costs from a risk event occurrence and/or reduced probability of occurrence. This allows the organization to achieve a best-cost outcome for each supply chain vulnerability. The best-cost outcome is one that addresses all of the highest priority risks first and in which the response is never more expensive than the risk itself would cost.

A cost versus benefit analysis can be done qualitatively using educated guesses, but for a higher degree of precision, the organization can use a technique called expected monetary value (EMV) to quantify the costs and benefits. This formula can only be used if a probability can be calculated.

The basic formula for EMV is the same as for the risk rating formula earlier, probability times impact. The only difference is that now the impact is expressed in terms of a monetary impact:

$$\text{Expected Monetary Value (EMV)} = \text{Probability} \times \text{Impact}$$

The resulting dollar amount can be used as a spending target or limit for risk mitigation or prevention efforts. For example, if a risk has an anticipated cost of US$1 million and a probability of 5 percent, the response should cost no more than US$50,000 (0.05 x US$1,000,000 = US$50,000).

Risk managers can use a cost justification formula such as this when presenting their plans and budgets for approval. Risk mitigation plans can also be justified by showing how much the risk probability will be reduced and what this means in terms of reduced costs from avoiding harmful risk events. However, cost justifications are not always as simple as doing math. For example, insurance on buildings often costs a little more than the expected value, but the insurance is justified because the potential loss is so great.

EMV for multiple outcomes of a risk or decision

EMV can be used to evaluate the risk of a decision that could have more than one outcome. For example, establishing a formal partnership with a supplier could result in an increase in revenues of US$10 million in the first year in the best case, but in the worst case it could only bring in US$1 million that year.

EMV makes the simplifying assumption that the options being considered are the only possible outcomes and so these outcomes sum to 100 percent of the possibilities. Therefore, if these are the only two options being considered, if there is a 75 percent chance that the partnership will bring in US$10 million, then there

is a 25 percent chance of the US$1 million result.

EMV is calculated separately for each option and then the options are summed to find the expected value of that decision. The calculations for this example follow:

$$\begin{aligned}\text{Expected Monetary Value (EMV)} &= \text{Probability} \times \text{Impact}\\ \text{Best Case} &= 0.75 \times \text{US\$10,000,000} = \text{US\$7,500,000}\\ \text{Worst Case} &= 0.25 \times \text{US\$1,000,000} = \text{US\$250,000}\\ \text{Net EMV} &= \text{US\$7,500,000} + \text{US\$250,000} = \text{US\$7,750,000}\end{aligned}$$

Here, the expected value of return is US$7,750,000 after all risks are accounted for. So while the expected result is somewhat less than the US$10,000,000 best case, the result is positive so the risk seems worth taking. However, this may not be true after the up-front investment is considered.

Net Impact EMV

When a risk has a response cost or an opportunity has an up-front cost, this can be factored in to the analysis. To continue the previous example, say that there is a US$5 million up-front investment. This cost is deducted from the impact prior to multiplying it by the probability. If the net result is positive, it is then an opportunity. If the net result is negative, then it is a threat (negative risk). The formula for calculating a EMV when there is an initial cost follows along with a continuation of the prior example:

$$\begin{aligned}\text{Expected Monetary Value (EMV)} &= \text{Probability} \times (\text{Impact} + \text{Cost})\\ &= \text{Probability} \times \text{Net Impact}\\ \text{Best Case} &= 0.75 \times (\text{US\$10,000,000} + -\text{US\$5,000,000}) = \text{US\$3,750,000}\\ \text{Worst Case} &= 0.25 \times (\text{US\$1,000,000} + -\text{US\$5,000,000}) = -\text{US\$1,000,000}\\ \text{Net EMV} &= \text{US\$3,750,000} + -\text{US\$1,000,000} = \text{US\$2,750,000}\end{aligned}$$

Note that the formula shows impact plus cost. This assumes that the cost will be a negative value and thus a deduction. If both numbers are negative, adding them makes a larger negative net impact.

Now the opportunity does not seem quite as appealing, but since the net value is still positive, it is still an opportunity. If the risk-adjusted benefits and costs of later years were added, the decision would become clearer.

EMV can also be used to decide between two alternatives. A decision tree is a way of diagramming a decision point where chance may be involved in some of the decisions. For example, in a decision involving whether or not to purchase insurance, one “branch” of the tree could calculate the net EMV of no insurance and the other could calculate the net EMV of getting insurance. Each of these branches would have a best and worst case, the best case for either option being no insurance claim is needed. The best case for the “get insurance” option still requires paying the insurance premiums. The worst case in the “get insurance” option would be the cost of the insurance plus the cost of any deductible (multiplied by probability). However, the worst case in the “no insurance” option would be that a risk event occurs and the organization needs to make a large payout. When calculating the EMVs, the probability adjustment would reduce the size of this payout to reflect its likelihood. In this case, both options would likely result in a negative EMV after the insurance payments are factored in, but the value of the model is that it would allow the organization to select the option with the smallest loss, in other words, to purchase the best amount of insurance relative to the risk.

Sensitivity analysis and simulation

Risk models can also be developed to understand how risks impact multiple parts of a supply chain system. Two common tools for modeling include sensitivity analysis and simulation, both of which are often developed in spreadsheets, but more specialized tools also exist. Users enter various input values, called variables, automated calculations occur on them, and the outputs show the impact on various supply chain metrics.

Sensitivity analysis

The *APICS Dictionary,* 16th edition defines a **sensitivity analysis** as

> a technique for determining how much an expected outcome or result will change in response to a given change in an input variable. For example, given a projected level of resources, what would be the effect on net income if variable costs of production increased 20 percent?

The key point about sensitivity analysis is that only one variable is changed at a time so that its impact can be studied in isolation. It can be used in risk analysis to study risks that have monetary impacts. For example, what would be the effect on net income if gasoline prices rise by 10 percent?

Simulation

The *APICS Dictionary,* 16th edition defines a **simulation** as

> 1) The technique of using representative or artificial data to reproduce in a model various conditions that are likely to occur in the actual performance of a system. It is frequently used to test the behavior of a system under different operating policies. 2) Within MRP II, using the operational data to perform what-if evaluations of alternative plans to answer the question, “Can we do it?” If yes, the simulation can then be run in the financial mode to help answer the question, “Do we really want to?”

A simulation can be used in risk analysis to enter a given risk scenario, meaning that multiple input variables might be altered from their baselines to fit a given set of assumptions. For example, if it is assumed that rising gasoline prices would place more demand on rail travel, then rail prices would be increased as well in the model. A common type of simulation is a Monte Carlo simulation.

The *APICS Dictionary,* 16th edition defines a **Monte Carlo simulation** as “a subset of digital simulation models based on random or stochastic processes.” Monte Carlo simulations use specialized tools or spreadsheet add-ons to allow developers to enter a range for each input variable rather than just one value. Then the simulation is run thousands of times using different random values from each input range at each pass. The result is an averaged set of results along with statistics such as probability distributions.

Once the organization has decided on an acceptable risk tolerance, identified, described, categorized, defined a risk rating for each risk, and entered these results in the risk register, it is time to debate possible risk responses, which is discussed in detail elsewhere in these materials.

Chapter 3: Risk Response

This chapter is designed to

- Define the four basic risk responses of accept, avoid, transfer, and mitigate
- Define a risk register, risk response plan, and risk response planning
- Explain the difference between preventive actions and contingent or corrective actions
- Describe how to generate and implement preventive action, prepare contingency plans, and share risks among supply chain partners.

Topic 1: Risk Response Planning

A key element in getting sufficient funds for supply chain risk management and for risk responses is to highlight that designing a secure supply chain—one that can keep functioning despite disruptive events—is a form of supply chain flexibility. You don't want to lose the ability to keep products and information flowing to customers during a disruption because part of your cost-management initiative has been to eliminate disaster planning. Every company buys insurance as a prudent investment. Risk response plans are investments like insurance. The organization needs to invest in security.

Deciding on risk responses starts with selecting a basic type of response for each identified risk, bearing in mind that what is needed is a best-cost risk response. While this means that the individual response needs to be cost effective, it also means that the organization wisely uses the funds it has allocated to its risk budget, which might mean that some risks get no response or a very inexpensive response. Once basic responses are selected, if a proactive response is called for, these individual risk response plans are developed. The organization then generates a risk response plan and summarizes all planned responses in the risk register.

Basic risk responses

An organization can take four basic responses for any identified risk, accept, avoid (exploit), transfer (share), and mitigate (enhance). The response in parentheses is the equivalent response for an opportunity. Accept is a passive response for either a threat or opportunity, while the rest are all types of proactive responses.

Each type is defined as follows:

- **Accept.** The *Dictionary* defines **risk acceptance** as "a decision to take no action to deal with a risk or an inability to format a plan to deal with the risk." In addition to risks that cannot be dealt with through planning, risk acceptance is often the strategy for low probability, low impact risks or risks that have high costs of proactive response. For example, sovereign risk includes the risk that a government could nationalize an entire industry. For each country the organization operates in, it will have to accept this risk. (If the risk is considered significant, it could avoid or transfer the risk by not working in the country or by finding an outsourcing partner in that country.) For opportunities, accept means to do nothing to make the opportunity become more likely or have a greater positive impact.
- **Avoid.** The *APICS Dictionary,* 16th edition, defines **risk avoidance** as "changing a plan to eliminate a risk or to protect plan objectives from its impact." For example, some pharmaceutical companies do not develop vaccines because of the risk of lawsuits from harmful side effects. For opportunities, this is

exploit, which is the opposite of avoid, meaning you invest as much time and money as is feasible in order to realize the opportunity.

- **Transfer.** Organizations can move the resource or financial effects of a risk to a third-party organization such as an insurance company or a supplier. This requires purchase of insurance or bonding or contractually transferring risk to an outsourcing partner. However, not all risks can be transferred, such as risks to production schedules for core competency activities that define part of the process's total end-to-end lead time (i.e., critical path). For opportunities, this is *share,* which transfers some of the benefits of the opportunity to ensure it can be realized, for example, by partnering with a specialist to add capabilities.

- **Mitigate.** Organizations apply preventive measures to reduce the probability and/or impact of identified risks. Proper design of facilities and processes, employee training, and compliance management are all examples. Methods for mitigating significant risks are discussed later. For opportunities, this is *enhance,* which means increasing the probability or impact of the opportunity. This might mean adding more personnel to a task, for example.

Responding to supply chain risks

Strategies to address supply chain risk should include a risk response plan and risk response planning. The *APICS Dictionary,* 16th edition, defines these terms as follows.

> **Risk response plan:** A document defining known risks including description, cause, likelihood, costs, and proposed responses. It also identifies current status on each risk.
>
> **Risk response planning:** The process of developing a plan to avoid risks and to mitigate the effect of those that cannot be avoided.

Risk response planning needs to be fully integrated into the organization's regular business processes for it to be effective. A way to achieve this integration is to perform regular progress reviews and risk response plan update meetings involving staff from a number of areas. Meeting outputs should include assignments of specific responsibilities to individuals.

The risk response plan is a living document that should be revisited regularly, such as at weekly or monthly meetings. The status of planned actions should be tracked at these meetings and signed off on once completed. New items can be added as new risks arise.

Some organizations will choose to combine the risk register and the risk response plan, generating just one large spreadsheet. In either case, some responses will require additional detailed plans of their own, such as a business proposal or project documents.

Preventive and contingent (corrective) action

Risk responses can be implemented in one or both of the following types of risk response plans:

- **Preventive action.** A preventive action is any risk response that occurs before a harmful risk event occurs. The intent is to respond proactively rather wait until an urgent response is needed.

- **Contingent/corrective action.** A contingent action is any risk response that occurs during a harmful

risk event or after it has occurred. The intent is to minimize the monetary, physical, or reputation damage from the risk event. A contingent action is called a corrective action when it involves responding to risk events related to variances from a plan. The intent of a corrective action is to get back on plan (e.g., back on schedule/budget).

Exhibit 3-19 shows an example of a risk response plan.

Exhibit 3-19: Risk Response Plan Example

Risk ID	Identified Risk	Response Type	Responsible	Preventive Response Team	Contingency Response Team	Preventive Budget Status	Contingent Budget Status
7.2.1	Nylon-12 supply could be disrupted for Product Lines A and B.	Mitigate and avoid	J. Rodriquez. VP Strategic Sourcing (jrodriquez@ corp.com)	W. Ngo Lead Purchaser (wngo@ corp.com)	J. Heisman Chemical Engineer (jheisman@ corp.com) P. Quincy Strategic Sourcing (pquincy@ corp.com)	US$190k of US$200k expended. Status: positive variance of US$10k.	US$20k of US$50k budget expended. Status: On budget.
7.2.2	Partner with Corporation ABC to build a second plant elsewhere.	Share	R. Russell VP Business Ventures (rrussell@ corp.com)	N/A	TBD	US$4k of US$10k expended. Status: On budget.	TBD

Risk ID	Preventive Action Plan	Start Date	Schedule Status	Contingent/Corrective Action Plan	Start Date	Schedule Status
7.2.1	Increase safety stock for raw material to 3 months' supply.	3/2017	Safety stock ordered, not yet arrived. Status: On schedule.	Project to search for substitute materials: Phase I: Search for candidate materials. Phase II: Lab test materials. Phase III: Select a prequalified replacement supplier. See detailed Project Plan 7.2.1.	3/2017	40% complete (Phase I: complete, Phase II: 10% complete. Status: On Schedule.
7.2.2	Generate interest in a partnership to build a new plant for shared revenues and reduced pricing on raw materials (transfer pricing).	6/2017	Supplier reluctant but still in talks.	Develop a detailed business plan if supplier shows interest in partnering.	TBD	Dependent on supplier interest.

Given a set of risks that are considered significant enough to warrant a proactive response and an approved action plan to address the risks, the risk response process may involve the following actions:

- Preparing preventive action plans

- Implementing the preventive action plans
- Preparing contingent/corrective action plans
- Coordinating supply chain risk management and transferring/sharing risks among supply chain partners

Generating preventive action plans for each risk to be mitigated

The primary function of a supply chain is to keep goods, information, and payments flowing through the network and arriving in the right numbers at the right time and in good shape. Therefore, the significant risks to supply chains are events that might disrupt these flows.

Exhibit 3-20 provides a high level overview of key supply chain risks and some possible preventive action plans for each. Some of these risks and responses are later discussed in more detail.

Exhibit 3-20: Examples of Significant Risks and Preventive Action Plans

Examples of Significant Supply Chain Risks	Examples of Preventive Action Plans
Failure of a mode of transportation, such as a train derailment, a power outage that closes down pipeline pumping stations, operator strikes, or similar disruptions	Preventive maintenance of equipment and vehicles, safety training, backup power supplies, extra capacity at plants, safety stock, maintenance of good labor relations
Harm to goods, facilities, or markets caused by adverse weather, fire, floods, vandalism, or terrorist activities	Insurance, geographic diversification, security systems and guards, financial diversification, GPS tracking of transport vehicles
Lead time variability, orders incorrect, or quality problems	Safety lead time, counting or quality control at receiving, supplier certification
Loss of a key asset or supplier	Understanding suppliers' organization and financial solvency, contractually obligated backup suppliers, redundant equipment and repair parts on hand
Inadvertent noncompliance with regulations, ordinances, licensing requirements, etc.	Compliance audits, legal review of new regulations, supplier certifications
Theft of real or intellectual property	Security guards and ink tags on items, digital music protection requiring license verification
Failure of or dramatic change in patronage by an important customer	Diversification of customer base, customer relationship management, rewarding customer loyalty

Preventive actions can lead to easier implementation of contingency plans. For example, after Japan's massive earthquake and tsunami in 2011, the resiliency of Toyota's supply chain (preventive action) helped speed its recovery (contingency plans). As North American auto industry analyst DeRosiers said in an article by Deichler, "And Toyota in particular has an incredibly capable supply chain and may be able to manage their way through this entirely." Note that Toyota also had some extensive recalls related to sticking accelerator pedals and braking systems failing (i.e., they had process risk). Since these issues clearly relate to driver safety, they have been a massive hit to the automaker's reputation and bottom line. This example shows how even organizations with sophisticated supply chains and quality and risk management are still vulnerable to risk.

Topic 2: Preventive and Contingent Action Plans for the Supply Chain

In another section we introduced one way to categorize risks in supply chain risk management involving the following risk categories:

- Strategic supply chain risks
- Supply risks
- Demand risks
- Process risks
- Environmental risks
- Hazard risks
- Financial risks
- Malfeasance risks
- Litigation risks

We will discuss some potential responses to risks in those areas next.

Responding to strategic supply chain risks

Often the best way to address risks to supply chain strategy is to focus on the fundamentals, for example by developing better, more integrated products and communications in the first place. This may be done using the “design for x” or the many similar strategies discussed elsewhere in this learning system. Getting suppliers involved early or investing in information technology for better design, analysis, and visibility are other examples.

Responding to supply risks

Exhibit 3-21 revisits the same examples of supply risks you may have seen previously, only now some examples of preventive and contingent/corrective action plans are provided. The particulars of the supply chain and business model will dictate what responses are useful. Note that many of the contingent/corrective plans are more along the lines of traditional responses while the preventive action plans are often more progressive.

Exhibit 3-21: Responses to Supply Risks

Supply Risks	Examples of Preventive Action Plans	Examples of Contingent/Corrective Action Plans
Supplier/subcontractor availability	• Contracts with backup suppliers. • Audit suppliers on capacity resilience.	Approach supplier finalists from RFP processes or use approved vendor lists.
Supplier pricing	• Careful contract crafting and enforcement. • Due diligence.	Visit supplier and negotiate.
Supplier quality	• Contract penalty clauses. • Sampling and inspection.	Supplier corrective action plan and probation.

Supplier lead time	• Safety stock. • Large orders for priority. • Diversify suppliers.	Place next order early.
Transportation lead time	• Contract penalty clauses. • Outsource to 3PLs.	Benchmark and notify.
Customs/import delays	• Translate/edit paperwork. • Outsource to freight forwarding organizations.	Call government contacts.
Labor disruption	• Diversify sources. • Safety stock.	Negotiate in good faith and prepare alternative solutions.

For manufacturers, a critical area for supply risk management is related to the cost, timing, and availability of raw materials. This is because 50 to 70 percent of a manufacturing organization's cost of goods sold is from raw materials. While a traditional response to supplier instability used to be ordering larger quantities from just one supplier to receive favored status, this practice has been replaced by diversification, not only for better resilience but also because the old methods created an incentive to use less due diligence.

When it comes to logistics related risks, a common solution is to benchmark one's own logistics costs and risks to that of specialist 3PLs. After performing due diligence on such providers, if it lowers costs and risks, then it is generally a good way to transfer risk.

Responding to demand risks

Exhibit 3-22 provides examples of preventive and contingent/ corrective action plans for demand-related risks.

Exhibit 3-22: Responses to Demand Risks

Demand Risks	Examples of Preventive Action Plans	Examples of Contingent/Corrective Action Plans
Forecasting error or bias	• Use statistical forecasting to set safety stock. • Aggregate forecasts. • Use S&OP and demand-driven techniques to balance supply to demand.	Benchmark against actual results.
Interorganizational communications	• Promote supply chain visibility and data sharing • Adopt processes and shared systems.	Request a meeting among supply chain participants.
Outbound shipping delays	Set realistic expectations with customers.	Notify customers of problems right away.
Outbound transportation delays	Follow up with freight forwarders.	Have discussions with carriers and customs agents.
Customer price changes/promotions	• Regular conference calls. • Price concessions.	Rescheduling other deliveries to handle their demand spike.
Quality issues	• Audit quality processes. • Near-term specification	Reschedule and rework, increasing inspections.

	changes and lower prices.	
Warranties/recalls	• Renew quality/integration. • Use liability, tort, and warranty insurance. • Limit warranty period.	Carefully craft public message and avoid being in denial.
Lost customers	• Improve other risk areas. • Develop win-back and new customer programs.	Find new buyers for earmarked inventory if possible or write off.
Unprofitable customers	• Use profitability metrics. • Developed tiered service.	Avoid win-back programs with unprofitable customers.
Customer's requirements change	• Contractually require change review and control. • Assess profitability and turn down if unprofitable.	Insist on contract addenda or a new contract as needed.
Customer product launches	Meet regularly and get involved early.	Increase capacity if needed, including overtime.

Unplanned customer promotions are a key source of demand risk because it can create demand spikes that then result in shortages up the supply chain, followed by overreactions in terms of excess safety stock. This lack of communication can only be remedied by extraordinary efforts to develop trust up and down the supply chain so that information is shared. Software such as collaborative planning, forecasting, and replenishment (CPFR) can help.

As with supply management, if 3PLs can move freight to customers at a lower cost and with less risk, it is a good risk transfer given due diligence.

Responding to process risks

Exhibit 3-23 provides examples of preventive and contingent/corrective action plans for process-related risks.

Exhibit 3-23: Responses to Process Risks

Process Risks	Examples of Preventive Action Plans	Examples of Contingent/Corrective Action Plans
Capacity and flexibility	• Invest in configurable equipment to handle more than one product line. • Contract with backup suppliers.	Reschedule production runs or deliveries.
Manufacturing yield	Improve regular maintenance.	Reschedule or use excess capacity.
Inventory	• Improve communications and visibility. • Control safety stock.	Discount or write off obsolete/spoiled inventory.
Information delays	Inter-organizational information sharing.	Hold ad hoc meetings and overtime if off schedule.
IT/telecommunications	IT backup system projects.	Practice team responses and

		responsibilities in drills.
Poor payables processing	• Build cash flow cushion or get credit. • Contract renegotiations.	Discuss situation early.
Poor receivables processing	• Phone calls and dialogue. • In-person visits.	Consider using a collection agency.
Intellectual property	• International contracts. • Split up trade secrets among vendors or vertically integrate.	Use the courts, fines, and penalties.
Mismanagement	• Emphasize collaboration. • Clarify roles and goals.	Measure and report on gaps.

Process risks are generally internal risks that can sometimes be difficult to develop a response because they are systemic and difficult to change. It takes real change management and often a serious failure before an organization will see a need for change and overcome its culture. In the meantime, issues with poor processes reduce the supply chain team's ability and motivation to respond to other risks. Often the response that is selected is a workaround to compensate for chronic but low impact risks.

Responding to environmental risks

Exhibit 3-24 provides examples of preventive and contingent/corrective action plans for environmental-related risks.

Exhibit 3-24: Responses to Environmental Risks

Environmental Risks	Examples of Preventive Action Plans	Examples of Contingent/Corrective Action Plans
Environmental legislation/regulation	• Create a change management project. • Invest in ordered change.	Use overtime and contractors to get in compliance quickly, pay fines and penalties.
Industry regulations	• As above and hire industry experts.	Acquire industry contractors.
Country regulations	• As above and hire local experts/start a subsidiary.	Contract with local experts.
Shifts in cultural expectations	• Learn about expectations and develop change plan. • Develop brand image marketing plan.	Develop media talking points and control who talks to the media.
Conflict minerals	• Use due diligence. • Find alternate sources.	Disclose facts if already in public domain along with a remediation plan.
Customs regulations	• Switch to 3PLs. • Develop relationship with customs agents.	Remedial paperwork or full cooperation with requests.
Interest group attention	• Discover what they want and their motivations. • Develop plans that take as many of their concerns into	Develop media talking points and control who talks to the media.

	account as feasible.	
Voluntary reporting	Adopt standard reports like the UN Global Compact.	Prepare rebuttals to negative representation of the report.

While environmental regulations are often perceived as a burden, a key benefit is that they tend to develop or change slowly and so the organization has ample warning to develop a response plan.

Responding to hazard risks

Two important means of addressing hazard risks is through contingency planning for business continuity, which is addressed later in this topic, and through purchasing the right amount and types of insurance. Avoidance of working in certain geographic areas or geographic diversification can also help. A brief overview of insurance is provided next.

Types of insurance

Exhibit 3-25 reviews various types of insurance for the supply chain.

Exhibit 3-25: Types of Insurance for the Supply Chain

Commercial property insurance	Be sure it includes business interruption insurance.

- Facility must be damaged, inaccessable, or had an extended utility outage for a claim.
- Coverage usually only allows losses from disruptions at first tier suppliers.
- Ensure coverage for all types of losses with a high enough risk rating.

Business interruption insurance	Check conditions for when it is triggered.

- Usually part of first-party commercial property insurance.
- Conditions for claim: damage is sufficient to shut down all operations, type of damage must be a covered type (e.g., flooding is covered), and damage totally or partially stops employees or customers from entry.
- Has a mandatory waiting period to start and is limited in duration to about a year at most.
- Pays salaries, relocation expenses, and lost net income.

Contingent business interruption insurance	A.k.a, dependent property insurance (controlled by suppliers/customers)

- Insured customer or supplier losses provide you with reimbursement for lost profits or other transferred risks.

Cargo insurance	Damage or theft of goods in transit.

- Theft of containers is the most prevalent type of claim.

Trade disruption insurance	Insurance for trade disruptions not involving physical asset damage.

- Addresses property, marine, and political risk related to losses unrelated to your or your supplier's assets.
- Addresses nondelivery, project cancellations, government appropriations, and so on.
- Fills gaps in above types of coverage.

Global logistics insurance	Addresses numerous areas where third parties are handling your cargo.

- Many kinds exist, e.g., customs bonds (fee guarantees), bailee (holders of others' cargo), consolidator liability (using bills of lading and cargo receipts), foreign port operator insurance, ship hull insurance, and truck liability.

Cyber insurance	Protects from disruptions caused by IT failures and cybercrime.

- New type of insurance but a growning necessity.

Responding to financial risks

When responding to financial risks related to the insolvency of a customer or supplier, some traditional preventive measures include monitoring their financial ratios and metrics that predict bankruptcy risk and contracting with alternate suppliers. Some contingent measures include loans, possible mergers, and litigation.

In regards to market volatility and credit risk, preventive measures include developing larger cash balance cushions, maintaining unused credit facilities, and developing specific contingency plans for serious reductions of revenue streams including what products or services will be trimmed or stopped first.

For commodity price risk, responses include buying larger quantities of rare raw materials than is needed when the prices are favorable and purchasing of hedging instruments, as discussed below. Hedging can also be used for currency exchange risk, but another option is to avoid the risk by buying and selling in the home country currency whenever the other party also agrees to it. If the party maintains a foreign currency account it can use these funds for all transactions in that currency. The transaction becomes risk transfer if the other party will need to exchange the foreign currency. In this case, it will require different pricing as a compensation. The parties can also agree to share these risks (splitting the burden between both parties). An example of this is an agreement to revisit a price when it comes nearer to the payment being due and then to take into account changes in exchange rates. This is called a formal currency review and would need to be specified in the contract and be subject to legal and financial review.

Hedging

Hedging is a risk transfer tool for commodities, currency exchange, and financial instruments. Hedging is often used to lock in a price now for something that needs to be purchased in the future, such as a commodity or a foreign exchange transaction. By locking in the price now, the organization is transferring the risk of the price going in an unwanted direction to the party offering the hedging instrument. The organization is also sacrificing the benefit it would receive if the price of the underlying asset being hedged goes in a favorable direction. In this sense, a long term contract with a supplier that fixes prices is a form of hedging, since the supplier bears the risk of its raw materials going up but cannot pass on those costs. For this reason, many fixed-price contracts have escape clauses in the event of severe commodity or foreign exchange rate changes.

The opposite of hedging is speculation. The hedger is working to reduce risk (uncertainty), not to increase profits. The speculator is the other party to a hedging transaction, who is betting in the opposite direction. The incentive of a speculator is to make a profit. It is absolutely critical to have financial experts arrange hedges and that even these experts have governance review. Hedging can become speculation in the hands of inexperienced persons. Hedging can create large liabilities that must be settled. Hedging does not guarantee a favorable result.

Three types of hedging instruments are forwards, futures, and options. Forwards and futures are very similar, with the key difference being that forwards are customized deals between two parties (the other is often a bank) while futures are standardized deals offered by large financial exchanges in standard amounts and for a limited number of currencies and commodities. Otherwise the two instruments serve the same purpose: lock in a price now for something needed in the future. Both are mandatory, meaning that you need to settle

them regardless of what the market does. Forwards are often used for things not on the organized exchanges or when another party offers customized terms that fit very well. A risk is that the other party will default. This risk is very low when working with an exchange, but it can be significant with other parties.

An option is like a forward or a future, only you have the option to use it or not. You pay the writer a premium (fee) to gain this flexibility. The fees can be sizable and must be taken into account when calculating the overall savings or loss from the hedge. For example, if oil options are offered at €65 per barrel and you purchase an option to buy 100,000 barrels of oil next year for a premium of €5 per barrel, then you are effectively paying €70 per barrel, so at least you have some budget certainty. If the price were €66 per barrel, you would exercise the option and pay €65 + €5 per barrel. The market price would need to be higher than €70 per barrel to be a real savings. If the price was €$50 per barrel however, you would not use the option and buy on the open market. The effective price for you would be €50 + €5 per barrel since the fee is paid either way.

Responding to malfeasance risks

Responses to theft (and other loss), bribery, abduction, corruption, counterfeiting, and other forms of criminal behavior need to be comprehensive and start at the top of the organization in the form of good governance and clearly stated policies and procedures. A good general response is to set up a comprehensive security system for the supply chain. A relevant standard to guide such a system is ISO 28000. As defined in the *APICS Dictionary,* 16th edition, **ISO 28000** is

> an International Standard that specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.

Other examples of responses follow.

Theft, damage, and vandalism

Theft, damage, vandalism, and other forms of loss of goods can be combatted in part by investing in information gathering and sharing. Organizations exist that track thefts and help coordinate theft incident communications, recovery, and deterrence, thus helping to coordinate the responses of law enforcement in multiple countries. For example, the CargoNet platform provides near-real-time theft alerts to organizations and law enforcement.

Loss of goods can be mitigated by insurance, but insurance cannot immediately replace inventory, nor will it fully reimburse a loss if there is a deductible. Proper security and handling procedures can reduce the occurrence of internal and external threats to inventory loss. Many of these procedures involve setting and enforcing proper operational and financial controls. One example of a key control is segregation of duties. For example, a warehouse employee should not be able to approve a material move and also carry out the move. Matching of invoice to purchase order and receiving documents is another control.

Incomplete enforcement or special exceptions for controls can cause problems. For example, one organization had a rule that prohibited unauthorized vehicles from parking in the warehouse yard. An exception was made for one employee, and one night after work he discovered a package taped to the underside of his bumper. He informed security and they left the package in place, eventually discovering a

ring of warehouse employees engaging in theft. While the employee with the vehicle was trustworthy, the exception to the control had been costly to the organization.

Other examples of preventive security measures include the following:

- Reducing product complexity or standardizing parts across product families to reduce the total number of supply chain sourcing risks
- Rerouting shipments to avoid problem areas
- Installing ISO/PAS 17712–approved seals on shipping containers (ISO/PAS 17712:2010 is the ISO publicly available specification [PAS] regulating classification and use of seals on shipping containers.)
- Selecting safer transportation modes (e.g., rail is less vulnerable to hijacking than trucks)

Preventive equipment-handling measures may involve finding ways to reduce lead times for perishable inventory, redesigning packaging to compensate for poor handling by third-party shippers, ensuring that containers are watertight, or regularly maintaining refrigeration equipment. One example of a preventive measure against risk of loss from truck accidents practiced in Europe is to have the truck driver drive on to a railway flatcar and sleep while the truck and its goods are transported by rail, which reduces the likelihood of the driver falling asleep (and complies with regulations for drivers' hours of operations while keeping the truck moving). This is also an example of a situation where one response can mitigate two risks, since railway travel also reduces the risk of hijacking (the rail portion of the journey could be timed to occur in countries where hijacking risk is considered more significant on the roadways).

Bribery

A good preventive response for bribery is to invest in visibility. Cloud-based software now exists that can help headquarters arrange and supervise supplier selection, due diligence, ongoing contact, approvals, and payments. These antibribery systems help with information gathering, regulatory compliance, and investigations, and rate third parties by assessing and scoring their bribery and corruption risk.

Fraud and corruption

Fraud and corruption needs to be addressed internally as well as with suppliers. Both internal and external risks need to be addressed by following best practices. The U.S. Conference Board and the Center for Responsible Enterprise and Trade published a report that laid out a seven part compliance program:

- **Due diligence:** Examine both legal and financial records, as well as government relations, policies, and ethics.
- **Contractual rights:** Specify compliance with laws, regulations and anticorruption policies, using termination clauses as a penalty. Also include the right to inspect supplier records and perform audits.
- **Monitor and audit:** Search for criminal activity, review high-risk supplier payments, review supplier policies, re-certify suppliers regularly, and conduct visits and audits.
- **Set and enforce policies:** Provide policies and education to employees on anticorruption, internal and third-party reporting, and ongoing compliance.
- **Set and enforce procedures:** Use procedures to implement policies such as requiring signed employment agreements, team review of bids, third parties needing written policies, or multiple

required approvals for third-parties.

- **Governance:** Board-level governance sets the tone and a committee reviews internal audits, legal, finance, and compliance. Procurement will often have governance duties over suppliers.

Another way to combat fraud and corruption on the part of suppliers is to turn to supplier co-management, which involves using a third-party supplier vetting and monitoring organization with expertise and mature processes and systems. It can ensure thorough due diligence and ongoing compliance. Since these organizations specialize in managing supplier risk, they can invest heavily in controls, monitoring software, statistical analyses, and human expertise. These can be leveraged with many suppliers and on the behalf of many clients. Spending the same amount of time and money would not be cost effective for just one organization. Similarly, the experts at these organizations will be up to date on the latest regulations and can provide early warning of issues.

Abduction

What are companies doing to protect their executives and sales representatives who frequently travel? Many companies now have kidnap and ransom insurance for their key management. Currently about 75 percent of Fortune 500 companies invest in this kind of insurance. The world's largest provider of kidnap and ransom insurance, The Chubb Group, reported a 15 to 20 percent increase in the number of companies seeking such insurance between 2007 to 2010.

Many companies are now offering their key contributors training on how to keep themselves safe and minimize the risk of abduction. The companies are also hiring protection services and consulting firms to help with this goal. They recommend the creation of a written threat assessment and plan for each organization. Expatriate and other employees need to be made aware of local cultural and political situations that may put them at risk. They need to be taught what to do, and what not to do, if they are kidnapped. The company should inform them in advance of precautionary measures, such as varying their routes and regular schedules, and explain what actions the company will take to secure their release. Executives should understand that negotiations will be handled by security consultants and insurance professionals. Despite their natural reaction to want to take the lead in this situation, executives should not attempt to escape or negotiate with the criminals. Unfortunately, the successful and dramatic escapes of kidnap victims often portrayed in movies does not reflect reality.

Counterfeiting and intellectual property infringement

The key to reducing the impact of counterfeiting is to know when it is occurring. When an organization's suppliers turn to grey markets to meet demand in excess of capacity, they are not only risking a loss of quality but are also performing an illegal act. A way to combat this has arisen in the marketplace. Franchised excess and obsolete (E&O) dealers are organizations that buy up excess or obsolete inventory and then sell it to suppliers if demand returns. Dealers who offer guaranteed product traceability can sell original inventory back to suppliers in many cases. Requiring this traceability can reduce risks of counterfeits being introduced.

An organization that is taking the lead on anti-counterfeiting measures in the U.S. is the Nuclear Regulatory Commission (NRC), which faces such significant risk from counterfeits ending up in nuclear plants that it has promoted tough measures to combat counterfeiting. In addition to policies such as regularly auditing not only suppliers but also distributors, it also stresses ways to detect if parts are genuine and to trace products.

Thermo-mechanical analysis and advanced scanning technologies are being used to scan parts as they arrive. For traceability, it is using advancements in serialization and product tags as well as a unique marking called SigNature DNA, which is only visible in ultraviolet light and uses a plant-based electronic signature marking that can differ for each manufacturer.

In addition to testing and tagging goods, organizations can encourage their distributors to look for counterfeits and inform them when counterfeits are found. They can educate employees and channel partners regarding counterfeit problems. Research by Chaudry et al. indicates that these regular discussions with channel partners can be effective. However, their research also states that advertising the inferiority or dangers of counterfeits to customers or providing rewards to distributors for not purchasing counterfeits has proven less effective.

The research points to the following additional countermeasures for protecting intellectual property:

- Ensure that all trademarks and patents are registered in all countries where there is significant demand for the product. Do this quickly in foreign countries (e.g., first to file a trademark in China owns it.)
- Create an enforcement team that finds counterfeits for sale and follows up with investigative work, legal action, and law enforcement contact.
- Pursue actions not only against manufacturers but also distributors and retailers offering counterfeit goods or using the organization's brand.
- Create a database for tracking counterfeits and their resolution status.

To protect intellectual property when travelling to certain high-risk countries, leaving sensitive data or even data storage devices at home may sometimes be the best protection.

Additional protections against intellectual property infringement include the following:

- Develop internationally recognized contracts that adhere to the Convention on the International Sales of Goods (CISG) and check the references of the other parties thoroughly.
- Engage in trade dress protection, which protects against look alike products with minor changes and is enforceable under the U.S. Digital Millennium Copyright Act for online materials.
- Learn which countries are high risk and avoid doing business in these places or take extra precautions when it is necessary.
- Consider establishing operations in foreign countries or at least gain access to local expert representation for greater control and business savvy. Local expert representation can be given purchasing authority in the form of a purchasing office, which helps to evaluate suppliers.

Whenever possible, directly pursue offenders in that country's court system. If a government is failing to enforce its intellectual property laws and the organization is large enough to be considered an asset to that government, the organization can threaten to pull operations out of that country if the government is failing to enforce its laws.

Responding to lawsuit risks

According to an article by Michael Metzger, a Kelly School of Business professor at Indiana University, following a number of basic rules can help reduce the risks of legal losses. These rules are paraphrased as follows:

- View your actions from the perspective of how a jury would see it.
- Adhere to the truth and ethical standards.
- Don’t seek trouble, but assume it is seeking you and watch for it.
- Invest in the details because a small issue can sometimes end in a large cost.
- Always stay professional, unemotional, and imperturbable (e.g., emotional reactions can provide grounds for the opposition, and pursuing some cases can cost far more than settling).
- Document everything.
- Don’t make policies unless you intend to enforce compliance.
- Pretending a problem doesn’t exist and trying to forestall the inevitable are futile and costly endeavors.

Topic 3: Business Continuity and Plan Implementation

Preparing contingency plans related to business continuity

As defined in the *APICS Dictionary,* 16th edition, a **business continuity management system (BCMS)** is

> Part of the overall management systems that establishes, implements, operates, monitors, reviews, maintains and improves the organizational capability of continuing to deliver products or services at acceptable predefined levels following a disruptive incident. It is based upon identifying potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Contingency planning to ensure continued operations in the face of an emergency can be called a BCMS, business continuity planning, or disaster planning depending on the focus of the plan. While the terms are sometimes used interchangeably, in other cases continuity planning is used to restore business functions and workplaces while disaster planning is used to get IT and other business support systems back on line. Both are usually needed and could be addressed together or separately. A business continuity management system encompasses both of these types of planning and includes a framework for plan implementation and continuous improvement.

A relevant standard for business continuity management systems is ISO 22301. The *APICS Dictionary,* 16th edition, defines **ISO 22301** as “an international standard that specifies requirements for setting up and managing an effective business continuity management system.”

This type of planning involves designating specific individuals to take on specific roles during an emergency, such as one person who is designated to contact persons on a list to give them further instructions. However, plans should be disseminated and practiced in advance so that if communications are disrupted, the organization’s contingency team members can work without needing further instruction.

Contingency plans should include step-by-step instructions and plans that indicate priorities for restoring services, such as getting communications back online first, followed by vital information systems and key production processes.

A company should also have a designated spokesperson to work with the press so that a consistent message is delivered and the organization is not placed at further risk by an employee’s well-meaning but poorly chosen words.

When developing business continuity plans for the supply chain, business continuity can be called supply chain continuity. The *APICS Dictionary,* 16th edition, defines **supply chain continuity** as

> the strategic and tactical capability of an organization to plan for and respond to conditions, situations, and events as necessary in order to continue supply chain operations at an acceptable predefined level.

To make contingency planning a part of your supply chain strategy, consider the following tactics:

- Get support for contingency planning from the top. Executives should create a governance structure to ensure proper preparation.
- Run a business impact analysis project to provide real data on risks, responses, and costs/benefits of funding contingency plans. This involves interviewing business process owners and assesses facilities, identifies critical resources and processes, vital records and data, and internal and external dependencies. Critical recovery times are set as baselines.
- Be prepared. Develop contingency policies and plans and review them regularly.
- Make sure that specifically named supply chain professionals own the supply chain contingency plans and are responsible for keeping them current and implementing them if the need arises.
- Don't rely only on extra stores of inventory. There can never be enough of it to cover all potential problems and it, too, is vulnerable. You need alternate processes to keep functioning after a disaster.
- Research best practices in your industry and globally. Use service contracts to require that supply chain partners follow best practices and submit written contingency plans. Like all other supply chain processes, contingency planning should cut across company and functional boundaries. While each organization will have specific responsibilities in a disaster, all the organizations' activities will have to be coordinated.
- Develop a sourcing process that takes the loss of each key supplier into account and includes specific alternatives.
- When sourcing outside your borders, consider the total cost of the product or service being provided. Assessing the value of a supplier on the basis of price alone is foolish. Rely on knowledgeable intermediaries when assessing foreign suppliers and customers. How likely are your foreign partners to be disrupted by earthquake, flood, fire, famine, war, political interference, or economic uncertainty? In the world after September 11, tsunamis, hurricanes, and floods, you have to plan as if the apocalypse were possible. Taking another look at sources closer to home may be advisable.
- Pay special attention to maintenance of information flows. Telephone lines can go down and stay down for hours, days, and weeks. Power can go out for similar periods of time, and generators require fuel supplies that can also run out. Know how you're going to communicate among supply chain partners to coordinate the disaster plan's implementation.
- Track your shipments with RFID and global positioning. You can't implement a contingency plan until you know you have a problem.
- Purchase business continuity insurance, not just asset loss insurance.
- Test your plans, and train employees and managers to understand and implement them. Run drills or table top walkthroughs for specific events or portions of the plan such as data center recovery from backup. This helps prepare individuals and verify their level of preparedness.

Implementing risk response plans

Preventive action plans that are never implemented are useless. However, many plans remain just plans.

Failure to implement preventive (or contingency) plans is a risk in itself. Organizations need to assign an individual the responsibility of turning a plan into a project. This entails defining the goals for all stakeholders and setting expectations (e.g., setting improvement targets and what the plan will and will not address), winning final project approval and release of funds, and exercising project management to execute the project. The plan's relative level of success against its goals must be measured. The risk response plans and risk register should be updated, for example, by removing an irrelevant underlying risk from the list, modifying its probability, or other appropriate action.

Part of implementing risk response plans is to ensure others in the supply chain are dealing with risk on their end as well.

Coordinating supply chain risk management and sharing risks among supply chain partners

It is important to decide how to share supply chain risks among partners. Transferring and/or sharing risk can be a reason to create some type of alliance in the first place, or it can occur after a risk coordination committee makes recommendations. Risk transfer should be made on the basis of which party is best suited to minimize the risk or respond to a risk event. The goal should be to minimize overall system risk, not to minimize one's own risk at the expense of other partners.

A 2009 global multi-industry risk management project approved by the former Supply Chain Council devised a number of best practices for coordinating risk management in the supply chain, many of which are basically the same risk identification and assessment guidelines presented earlier. For example, it advocated that risk management be a formal and systematic process coordinated among partners to reduce the negative impact of risk events on the supply network. It also advocated for visibility and quantification of risk between supply chain members through processes such as joint risk identification and contingency planning.

Exhibit 3-26 lists some of the other best practices resulting from the study. (These practices also support SCOR Model 11.0.)

Exhibit 3-26: Risk Management Best Practices

Risk Management Best Practices	
Best Practices: Coordinated Risk Management	
Risk management program's coordination with partners	Coordinating risk management with supply chain partners by emphasizing cooperation among departments within a single company and among different companies of a supply chain to effectively manage the full range of risks as a whole; establishing a risk management coordination committee
Sourcing risk mitigation strategies	Includes strategies to address source risks, for example, multiple sources of supply, strategic agreements with suppliers, and supplier partnerships
Crisis communication planning	Creating joint contingency plans
Best Practices: Supply Chain Designed to Manage Risk	
Supply chain business rules	Establishing business rules (e.g., customer priority, supplier priority, production routing, transportation routing, etc.) based on minimizing supply chain risk

Supply chain information	Managing supply chain information networks to minimize supply chain risk; includes information sharing with partners as well as internal locations; helps all parties to be quickly informed of a real or potential disruption and respond quickly and appropriately to minimize the disruption impact
Supply chain network	Designing node locations, transportation routes, capacity size and location, number of suppliers, production locations, etc., in a fashion that mitigates potential disruptions to the ability to deliver product/service to the end customer

Source: Supply Chain Risk Management Team, Supply Chain Council, Inc., 2009

Chapter 4: Security, Regulatory, and Compliance Concerns

This chapter is designed to

- Describe some common security and regulatory concerns, including risk of loss and complying with import and export requirements
- Discuss the costs and benefits of participating in security partnerships as well as of meeting sustainability regulations
- Explain how product traceability assists with risk reduction
- Describe ISO 31000 Principles and Guidelines for risk management and its supplemental standards ISO 31010 and Guide 73
- Discuss some other guidelines and best practices in risk management.

Topic 1: Security and Regulatory Concerns

Effective supply chain management encompasses a wide array of security and regulatory concerns, especially in the movement of materials and reporting of transactions. Security and compliance issues often have implications for supply chain cost management, timing, or information systems that require management's involvement. Failure to comply with security and other regulations and requirements can result in problems ranging from costs and delays to significant fines or even complete shutdown of business activity followed by civil or criminal penalties.

The management challenge is to meet requirements imposed by countries and trading blocs as well as those mandated by tax revenue, environmental, and security agencies and to do so with the least possible financial impact. With the increased focus on security since the September 11, 2001, terrorist attacks in the United States, supply chain risk management has increased in importance and has become a major focus for supply chain managers.

Key security and regulatory issues include the following:

- Ensuring the physical security of modes of transportation and storage
- Meeting increased identification requirements and establishing systems to deny access of unauthorized people to supply chain materials
- Keeping supply chain information systems secure from hacking and denial of service attacks
- Deciding whether to voluntarily comply with global antiterrorism initiatives, such as the C-TPAT (Customs-Trade Partnership Against Terrorism) initiative in the United States or the AEO (Authorized Economic Operator) program of the European Union
- Maintaining proper internal operational and financial controls

An example of a risk related to physical security and compliance is the limitation on the amount of flammable materials that can be stored in a given warehouse. Warehouses with flammable (or explosive or otherwise unstable) materials need to manage risks by ensuring that there is sufficient stock of inventory to conduct business while staying below the regulatory limits for the materials. Ensuring compliance with all safety protocols is also a key risk control.

An example of a risk related to compliance with internal operational and financial controls is compliance with the U.S. Sarbanes-Oxley Act (SOX). Compliance with this act is required for any U.S. or foreign organization whose stock is publicly traded on U.S. stock exchanges. Segregation of duties to prevent conflicts of interest is a key concern. For example, the buyer in a transaction should not also be the seller or any associate of the seller who might profit from the transaction. SOX also requires that the organization's quarterly and annual financial reports disclose certain off-balance-sheet transactions and provide detailed descriptions of certain internal control systems. The off-balance-sheet reporting disclosure requirement could impact vendor-managed inventory (VMI) arrangements, for example, because this could involve moving an asset (inventory) off of the balance sheet. Similarly, outsourcing arrangements may need to show that adequate internal controls exist. Penalties for noncompliance could include fines from civil lawsuits brought by the U.S. Securities and Exchange Commission, reputation damage, or criminal suits against executive officers accused of falsely certifying reports.

Complying with import and export requirements

Details regarding import and export requirements were provided in the section on "Procure and Deliver Goods and Services." Here we address risks related to compliance. Compliance with import and export requirements can become complex due to myriad requirements and trade agreements in both the importer's and exporter's country. International shipping laws may also need to be considered.

Many times, these regulations contain numerous exceptions that can save the organization considerable expense if it understands these exceptions and applies them without inadvertently violating the regulation. For example, the harmonized system classification codes are used to identify a product's type, but there may be leeway to classify a good as one type or another, possibly resulting in a tax or customs advantage. However, a risk is that customs could disagree with the classification, resulting in delays and/or fines. Legal review is needed.

In addition, import/export can create significant risks of delays at customs. One way to mitigate this risk is to use electronic messaging to preclear product shipments rather than risking problems at the port of entry/exit. This is especially the case when the supplier lacks the trust of the importing government: Complex electronics or chemicals may experience customs delays as they are checked for contraband. Sourcing these goods domestically may be the only way to reduce this risk.

Two examples of import/export requirements are prohibited goods and labeling and documentation requirements.

Prohibited goods

Countries may prohibit certain goods from entering or leaving the country for national security reasons, domestic trade protection, or protection of the health and safety of its citizens. Some potential suppliers are banned because they are connected to terrorist organizations or organized crime. For example, in the U.S., several agencies maintain lists of prohibited individuals and entities, including the Office of Foreign Assets Control (OFAC). U.S.-based organizations and citizens are not allowed to trade with or have financial transactions with these entities. It is the organization's responsibility to check such lists for the countries in which they operate, although trade relationship management software can automate verification.

Another reason goods may be prohibited is due to a pandemic outbreak of disease or other source of contamination of foods or other goods. For example, a country could ban imports of toys if testing confirmed the presence of lead. After the 2011 earthquake in Japan, the U.S. prohibited imports of milk, fruits, and vegetables from Japan due to the radiation from damaged nuclear reactors.

Dangerous goods, which were covered in the section on “Manage Reverse Logistics,” also face restrictions. There is a movement to support more thorough documentation and disclosure of potentially problematic material content of goods exchanged in trade. One risk is having out-of-date information, which can be prevented by regular checking.

Organizations face serious consequences such as significant fines for failing to verify that goods can be imported or exported prior to attempting the transaction. The risk of ones’ own goods being prohibited due to contamination is likely a type of risk that cannot be adequately planned for and may or may not be covered by insurance.

Labeling and documentation

Product labeling and documentation regulations for imports and exports often require organizations to label goods in the import country’s local language(s). Delayed differentiation and delayed packaging strategies can reduce the risks of carrying too much product in one country and not enough in another solely due to packaging. Organizations should verify that they understand all labeling requirements such as product warnings, ingredient lists, or health facts. Also, many regulations exist related to misleading labeling, which creates a risk that a product could be banned.

There is a large amount of documentation for international trade, and as such there is a risk that some of it could be missing or incorrect. Documentation may include letters of credit, bank drafts, bills of lading, combined transportation documents, commercial invoices, certificates of origin, material safety data sheets, and insurance certificates. Each must comply with regulations. Such documentation may be required to be multilingual, not only for the country of import and export but for every country the goods pass through. When this documentation is complex, it creates a risk of delaying shipments to get the documents translated. One way this risk can be mitigated is for organizations to use standardized electronic messages when they are allowed in place of physical documentation.

Security partnerships

Because most of the imports and exports to and from a country are in the form of private party trade goods, governments wanting to increase border security and prevent terrorists from intrusion into supply chains have a choice: Subject all imports to additional security measures at enormous expense for the government and with lengthy delays to the movement of goods, or forge partnerships with organizations and other customs agencies to improve security. The primary benefit for organizations is that the customs process may be faster and smoother. Examples of security partnerships follow:

- C-TPAT for imports (defined below)—U.S.
- Authorized Economic Operator (AEO) program—EU
- Partners in Protection (PIP)—Canada
- Secure Trade Partnership (STP)—Singapore
- AA rating for customs—China

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a joint government–business endeavor for imports (not exports) to increase the security of supply chains and U.S. borders. Initiated by U.S. Customs, C-TPAT is based upon the idea that achieving the highest levels of security requires cooperation between the U.S. government and supply chain participants such as importers, carriers, brokers, warehouse operators, and manufacturers. U.S. Customs has used C-TPAT to establish mutual recognition security arrangements with New Zealand, Canada, Jordan, Japan, Korea, the EU, Taiwan, Israel, Mexico, and Singapore as of December 2014.

Costs and benefits of participating in security partnerships

C-TPAT will be used to illustrate the costs and benefits of participating in security partnerships. Various partnerships have differences, but the costs and benefits should be comparable.

Costs

Participation in C-TPAT by businesses is voluntary, but participation will result in costs related to implementation, audits, and compliance actions.

Acceptance in C-TPAT is based on submission of an online application and a signed agreement to take the following actions:

- Assess/validate the company's own supply chain security in accordance with C-TPAT guidelines that encompass procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security. Guidelines are available in the Resource Center.
- Submit a supply chain security profile questionnaire to U.S. Customs.
- Develop and implement a program to enhance supply chain security in accordance with C-TPAT guidelines.
- Communicate the C-TPAT guidelines to partners in the supply chain and work toward including the guidelines in relationships with those companies.

Benefits

In return for instituting C-TPAT security guidelines, participating businesses receive the following benefits (after evaluation of the application):

- Fewer inspections, for reduced border time (Note that while many partners do experience these benefits, C-TPAT legal language specifically states that membership will not speed up clearance or help avoid searches.)
- Assigned account manager
- Access to the C-TPAT membership list (provides members with access to C-TPAT–certified providers that may be appropriate to their supply chains)
- Eligibility for account-based processes such as bimonthly or monthly payments
- Emphasis on self-policing rather than customs verifications
- Membership treated as a positive risk-assessment factor by customs
- Helps establish the organization as a good community partner
- When mutual recognition arrangements exist, less duplication of effort between the countries' customs authorities (Participants have to conform to only one set of standards, not two.)

C-TPAT began offering partnership admission to importers and carriers with the intent to expand enrollment to all supply chain participants. Partly because of this and partly because the program is voluntary, supply chains may have some partners who are compliant and some who are not. Often a transportation partner such as a freight forwarder will participate in C-TPAT while the manufacturer may not. Business partners cooperate with customs in developing security guidelines, with the explicit intention of keeping costs down and reflecting a realistic business perspective.

Noncompliant C-TPAT participants may have their benefits suspended or the participation canceled. Otherwise, C-TPAT creates no new liabilities beyond existing trade laws and regulations.

Costs and benefits of meeting sustainability regulations

When sustainability regulations exist, they may take the form of voluntary partnerships, formal regulations with required compliance, or individual organizational initiatives. For voluntary programs or individual initiatives, the organization will need to weigh the costs of implementing compliance programs against their benefits. From a risk perspective, this could include lower reputation risk and lower risk of lawsuits for environmental or community impact of the operations of the business. For mandatory laws and regulations, the same costs apply, but the cost of noncompliance such as fines or legal liability may outweigh other considerations. These three types of sustainability programs are discussed next. Afterwards, there is a discussion of sustainability risks for packaging and shipping materials.

Voluntary program compliance

Examples of voluntary programs include programs to encourage reuse, recycling, and recovery of industrial materials and responsible handling of products at the end of their useful life. Material content reporting is part of such efforts. One example is the UN Global Reporting Initiative (GRI) which disseminates globally applicable sustainability guidelines for voluntary use.

One benefit of voluntary compliance is the ability to implement sustainability at a measured, cost-effective pace rather than waiting until mandatory compliance requires frantic effort. Another benefit could be an improved and less costly reverse logistics infrastructure in the long run. The costs could include infrastructure investments such as dirty equipment replacements, more expensive contracts with local suppliers, and new report preparation and disclosure costs. Another potential cost or benefit (risk) is that with increased disclosure comes increased scrutiny by the press or activists, which may or may not be positive.

Nokia provides one example of a company that has developed its own reporting system by applying GRI guidelines. This reporting system is accessible in our online Resource Center. It includes a summary of its extensive sustainability report, which includes disclosure of energy consumption, carbon dioxide emissions, water consumption, waste, and ozone-depleting substances.

Mandatory sustainability programs

As an example of a mandated sustainability regulation, the European Union’s Restriction of Hazardous Substances (RoHs) directive states that electrical and electronic equipment sold in the EU must be substantially free of six substances identified to be toxic to humans and the environment: cadmium, hexavalent chromium, lead, mercury, and two classes of poly-brominated plastics. To give it legal force, the directive was transposed into the national laws of EU member states. Penalties for products containing these

substances can be severe, including removal of an entire stock of product from the market. These laws require no documentation or product certification; rather they assume that all electrical and electronic products on the market after the directive's July 1, 2006, deadline should be compliant. However, compliance authorities could require that an organization prove its products are compliant, which can be a very difficult endeavor. Like other supply chains, electrical and electronic equipment supply chains have become extended and subcomponent designs are often based on functional requirements rather than being rigidly specified by the organization. This means that a supplier could design a subcomponent to function properly using substitutes, for example, several different types of transistors could be substitutes because they work the same even though they contain very different raw materials. Thus, the RoHs directive has resulted in a need for organizations to minimize their risk of noncompliance by gathering extensive information from not only their suppliers but their suppliers' suppliers on a continual two-way basis.

The risks involved in noncompliance with mandatory laws generally outweigh the cost considerations; it is a price of doing business in that region. If the costs of compliance prove to be too great to sustain profitable operations, the organization may choose to avoid doing business in that region.

Organization-specific sustainability programs

A third way that sustainability can be implemented is through independent programs. For example, the U.S. shoe manufacturer Timberland developed the following set of "EcoMetrics" to assess the environmental impact of its products:

- Energy to produce
- Global warming contribution
- Material efficiency (weight of product in relation to weight of material used in making it)
- Additional attributes (for example, use of renewable energy in manufacturing the product)

The company has also been developing a list of "ingredients" to include with each product, as food manufacturers list ingredients on their packaging. Since there are on average 55 parts per shoe, that task has proved difficult. However, the organization has made sustainability into a market differentiator, and a clear benefit is loyalty from market segments that value sustainability.

Sustainability risks from packaging and shipping materials

Not only the products exchanged in trade but the packaging and shipping materials involved can pose sustainability risks. Wooden pallets, for example, have become controversial for a variety of reasons. A number of countries such as the United States and China and regions such as the European Union have adopted international restrictions on incoming materials packed on pallets made of soft woods that may contain harmful insects. Acceptable methods of heat and chemical treatments are governed under International Standards For Phytosanitary Measures regulation ISPM15. Chemical treatments to sterilize the wood have come under fire for themselves being hazardous. Aside from harboring harmful pests, the pallets can be a significant source of waste if they are used only once and discarded (as many have been designed to be used). The wood itself is still a resource and should be recycled.

Solutions to the problems with wooden pallets include the following:

- Sterilizing the wood with heat or chemicals as per regulation ISPM15
- Reusing undamaged pallets and repairing damaged pallets

- Grinding up pallets that are beyond use or repair for recycling
- Using pallets made of materials such as plastic and corrugated cardboard
- Using slip sheets (corrugated or plastic sheets) instead of pallets, a solution adopted successfully by Home Depot, Xerox, and Apple Computer

The benefits of converting to sustainable shipping materials include lower risk of rejection at ports and possible innovation of even less costly shipping methods. The costs may include the inability to make full use of prior infrastructure investments and the need to invest in something that is not value-added in the eyes of the customer.

Product traceability and configuration management

Product traceability refers to the ability to provide a chain of custody for a product and its components or ingredients. Traceability tracks a product's source materials and the finished good itself by their national origin and production facility, through each point of distribution, possibly to the specific final customer.

Product traceability and configuration management

- Reduces the size of product recalls to just those items affected rather than having to expand the recall (and customer anxieties)
- Differentiates goods when region-specific bans on goods are put in place in response to contamination or food-borne disease epidemic risks
- Assists compliance audits, such as when verifying a claim that milk is free from bovine growth hormones as advertised
- Provides evidence that conflict minerals were not used
- Helps with compliance with free trade zone agreements and labels such as "Made in the U.S.A." (All or virtually all components must be U.S.-sourced.)
- Helps establish a chain of custody for sensitive goods such as pharmaceuticals as they move between countries and supply chain points (e.g., compliance with U.S. Food and Drug Administration regulations)
- Assists with customs inspections.

Product traceability and configuration management also affect trade agreements such as free trade zones, as discussed in the section on "Procure and Deliver Goods and Services." These agreements provide special benefits for goods originating within the trade zone country but have limits on the number of components or ingredients that can come from outside the zone. Tracing the national origins of product components may be necessary.

Traceability is enabled by technology systems such as some types of bar codes, radio frequency identification (RFID), global positioning systems (GPS), and information systems such as transportation management systems (TMS) and warehouse management systems (WMS). Each of these topics was discussed in the section on "Design the Supply Chain."

Topic 2: Risk Standards

Before discussing the ISO 31000 family of risk standards, this topic discusses risk management frameworks in general and provides a few examples.

Risk management frameworks

A risk management framework is an organizational structure that can be configured to support the organization's strategic and tactical choices regarding risk management. Frameworks that address risk include COSO ERM and Governance, Risk, and Compliance (GRC), which are discussed next.

COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed an Enterprise Risk Management (ERM) framework in 2001. COSO ERM is a process that the board of directors, management, and staff enact to set risk strategy, identify risk events, and manage risk within the organizations risk appetite, with the goal of ensuring organizational objectives can be met.

The COSO ERM framework has eight components that need to be tightly integrated:

- **Internal environment.** Perspective from which risk is viewed including risk management philosophy, appetite, ethics, and integrity.
- **Objective setting.** A formal objective-setting process aligns with organizational mission and risk appetite.
- **Event identification.** Identify threats and opportunities to objectives. Opportunities loop back to strategy/objective setting.
- **Risk assessment.** Risk likelihood and impact determine response.
- **Risk response.** Select a type of response that aligns with appetite.
- **Control activities.** Policy and procedure reinforce responses.
- **Information and communication.** Timely information is shared down, up, and across the organization.
- **Monitoring.** Management and audit continuously improves ERM.

Governance, Risk, and Compliance (GRC)

The GRC framework is like a three-legged stool: each leg must be in place for the organization to remain balanced: governance, risk management, and compliance. Governance is the decision-making hierarchy that forms the overall management approach of an organization. This is the tone at the top but also the tools and processes in place to get that message integrated into management activities so they are efficient and systematic. Risk management is the same identify, analyze, and respond appropriately methodology discussed elsewhere. GRC risk focus categories include commercial and financial risk, IT security risk, and legal and external risks. Compliance is conformance to stated requirements in the form of identification, assessment, prioritization, funding, and corrective action. This includes identifying applicable laws, regulations, contractual requirements, and internal policies, assessing the as-is state and the costs and benefits of compliance, then sufficiently funding compliance in order of priority. When deemed deficient, the organization self corrects.

GRC is implemented by focusing on alignment of executive and management agendas, selecting

organizational initiatives by risk weighting them, promoting accountability and standard communication channels, ensuring staff have visibility to current regulatory requirements, standardizing risk management workflow and using a central risk database, looking at expected monetary value from the perspective of brand equity, monitoring key risk indicators, and aggressively meeting compliance to open up new markets.

The goal is to move GRC activities from feeling obligatory to just being part of the culture. A benefit of adopting GRC is that organizations can actually start taking more risks to pursue opportunities because they know what their appetite is and can quantify the costs and benefits more precisely. Emphasizing compliance can also help an organization successfully expand globally.

Organizations will know they are succeeding with GRC when their overall expected monetary value of risk goes down each year along with its overall cost of compliance, when new market revenue goes up, its compliance audits were positive, and its governance activities were successfully enacted more times per year.

ISO risk standards

The ISO Working Group on Risk Management, chaired by Kevin W. Knight AM (Order of Australia), developed ISO 31000, ISO 31010, and a complementary resource, ISO Guide 73:2009, Risk Management Vocabulary. These are discussed next.

ISO 31000

According to the *APICS Dictionary,* 16th edition, **ISO 31000** is

> a standard adopted by the International Standards Organization that outlines principles and a set of guidelines to manage risk in any endeavor. The standard outlines guidelines for understanding risk, developing a risk management policy, integrating risk management into organizational processes (including accountability and responsibility), and establishing internal and external risk communication processes. ISO 31000 is not a management system standard and is not intended or appropriate for certification purposes or regulatory or contractual use.

Published in 2009, it is designed to help any size or type of organization effectively manage risk. It includes a framework and processes for systematic development of risk management at an organization. Frameworks are designed to be adapted to the specific risk needs of an organization in terms of scope and organizational context. Frameworks are also flexible and can grow with an organization and be subjected to continuous improvements.

Proper management of uncertainty makes an organization more attractive to investors and helps the organization to achieve its objectives. According to Knight in an ISO press release, “It can be argued that the global financial crisis resulted from the failure of boards and executive management to effectively manage risk. ISO 31000 is expected to help industry and commerce, public and private, to confidently emerge from the crisis.”

Knight added that “ISO 31000 is a practical document that seeks to assist organizations in developing their own approach to the management of risk. But this is not a standard that organizations can seek certification to. By implementing ISO 31000, organizations can compare their risk management practices with an

internationally recognized benchmark, providing sound principles for effective management."

ISO 31000 principles

ISO 31000 follows a set of principles that help develop and implement transparent and credible risk management systems. These principles can be paraphrased as follows:

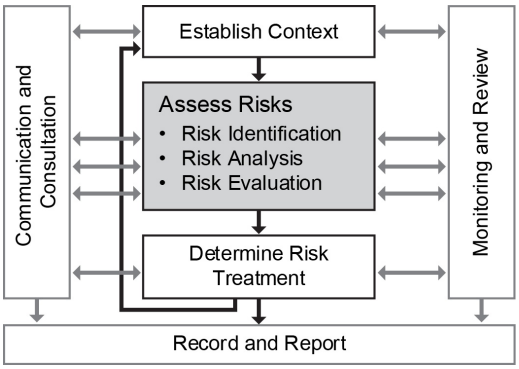
- Risk management adds value to the organization.
- It is integral to the organization's operational and decision-making processes.
- It unambiguously addresses uncertainty in an orderly, structured, and well-timed manner.
- It makes use of the best available information.
- It is customized to the organization and accounts for human and cultural factors.
- It is inclusive of all stakeholders, auditable, and transparent.
- It has a cyclical framework that allows for continual improvement, organizational learning, and responsiveness to changing environments.

ISO 31000 framework

The ISO 31000 framework, at a high level, is an iterative process that starts with an executive-level mandate and commitment toward risk management. This mandate should be based upon the ISO 31000 principles just mentioned.

This step leads to the customization and design of the framework itself, which is then implemented, monitored and reviewed, and continually improved based on review results, which leads back to further customization and design. In the implementation phase, the framework contains a set of subprocesses that are also iterative, as shown in Exhibit 3-27 (actual ISO process names differ slightly).

Exhibit 3-27: ISO 31000 Process Framework for Implementation Phase



ISO 31010—Risk Management–Risk Assessment Techniques

ISO 31010 is a supporting standard for ISO31000. ISO 31010 is intended to help organizations select systematic risk assessment techniques. After providing an overview of risk assessment concepts such as a framework and the overall process, the standard reviews the process discussed in ISO 31000 with more emphasis on risk analysis, including the following topics:

- Controls assessment
- Consequence analysis
- Likelihood analysis and probability estimation
- Preliminary analysis
- Uncertainties and sensitivities

In addition to discussing how to monitor and review risk assessments, the standard also discusses how to apply assessments during various life cycle phases.

The standard then turns to how to select techniques based on what resources are available, how much uncertainty is present and its nature, and the relative complexity of the system.

An appendix to the standard reviews and compares a wide range of risk assessment techniques, many of which are discussed elsewhere in this learning system. Examples of techniques reviewed include interviewing, brainstorming, root cause analysis, Ishikawa (fishbone) diagrams, checklists, probability and impact matrix, decision tree analysis, failure modes and effects analysis (FMEA), Monte Carlo simulation, and many more.

ISO Guide 73:2009

ISO also published ISO Guide 73:2009, Risk Management Vocabulary. The *APICS Dictionary,* 16th edition, definition of **ISO Guide 73** follows:

> Provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

This glossary complements ISO 31000 by providing organizations and their extended supply chain partners a way to discuss risks using a common understanding of risk management terms and definitions. According to Knight, ISO Guide 73 will “ensure that all organizations are on the same page when talking about risk.”

Benefits of ISO 31000, ISO 31010, and Guide 73

Benefits for organizations of implementing ISO 31000, ISO 31010, and Guide 73 include the following:

- Implementation increases organizational risk awareness and identification.
- It increases the probability of meeting or exceeding organizational objectives due to better operational resilience, efficiency, and effectiveness.
- It reduces the probability of identified risks and reduces losses from risk events.
- It allows more accurate assessment of internal strengths and weaknesses and external opportunities and threats (i.e., SWOT analysis).
- It helps with compliance with regulations, laws, and international standards.
- It enhances internal controls and corporate governance.
- It enhances external controls such as for financial reporting.
- It reduces uncertainty, improving stakeholder trust and confidence.
- Managers can proactively prepare for problems instead of just reacting.

- Managers can plan, decide, and budget based on reliable and custom tailored risk assessments.
- It assists with organizational learning.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

P

Q

R

S

T

U

V