Enterprise Risk Management

A Methodology for Achieving Strategic Objectives

GREGORY MONAHAN

Contents

CHAPTER 1

Defining Enterprise Risk Management

A trusted colleague and friend advised me that I should not begin with a definition of the term "enterprise risk management." After much deliberation, I have decided to include my definition, because I feel it is imperative that you and I share a common understanding of what I am writing about in this book. If you accept my definition, then you can consider everything else I espouse within the context of this definition. If you prefer some other definition, you probably should consider whether the other things I say need to be adjusted for your preferred definition. That said, and with respect and thanks to my friend for his advice, I begin with definitions gleaned from *Merriam-Webster's Eleventh Collegiate Dictionary* of each of the words in the phrase:

Enterprise A unit of economic organization or activity; especially: a business organization

Let us proceed on the basis that an enterprise is a group of legal vehicles, divisions, business units, and so forth that make up an organization. I like the term "organization," because it seems to carry less connotation about the nature of the organization than, say, "company" or "business." In my view, "organization" carries no connotation of size, operation, or objective; it could just as easily be a local symphony orchestra as it could be the U.S. Federal Reserve or Barclays PLC. So an "enterprise" is an organization.

Risk Someone or something that creates or suggests a hazard

Here we need to move away from the dictionary definition (with all due respect) and consider a more professional, as opposed to casual, definition. What we are really talking about is variability; that is, risk is anything that produces a distribution of various outcomes of various probabilities. From here on think of "risk" as meaning "uncertainty," and imagine that we can represent that uncertainty as a distribution of possible outcomes of varying probabilities. I know we cannot always do that with a great deal of certainty or ease, and I am not suggesting we need to be able to. I am hoping that each time you read the word "risk" you will visualize a distribution of outcomes and associated probabilities. It might look like a typical normal (bell-shaped) distribution, or it might not; it does not matter.

In addition to defining risk, we need to consider those things that go hand in hand with risk. The SOAR (Strategic Objectives At Risk) methodology views risk in this context: Risk thrives on risk drivers or causes and manifests itself in events that have consequences (or outcomes). Let me repeat as this is an absolutely vital element to our definition of risk: Risk manifests itself in events that have consequences. Once you recognize that you are faced with a particular risk, you have to accept the fact that an event can happen and that it will have consequences. The SOAR methodology defines a process that (1) enables you to determine whether to take the risk and (2) prepares you for the consequence of an event. The other element in the risk universe is risk mitigation, or controls. The risk universe can be viewed in Exhibit 1.1.

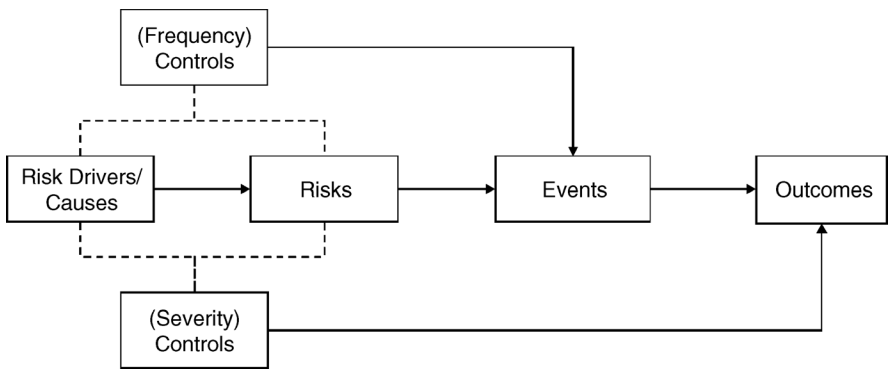

EXHIBIT 1.1 **RISK UNIVERSE**

In the exhibit, you can see what you often hear—for example, you might hear someone talk about:

- The risk of being hit by a car (being hit by a car is an event.)
- The risk of serious injury (serious injury is an outcome.)

From an organizational point of view:

- In key man risk, the event is someone of perceived importance leaving.
- In the risk associated with entering new markets, an event might be failure to adhere to local regulations.

I do not want to focus on the definition of risk, but I feel it necessary to comment on the definition of "risk" offered by Deloitte in "The Risk Intelligent Enterprise":

> Risk is the potential for loss caused by an event (or series of events) that can adversely affect the achievement of a company's objectives.[1]

Despite the fact that the definition recognizes only losses and adverse effects, Deloitte then goes on to say:

> The Risk Intelligent Enterprise views risk not just as vulnerability to the downside, but also preparedness for the upside.

I ask you this: Why would anyone who accepts the Deloitte definition of "risk" be prepared for upside? Consider also this definition: "The key is not to predict the future, but to be prepared for it."[2] The author, Pericles, fails to address the obvious question: "Prepare for what?"

It is sometimes difficult to articulate certain risks. The best way to get around this problem is to use the type of language employed in the examples given earlier. Let us say you are building a tunnel for a road under an existing structure (e.g., a city), and someone asks you to identify the risks you face. Do you say something like "tunneling risk"? Or "inaccurate measurement risk"? These are not very helpful responses. A more meaningful answer might be something like: "We might do something wrong that causes the tunnel to collapse and the stuff on top falls in, destroying buildings and killing people." Without really giving any definition of or name to the "risk," you have clearly articulated a driver (do something wrong), a possible event (collapse of the tunnel), and a couple of outcomes:

Buildings collapse and people die. The truth is, it does not really matter what you call the risk, or even whether you can clearly articulate it. However, it is absolutely essential that you are able very clearly to define those things around the risk: the drivers, the controls, the possible events, and the possible outcomes.

Let us work backward through the risk paradigm starting with one of our strategic objectives as the desired outcome. In this case, the outcome we seek (or objective we aim to achieve) is to be recognized as the country's best employer. Let us imagine that our distribution of possible outcomes includes us being rated as the worst, the best, or something in between. For ease, we will limit the outcomes to best, good, middle of the pack, poor, and worst. Our role, as enterprise risk management officers, is to manage a process that will provide the people responsible for the outcome(s) the best chance of achieving their desired outcome(s). The focus of that process must be on those elements that can influence the outcomes. From Exhibit 1.1, we can see that the elements that influence outcomes are (working backward from right to left):

- Events
- Risks
- Risk drivers
- Controls

Risks

I have defined "risk" as meaning "uncertainty," and I have proposed that the presence of risk (uncertainty) is evident in the distribution of possible outcomes. I think it is easy to fall into the trap of spending way too long trying to determine a clear definition of each risk associated with an objective. Take, for example, the case where your objective is to increase total revenues by at least 10% over the next year. You could, quite simply, summarize all of the risks you face as "the probability that we do not increase total revenues by 10% over the next year." Is that sufficient for application of the SOAR process? Absolutely.

In truth, I have included "risks" in my view of the risk universe only because I thought everyone would expect to see it there and that great numbers of readers would rebel if I did not include it. For the application

of the SOAR process, I advocate that risks be stated as in the previous example (i.e., the one about increasing total revenues), for three reasons:

1. By simply defining risk as the probability of not obtaining your objective, you maintain your focus on the fundamental concept of the SOAR methodology: You face a distribution of possible outcomes of varying reward and probability.
2. You do not waste time debating possible (and completely academic) definitions of the risks you face.
3. You have a much higher likelihood of identifying all of the possible influential factors—namely drivers and controls—and this is where your focus should be.

Risk Drivers

Risk drivers and controls are factors that influence the outcome. I distinguish between them as follows: Risk drivers are factors that increase uncertainty while controls are factors that are intended to reduce uncertainty or help soften the blow of an adverse outcome. It is useful to think of drivers and controls in terms of their impact on the distribution of possible outcomes. Take the case where there are no risk drivers; that is, the outcome is certain. In this case, the (certain) outcome could be represented as a single value on a graph (see Exhibit 1.2).

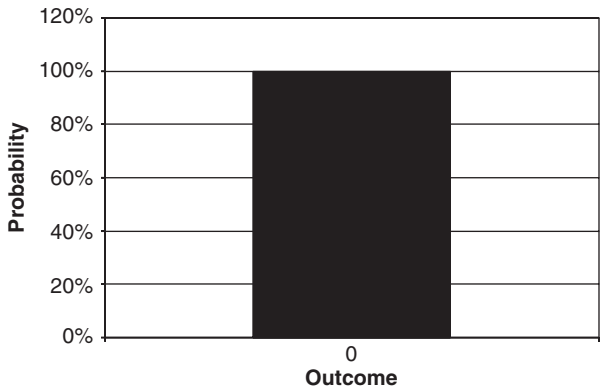

EXHIBIT 1.2 **CERTAIN OUTCOME**

In the presence of risk drivers, the distribution of possible outcomes might look something like Exhibit 1.3.

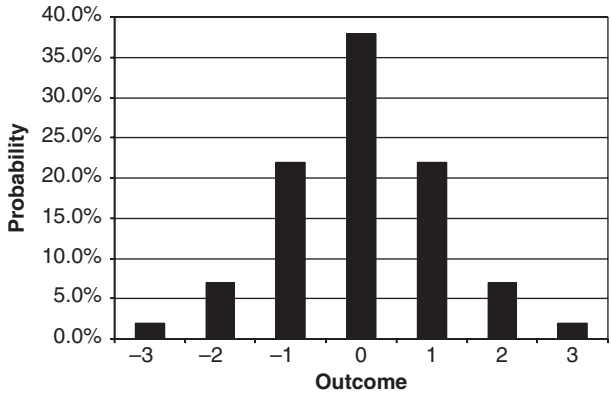

EXHIBIT 1.3 **SIMPLE DISTRIBUTION OF OUTCOMES**

Without any form of analysis whatsoever, let us assume that the greater the number of risk drivers, the greater the number of possible outcomes and that increasing the number of risk drivers flattens and broadens the distribution. This (assumed) effect can be seen in Exhibit 1.4.

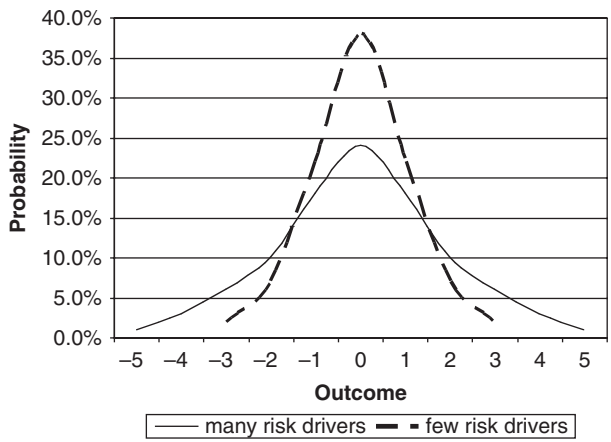

EXHIBIT 1.4 **DISTRIBUTIONS OF OUTCOMES INFLUENCED BY A DIFFERENT NUMBER OF RISK DRIVERS**

The fact is, of course, that our assumption is not always true. It will not always be the case that more risk drivers leads to a flattening and broadening of the distribution of possible outcomes. Furthermore, a single driver of risk A may produce a different distribution of possible outcomes than a single driver of risk B; the driver of risk A may produce something like the tall, thin distribution in Exhibit 1.4 while the driver of risk B may produce the shorter, wider distribution. Which would you rather face?

Controls

As discussed earlier, risk drivers and controls are factors that influence the outcome. I stated that controls are intended to reduce uncertainty or soften the blow. The term "intended" is used for a reason—to highlight the fact that controls are created with thought, as opposed to drivers, which simply exist. In addition, the term "intended" implies that the reality may differ from the idea; that is a control may not have the intended effect.

Similar to the difference between distributions of outcomes influenced by few risk drivers and those influenced by many risk drivers, distributions influenced by controls should be taller and narrower than distributions not influenced by controls. That is really the primary responsibility of the enterprise risk management office—to raise and narrow the distribution (of possible outcomes) around the desired outcome. The identification and application of controls is the most critical element of the SOAR process and the main reason for the enterprise risk management office to exist. Controls do not always soften the blow; often they are designed to avoid the hit altogether. In language more suitable to the context, controls are measures that are put in place to reduce the probability or severity of an adverse outcome. It is unusual for a control to be designed to reduce both frequency and severity. The brakes on a car are a good example of a control that reduces both frequency and severity. If you did not have brakes, you can be pretty sure you would crash more frequently than if you did have brakes. If you had an accident without braking, you can be pretty sure the damage would be worse than if you had braked. An airbag, however, can reduce the severity, but it is not intended to address the likelihood of an accident. A quick word of caution on the use of controls: Be careful they do not incite recklessness. To continue the car theme a moment, have you ever been in a car when the driver has said something like "strap in" as he

accelerates? The implication is that the driver thinks he can take more risk if the control is in place. In the context of application of the SOAR process, there is probably little to worry about—just keep in mind that the application of controls *may* influence behaviors in a way that you did not intend.

Inherent and Residual Risk

Exhibit 1.5 introduces the concepts of inherent and residual risk. Inherent risk is the raw or untreated risk that produces the set of possible outcomes, without controls. Controls are the vehicles employed by the enterprise risk management office to mitigate inherent risk and I, like many others, refer to mitigated risk as "residual risk." In the absence of controls, residual risk equals inherent risk. More generally, we can express the relationship as:

$$\text{Residual risk} = \text{inherent risk} - \text{impact of controls}$$

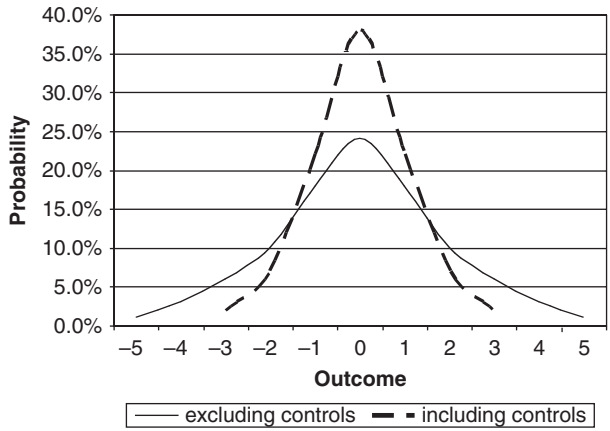

EXHIBIT 1.5 **DISTRIBUTIONS OF OUTCOMES INCLUDING AND EXCLUDING THE INFLUENCE OF CONTROLS (INHERENT AND RESIDUAL RISK)**

The equation is not strictly correct mathematically, as we have defined risk as being represented by a distribution, and the distributions of inherent risk and the impact of controls are not directly additive. However, the

equation is good enough for our purpose, which is to show that controls are the tools we use to reduce risk.

Residual risk should be the main focus of the enterprise risk manager as residual risk drives the distribution of possible outcomes and it is the distribution of possible outcomes that we are aiming to understand and manage. An understanding of residual risk implies an understanding of inherent risk, though that may not always be the case. If, for example, some unidentified control exists, it would be possible to mistake residual risk for inherent risk. An example would be something like active suspension in a car that stiffens to prevent body roll when cornering. As the driver, you may not know that the technology (i.e., the control) prevented you from having an accident (i.e., an event) as you took a corner at 80 miles an hour.

Events

Events are things that happen. They are important to the enterprise risk management office (and the SOAR process) for four reasons:

1. They evidence the presence of risk.
2. We can learn from them.
3. They have consequences, and these consequences are the things that we are trying to achieve or avoid.
4. They precede an outcome, so we may still have the ability to influence the outcome.

Outcomes

Outcomes are the consequences of events. Despite the fact that they are the ultimate element in the flow of risk, they can be controlled (i.e., they can be subject to the impact of controls). Consider, for example, the very common case of a car accident. The accident is an event. The outcome could be that your car is written off and you have to buy a new one, at a replacement cost of $20,000. In the presence of insurance, the *financial* impact (or outcome) of the event might be reduced to just $500, representing the policy excess (or deductible amount). This is the type of thing to which I was referring earlier when I mentioned "softening the blow" as part of our discussion on risk drivers.

Management

There are a couple of appropriate definitions for management:

Management Judicious use of means to accomplish an end
and
the conducting or supervising of something (as a business)

Think of "management" as meaning "dealing with it." But I must spend a moment on the meaning of "judicious" as it forms part of the definition of "management":

Judicious Having, exercising, or characterized by sound judgment

Those of you who know me even just a little might be expecting me to make some crack about the contradiction between "management" and "sound judgment," but I'm not going to, because we are using the term "management" as it relates to action rather than as a body of people. What I really want to point out is that "management" involves the application of (sound) judgment. If judgment is involved, will that add to the uncertainty? Unfortunately, the answer is more likely to be yes than no. But fear not, we will "manage" that!

Without thinking too much, we can imagine that our ability to influence the outcome decreases as we approach the outcome or rather that we have the greatest ability to influence the outcome if we can manipulate the risk drivers (causes) and the controls. Back to our example of aiming to be recognized as the country's best employer. Let us say employers are assessed on an annual basis, and the assessment is based on the results of surveys of employees. In order to be rated "best employer," we must get the highest average score across surveyed employees of a number of employers. We want our employees to recognize things we do as being in line with the actions of a great employer. In other words, we want to produce a number of outcomes that please our employees. Imagine that we decide to issue shares (i.e., the *event*) under a bonus scheme expecting that the *outcome* will be our employees think we are a great employer. With an enterprise risk management hat on, we consider the fact that our desired outcome is one of a range of possible outcomes, and we need to consider ways to maximize the probability of achieving our desired outcome. We recognize that one outcome that might eventuate is the bulk of employees become disgruntled at

the inequity of the share allocation, which seems to favor employees who already receive higher salaries. Still wearing the enterprise risk management hat, we would also consider that being rated "best" is a relative assessment, and that means that we need to consider what other employers are doing too. From that broader point of view, the enterprise risk management office needs to recognize the assessment of the organization of which it is a part relative to other employers as the ultimate outcome—or, rather, distribution of outcomes. From this point of view, events that lead to favorable outcomes include things our organization does well and things other organizations do poorly. Say, for example, that we were ranked second in last year's survey. If nothing changed other than the company ranked number one dissolved, we would be number one.

The enterprise risk management office has to determine the universe of possible outcomes and their probabilities, then look back at how those events might unfold and what the organization could do to make sure the events unfold according to a plan that maximizes the chance of attaining the goal. In doing so, the enterprise risk management office may have to accept that some elements of the ultimate outcome are beyond its control—such as the actions of other organizations that thrill their employees. Given that these are beyond their control, should the enterprise risk management office ignore them? Absolutely not. The organization must recognize risks beyond its control; in the case of unmanageable risks, the function of the enterprise risk management office is to help prepare the organization for the possible outcomes, albeit in the knowledge that the organization is unable to influence the outcome. Adverse outcomes still can be managed. Say that, despite our best efforts, we end up ranked second . . . again! "Managing" the outcome might involve preparing a cleverly articulated press release expressing delight at maintaining the second position and praising the efforts of all involved for helping the organization achieve this enviable result.

Enterprise Risk Management

What is our definition of enterprise risk management? Simple.

Enterprise Risk Management Dealing with uncertainty for the organization

I do not want to make it any more complex than that; there is nothing to gain from doing so. I will, however, bound the application of the methodology presented within this book to uncertain outcomes that should be dealt with at an organizational level as opposed to, say, by a line manager. To this end, I advocate the application of this methodology to the strategic objectives of the organization. This restriction is not inherent within the methodology; if you wish, you can apply it more broadly. I apply the methodology at this level because I see the management of risks associated with strategic objectives as being the most poorly addressed problem facing organizations today. I have developed the methodology to address this problem: a failure to manage the risks associated with attempting to achieve strategic objectives. By both the title and content of this book, I propose that enterprise risk management is defined as a methodology for managing risks associated with strategic objectives of an organization.

NOTES

1. Deloitte Touche Tohmatsu, "The Risk Intelligent Enterprise—ERM Done Right," Deloitte Development LLC, 2006.
2. Pericles, 495-429 BC.