CHAPTER 1

An Introduction to Risk

Risk and risk management are two terms that comprise a central component of organizations, yet they have no universal definition. In this chapter we discuss these terms, explain at a high level the manner in which a risk assessment is conducted, and discuss factors of which risk management practitioners should be aware in conducting such assessments.

This chapter also serves as an introduction to the body of work presented in subsequent Section I chapters and to the quantitative methodologies that supplement this information in Section II.

Definition of Risk

There is no single definition of risk or, for that matter, a set of heuristics or rules by which one can deem a given level of risk to be acceptable. However, we offer the reader the following definitions of risk, exposure, and events:

Risk = Probability that a problem occurs
Problem = An event or incident that would be harmful to objectives
Incidents or Events = Risk times the opportunities for occurrence, mitigated by the environment and control activities
Consequences = Harm or loss caused by an incident. The reverse of an objective
Exposures = Incidents times the magnitude of the consequences

COSO-ERM uses the word *events* for things that might happen, and could be favorable or adverse. Favorable events are important in some contexts, but we use the word *incident* when referring to adverse events. We also use the word *problem* to discuss the nature of what could potentially go wrong, creating an incident.

Let's begin with an example:

For instance, suppose that a data entry clerk will make an error in 1 out of every 10,000 keystrokes. She is tasked with inputting data containing a total of 1 million keystrokes. The risk of events occurring associated with a bad entry is then 1/10,000 =0.0001, whereas the number of opportunities for this event are 1 million. Thus the expected incidents associated with a bad entry are 1/10,000 ×1 million =100 events.

The exposure associated with a risk is defined by the expected number of incidents of risk multiplied by the magnitude of the event's consequences. In most instances, this magnitude will be quantified in terms of dollars. Returning to our example, suppose we estimated that correcting each entry cost $0.50 in labor charges. We assume no other exposure due to these risks. Then the expected exposure associated with this risk would be $50.

The risk management literature sometimes uses the word *risk* to denote the nature of a potential problem and other times to denote what we call *exposure*. Generally, when risk management authors refer to *risk* in the singular format, they are referring to the probability of incidents occurring. However, when authors use the word *risks* in the plural, they usually are referring to either the nature of possible incidents or to exposures. These mixed meanings cause poor communication in discussions of risk management. However, within our framework, risk, incidents, and exposure are three different notions, related by the preceding definitions.

Risk management terminology is meaningful only in the context of the future. Incidents that have already occurred are said to have a probability of 1. Historical information will help us understand the probability of occurrence and opportunities associated with the risk, but the exposure of the event may still remain uncertain.

Consider the case of a material misstatement uncovered by auditors in a firm's financial statements. The probability that this event occurs is 1 by definition: The event has already occurred. However, the magnitude of the event is not yet fully understood. Due to the uncertainty in the magnitude, the exposure associated with this risk is uncertain. Even though the auditors may be able to quantify the size of the misstatement, the magnitude of the event remains unknown: Will shareholders punish the company for such an error? Will customers view the company differently? Has the company ruined the goodwill of those within its supply chain?

With this simple example we have also elaborated a potential complexity associated with risk management engagements: The realization of an event can necessitate the estimation of a completely new series of risks and exposures associated with these risks. Knowing what new risks and exposures necessitate estimation requires risk practitioners to have an intimate understanding of the firm's operations. For this reason, risk management engagements may also be called *operational assessments*. The scope and

depth of an operational assessment will largely depend on the goals set forth within an organizational risk management strategy.

The Risk Management Strategy

A risk management strategy is composed of three interrelated components: risk identification, risk evaluation, and risk mitigation. The form each of these components takes will differ by assessor and purpose. For instance, risk identification in a manufacturing setting might involve a detailed walk of the plant floor to examine hazards workers may face; risk identification performed by a C-level executive could seek to identify risks associated with the business's strategy. However, irrespective of the form a risk management strategy takes, the identification of risks must precede other actions taken by professionals in executing this strategy.

Risk Identification

Identification of potential risks is the first step in a risk assessment. Without proper identification of risks, a risk analysis will be sorely lacking in its potential implications. When identifying risks, a practitioner should not only elaborate these risks himself, he should also speak with other experts in the field applicable to the scope of the project to hear their opinions on potential risks. By doing so, the practitioner reduces the chance that a risk is not elaborated. *This issue is a risk of the risk assessment itself.*

Risk identification can take many forms, but we proceed with an example for a manufacturing setting. In Exhibit 1.1, we have elaborated a series of potential problems. Note that this list is not comprehensive.

The format of this list will look significantly different depending on the nature of the assessment. If the risk practitioner is focusing only on risks associated with labor strikes, the enumerated list will represent risks associated purely with labor strikes; if the risk practitioner is focusing on more broad, strategic objectives, the list will include higher-level items.

EXHIBIT 1.1 Examples of Potential Problems in a Manufacturing Setting

Problems
Labor strike
Retail market demand changes
Facility damaged by nature
Raw material inventory depleted
Power failure
Change in government regulations

Risk Evaluation

Having constructed lists enumerating potential risks of various problems, the practitioner should next enumerate consequences associated with each of these risks. How will revenue be impacted by these risks? How will customers be impacted? What about suppliers? Employees? All stakeholders in general? This list of consequences can serve as a foundation for an analysis of exposure due to potential risks.

Once exposures have been evaluated, it is important for the practitioner to next elaborate control measures that are currently in place to mitigate these risks. Various frameworks exist to evaluate these controls, but the one we employ in this book is an augmentation of the COSO Enterprise Risk Management Framework. Current control measures can serve to minimize the probability that an event occurs as well as the magnitude of exposure associated with the event. For example, removing causal factors of a fire from an ignition source effectively lowers the probability that such an event will occur. However, having up-to-date fire sprinklers in place to remediate the fire minimizes the magnitude of the exposure: They help prevent the fire from spreading.

Another component of risk evaluation is the act of comparing levels of risk to organizational tolerances. Risk will be present in any organization, no matter how well run that organization is. Risk is not only a function of controllable events, it is also dependent on events for which we have no control—for example, natural disasters. The important issue within the risk evaluation framework is that potential risks, having been enumerated and analyzed, are accepted as tolerable by the organization.

Risk Mitigation

Once risks have been identified and the consequences and controls elaborated, a risk mitigation strategy should be implemented. This strategy should focus on any risks and exposures that the organization deems intolerable. Risk mitigation might involve revising current control measures, implementing new ones, or removing causal factors that could cause risks.

In implementing a risk mitigation strategy, a practitioner should focus on decreasing both the probability that the event occurs and the exposure associated with the event, should it occur. Doing so will best allow the effect of the risk to be minimized.

For a risk mitigation strategy to achieve effective results, it is important that all individuals within the concerned process support proper mitigation procedures. A proper "tone at the top" should be set by a manager prior to strategy implementation, the strategy should be implemented by practitioners, and periodic audits should be conducted to ensure that the mitigation

process is in fact occurring according to plan. The nature of the mitigation strategy—and the players involved in it—will largely depend on the scope of the risk management engagement.

The Scope of a Risk Management Engagement

A risk management engagement is a function of the scope and desired precision of the assessment. In compiling a risk management strategy, it is essential for a risk practitioner to first identify the scope of the engagement. Is the practitioner responsible for assessing strategic risks to the organization? Operational risks? Financial reporting risks? Regulation compliance risks? The scope should be mutually agreed on by both the practitioner and the "customer" associated with the assessment. When a risk practitioner is someone outside the organization, it is relatively easy to identify the "customer": It is the person or people calling for the engagement. However, when the risk practitioner is himself a member of the organization desiring the assessment, he must first understand who will be the eventual recipients of his report. He can then contact these individuals to devise a proper scope for the engagement. Once a common scope is achieved among the future recipients of the risk assessment, this scope should be well documented and circulated to keep the engagement focused on its original objectives.

The desired level of precision is another important estimate that risk practitioners must make at the onset of any engagement. An auditor's standard of precision is usually the threshold for materiality. Board members could have very different standards of precision for engagements tasked with assessing strategic risks to the organization. They might want to know with a high degree of precision the risks associated with new product development processes or external threats from competitors.

Of course, many individuals will desire a very high degree of precision; however, they are not willing to expend unbounded costs in achieving this goal. Establishment of a proper budget in conjunction with a risk management engagement can assist all parties in making sure the engagement achieves its desired objectives. In this way, managers and practitioners can optimize the level of risk assessment they want to perform for any given task. Understanding the economics of risk management can help a practitioner with such a cost/benefit analysis. Optimization of risk management costs and benefits can be thought of in a manner akin to standard economic intuition: namely, that the level of the assessment should occur where the marginal benefits associated with conducting the assessment equal the marginal costs. There will likely be decreasing returns associated with the expansion of any risk management engagement. It will generate large marginal benefits for low levels of cost, but as costs begin to increase, these marginal benefits will

tend to decrease and level off. Understanding this issue will help managers "right-size" risk assessments with their associated objectives.

Influences in Risk Assessments

Assessing the risk of a given event is a function of many factors. Professional judgment, the quality of information, and bias are but a few that influence a practitioner's estimate of risk.

Professional Judgment

Professional judgment is one of the most important factors a practitioner must use in estimating risk. Here we speak of judgment not as a final assessment of risk but as a factor that should be employed to arrive at a conclusion. Practitioners amass large amounts of experience over their careers; they see the effects of business cycles on the organization, they witness the changes made due to consumer demand shifts, and they understand the organization's culture. Significant knowledge of each of these issues allows a practitioner to critically examine evidence in whatever form it takes.

In the coming chapters, we show that risk assessments must be made using subjective information. If organizations were able to analyze risks using only available objective data, risk practitioners, directors, and executives would have a relatively simple job. Unfortunately, purely objective data does not exist in the context of a risk assessment because of a central issue with the risk assessment process: We are estimating the risk associated with an event in the *future*, not a past event. Analyzing future risks introduces an element of subjectivity into a risk assessment. Past is not always prologue in the context of risk. Therefore, it is the responsibility of the risk practitioner to critically examine past information—and gather new information—about the riskiness of a particular event. He must then exercise professional judgment in estimating the future risk.

The Quality of Information

The quality of information, or Information Integrity™, is a central component of risk analysis. When a risk manager performs an assessment, he must first compile data from various sources within the organization. This information will primarily take two forms: It can be derived from automated systems or provided by individuals.

Before using the information in a risk analysis, the practitioner should understand and examine the source of the data. Although many organizations are replete with automated systems that provide information to many

users, it is important to note that these systems—though seemingly providers of objective information—can be corrupted or influenced by individuals. At the heart of each of these systems is a program that has been devised by an individual for a specific application. An error in this program can cause faulty data. For example, consider the number of computer glitches in a typical operating system. The interface with an organization's automated system is arguably less complex in its design, but it is also subject to fewer quality control checks and testing methods than a standard computer operating system. Moreover, the propensity for programming errors in an automated system is likely a function of its price.

If the price of an automated system is high, the manufacturer can employ more programmers in the debugging function. One could argue that rather than doing so, it is in the manufacturer's best interest to minimize the costs associated with production, and hence, the manufacturer would employ a minimum number of programmers in such a function. However, if a product sells for a higher price than another good in a competitive market, it must be true that consumers perceive a difference between similar goods, since one commands a higher price. If they did not, the higher-priced good would not sell.

Automated systems also face potential corruption from human errors. For instance, though a general ledger system can easily compile all outstanding receivables, it requires that these receivables are first recorded properly by a data entry clerk to ensure information accuracy.

With respect to information obtained from individuals, it is important that the risk practitioner always consider the potential incentives possessed by an individual. For example, if a component of a division manager's salary is a function of the division's sales, he might overstate the sales so that he receives greater benefits. Also consider the example of an engineering manager working to build a prototype of a new product. If a risk practitioner asks this individual if the prototype will be completed on schedule, he might indicate that this is the case, even if he has a privately held belief that it is not true. The risk practitioner is thus always forced to evaluate not only the information he receives but also the source of the information. A practitioner can trust both an individual and an automated system to provide information, but it is important that he adhere to the adage, "Trust, but verify."

Arguably the largest risks within organizations are caused not by physical hazards but by the culture that pervades an organization. In gathering information, it is important to be aware of this culture and how it influences the quality of information received throughout the risk analysis process. This is especially true of executives and board members, who often use information that has been compiled by many individuals. The more individuals who "touch" the process, the greater the likelihood that the data generated by it will be corrupted.

Bias

Bias can be present in information received by the risk practitioner. We talked about *intentional* bias in a previous discussion on the quality of information, but bias can also be unintentional. If information about a population is constructed using sampling, it is important that the sample be representative of the population and free of bias. Careless collection of data can introduce significant bias, however unintentional, into information. Such bias could also be present when an individual provides information received from another source; the bias might be present with the individual creator of the data, independent of any bias from the disseminator. In procuring data for risk assessments, risk practitioners should thus always consider not just the *immediate* source of information but also the *originating source*.

Summary

Risk is a feature that is present in all organizations, no matter how well those organizations are run. The incidents associated with an event can be defined by the probability that the event occurs, multiplied by the number of opportunities for this event to occur. The exposure associated with an adverse event is equal to the probability of the consequences multiplied by the magnitude of the consequences.

In performing risk management engagements, practitioners should strive to minimize these two elements associated with potential risks faced by the organization. They should also be conscious of the quality of information they receive, the bias inherent in any datasets they analyze, and the professional judgment required of those preparing the data.