CHAPTER

3

Risk

This chapter defines risk, explains how usefully to describe a particular risk, explains how risks are categorized, introduces different statistical calculations of risk, and describes how to analyze and assess risks.

Defining a Risk

At most basic, risks are the potential returns from an event, where the returns are any changes, effects, consequences, and so on, of the event (see Chapter 7 for more on returns and events). As some potential event becomes more likely or the returns of that event become more consequential, the higher becomes the risk. Realizing risk as a resultant of these two vectors makes risk more challenging but also more useful than considering either alone.

Taken alone, either the likelihood or the return would be an unreliable indicator of the risk. For instance, in Table 3.1 the most likely scenario is the least risky (scenario 3); the scenario offering the highest return (scenario 1) is not the riskiest; the riskiest scenario (scenario 2) has neither the highest probability nor the highest return.

Risk is often conflated with other things, but is conceptually separate from the event, the threat that causes the event, and any other cause or source. Such conceptual distinctions help the analyst to clarify the risk, principally by tracing its sources through the process to potential returns. You could be certain about the threat or certain about what the returns would be if a threat were to cause a certain event but uncertain about the probability of the threat acting to cause that event. Similarly, I could be certain that a terrorist group means to harm my organization, but I would remain uncertain about the outcomes as long as I am uncertain about how the terrorist group would behave, how my defenders would behave, how effective the group's offensive capabilities would be, how effective my defensive capabilities are, and so on.

Another common semantic error is the use of the phrase "the risk of" to mean "the chance of" something. The *chance of something* amounts to a risk. To speak of *the risk of death* does not make much

Table 3.1 The Likelihood, Return, and Expected Return of Three Notional Scenarios

Scenario	Probability	Return	Expected return
1	10%	$1,500,000	$150,000
2	20%	$1,000,000	$200,000
3	70%	$1,000	$700

sense except as the *chance of death*. When we speak of the *risk* of something, literally we mean the potential returns associated with that thing. For instance, literally the risk of terrorism is the potential returns from terrorism, not the chance of any particular terrorist threat or event.

Pedagogy Box 3.1 Definitions of Risk

Unofficial

Risk is "a measurable uncertainty" (Knight, 1921, p. 26), "a measure of the probability and severity of adverse effects" (Lowrance, 1976), "the potential for unwanted or negative consequences of an event or activity" (Rowe, 1977), "a measurement of the chance of an outcome, the size of an outcome or a combination of both" (Ansell & Wharton, 1992, p. 4), "uncertainty and has an impact" (Carter, Hancock, Morin, & Robins, 1994, p. 16), "the product of the probability and utility of some future event" (Adams, 1995, p. 30), "a measure of the amount of uncertainty that exists" and relates "primarily to the extent of your ability to predict a particular outcome with certainty" (Heerkens, 2002, p. 142), "uncertain effect" (Chapman & Ward, 2003, p. 12), "a scenario followed by a policy proposal for how to prevent this scenario from becoming real" (Rasmussen 2006, p. 2), "an uncertain (generally adverse) consequence of an event or activity with respect to something that humans value" (IRGC, 2008, p. 4), or "the likelihood and potential impact of encountering a threat" (Humanitarian Practice Network, 2010, p. xviii).

Semantic analysis sometimes "frames" a concept as an actor, action, and object in some context. "The 'risk' frame crucially involves two notions—chance and harm" (Fillmore & Atkins, 1992, p. 80). Therefore, risk is "the possibility that something unpleasant will happen" or "a situation which puts a person in danger" (https://framenet.icsi.berkeley.edu).

United Nations

Risk is the "expected losses (of lives, persons injured, property damaged, and economic activity disrupted) due to a particular hazard for a given area and reference period. Based on mathematical calculations, risk is the product of hazard and vulnerability" (UN DHA, 1992). Risk is "the combination of the probability of an event and its negative consequences" (UN ISDR, 2009, p. 11).

Australia/New Zealand and International Organization for Standardization (ISO)

Up to 2009, the Australian/New Zealand standard had defined risk as "the chance of something happening that will have an impact on objectives." From 2009, it joined with the ISO to define risk as the "effect of uncertainty on objectives," which is "often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence." "Organizations of any kind face internal and external factors and influences that make it uncertain whether, when[,] and the extent to which they will achieve or exceed their objectives. The effect this uncertainty has on the organization's objectives is 'risk'" (A/NZ, 2009, pp. iv, 1; ISO, 2009a, pp. 1–2).

Britain

Influenced by the Australian/New Zealand standards, the British Standards Institution (2000, p. 11) defined risk as a "chance of something happening that will have an impact upon objectives, measured in terms of likelihood and consequences." Nonetheless, the British government has no government wide definition. The National Audit Office (NAO) found that only 20% of departments (237 responded) of the British government reported a common definition within the department. The NAO defined risk as "something happening that may have an impact on the achievement of objectives as this is most likely to affect service delivery for citizens" (NAO, 2000, p. 1). The Treasury (2004, p. 49) defined risk as "uncertainty of outcome" and "combination of likelihood and impact." For the British Civil Contingencies Secretariat, risk is a "measure of the significance of a potential emergency in terms of its assessed likelihood and impact" (Cabinet Office, February 2013).

The Ministry Of Defense (2004, p. 3.4) has defined risk as "the chance of something going wrong or of the Department missing an opportunity to gain a benefit" (JSP525, May 2004: chapter 3, paragraph 4) and later (January 2010, p. 6) as "the consequences of the outcomes and how they could manifest themselves and affect defense business." "Military risk [is] the probability and implications of an event of potentially substantive positive or negative consequences taking place" (MOD, November 2009, p. 237).

Canada

Risk is "the combination of the likelihood and the consequences of a specified hazard being realized; refers to the vulnerability, proximity, exposure to hazards, which affects the likelihood of adverse impact" (Public Safety Canada, 2012, p. 81).

United States

Before the institutionalization of homeland security, the Federal Emergency Management Agency (FEMA) was the U.S. Government's effective authority on risk: "Risk means the potential losses associated with a hazard, defined in terms of expected probability and frequency, exposure, and consequences"

(Continued)

(Continued)

(FEMA, 1997, p. xxv). The Department of Homeland Security, which took charge of FEMA in January 2003, defines risk as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequence" (DHS, 2009, p. 111), although in the context of cyber risks a subordinate authority defined risk as "the combination of threat, vulnerability, and mission impact" (Cappelli, Moore, Trzeciak, & Shimeall, 2009, p. 32).

The Government Accountability Office (December 2005, p. 110) defines risk as "an event that has a potentially negative impact and the possibility that such an event will occur and adversely affect an entity's assets, activities, and operations."

The Department Of Defense (2010, p. 269) defines risk as the "probability and severity of loss linked to hazards."

Describing a Risk

A good description of risk helps analysis, recording, shared understanding, and communication. A good qualitative description of a particular risk should include the following:

- the temporal and geographical scope,
- the source of the potential event,
- the potential event,
- the probability of the potential event, and
- the potential event's returns.

This is a notional example of a good description: "Within the next year and the capital city, terrorists likely would attack a public building, causing damage whose costs of repair would range from $1 million to $2 million."

Pedagogy Box 3.2 Different Standards for How to Describe a Risk

The Australian/New Zealand and ISO standards (2009, p. 5) define a *risk description* as "a structured statement of risk containing the following elements: source, events, causes, and consequences." These standards prescribe *risk identification* as the second step in their 7-step process for managing risks. They define risk identification as a "process of finding, recognizing, and describing risks" including "risk sources, events, their causes, and their potential consequences" (see Chapter 8).

The Canadian Government generally follows ISO's guidance and does not define *risk description* but defines a *risk statement* as "a description of a risk, its likelihood, and its impact on any given environment" (Public Safety Canada, 2012, p. 85). Canadian federal guidance prescribes a description of the potential event, the natural environment, the meteorological conditions, and coincident vulnerability (Public Safety Canada and Defense Research & Development Canada, February 2013,

p. 16). The British Government's project risk management standard (PRINCE2®) prescribes a description of risk that includes cause, event, and effect (OGC, 2009).

The International Risk Governance Council (2008, p. 7) prescribes analysis of a risk by the following dimensions:

- degree of novelty (emerging, re-emerging, increasing importance, not yet managed);
- geographical scope;
- range of impacted domains;
- time horizon for analysis;
- time delay between risk and effects;
- hazard (ubiquitous, persistent, irreversible); and
- scientific or technological change (incremental, breakthrough).

A private British standard has prescribed the use of a table (see Table 3.2) in order to encourage a more "structured format" and fuller description of the risk, although readers might realize that this table looks more like a risk register or risk log (see Chapter 11) than a risk description.

Table 3.2 A *Structured Framework* for Describing Risk

1. Name of risk	[name]
2. Scope of risk	Qualitative description of the events, their size, type, number, and dependencies
3. Nature of risk	[category]
4. Stakeholders	Stakeholders and their expectations
5. Quantification of risk	Significance and probability
6. Risk tolerance/appetite	Objectives for control of the risk and performance
7. Risk treatment and control	Primary controls; confidence in existing controls; protocols for monitoring and review
8. Potential action for improvement	Recommendations to reduce risk
9. Strategy and policy developments	Identification of function responsible for developing strategy and policy

SOURCE: AIRMIC, ALARM, IRM, 2002, p. 6.

Categorizing Risks

Risks are routinely categorized by type. Categories help to communicate the scope of the risk, to assign the responsible authority to handle the risk, to understand the causes of the risk, and to suggest strategies for controlling the risk.

The subsections below describe categorizations as negative and positive risks, pure and speculative risks, standard and nonstandard risks, organizational categories, external levels, and higher functional categories.

Pedagogy Box 3.3 Prescriptions for Risk Categories

The Australian/New Zealand standard and ISO (2009a, p. 4) prescribe categorization of risks and list 6 categories (natural and competitive environmental; political; legal and regulatory; economic; socio-cultural; and technological). Similarly, the Canadian government prescribes a "risk taxonomy" — "a comprehensive and common set of risk categories that is used within an organization" (Public Safety Canada, 2012, p. 85). PRINCE2®, the official British project risk management standard, suggests categorizing risks at the end of "risk identification," before the "assessment," and offers 7 categories and 60 sub-categories. Another source on project management listed 10 categories and 64 sub-categories (Heerkens, 2002, p. 146). A typical government department or large commercial organization would identify even more subcategories. The World Economic Forum (in its latest annual report, "Global Risks 2013") identifies 50 global risks across 5 categories (economic, environmental, geopolitical, societal, and technological). By contrast, the International Risk Governance Council (2008, p. 6) recognizes just 4 categories of risk (natural, technological, economic, and environmental). Some project management authorities (such as the Association for Project Management) ignore risk categories entirely.

Negative and Positive Risks

The easiest but most neglected categorization of risk is to distinguish between negative risks (uncertain harm) and positive risks (uncertain benefit).

In general use, the noun *risk* is associated with harm, as in the phrase "a risk that this would happen" (Fillmore & Atkins, 1992, p. 81). The normative conception of risk as negative encourages actors to forget positive risks. Risk managers should remain aware of both positive and negative risks and not use confusing synonyms or conflated concepts to describe these categories. A disciplined analyst should look for potential allies and positive risks, so that, for instance, a government would not look on another country as a nest of negative risks alone and forget the chance of allies, trade, supplies, intelligence, and more. Although risk managers should always consider whether they have forgotten positive risks, in practice most risk managers are concerned with negative risks most of the time. Heerkens notes this below:

> With all due respect to the notion of capitalizing on opportunities, your time will probably be better spent focusing on trying to counteract threats. Experience tells us that you'll encounter many more factors that can make things bad for you than factors that can make things better. (Heerkens, 2002, p. 143)

Pedagogy Box 3.4 Official Conflation of Positive Risks

The reader might think that no responsible official could forget positive risks, but consider that the United Nations International Strategy on Disaster Reduction (2009, p. 11), the Humanitarian Practice Network (2010, p. 28), and the U.S. Government's highest civilian and military authorities

on security and risk each define risk as negative (GAO, 2005, p. 110; DOD, December 2012, p. 267). In 2009, the ISO added "potential opportunities" after admitting that its previous guides had addressed only negative risks (p. vii). The word *opportunity* has been used by others to mean anything from positive hazard to positive risk, while the word *threat* has been used to mean everything from negative hazard to negative risk. For instance, the British Treasury and National Accounting Office (NAO, 2000, p. 1) have defined risk in a way that "includes risk as an opportunity as well as a threat" and the MOD (2010, p. 6) has defined "risk and benefit" together.

Pure and Speculative Risks

Another binary categorization of risk with implications for our analysis of the causes and strategies is to distinguish between pure (or absolute) and speculative risks. Pure risks are always negative (they offer no benefits) and often unavoidable, such as natural risks and terrorism. Speculative risks include both positive and negative risks and are voluntary or avoidable, such as financial investments. This distinction is useful strategically because the dominant responses to pure risks are to avoid them or to insure against them, while speculative risks should be either pursued if positive or avoided if negative. (Strategic responses are discussed more in Chapter 10.)

Standard and Nonstandard Risks

Standard risks are risks against which insurers offer insurance at standard rates, albeit sometimes parsed by consumers. Most standard risks derive from predictable causes, such as unhealthy behaviors, or frequent events, such as road traffic accidents, that give the insurer confidence in their assessments of the risks. Nonstandard risks tend to be risks with great uncertainty or great potential for negative returns, like those associated with war, terrorism, and natural catastrophes (although a few insurers specialize in these risks). To insure against a nonstandard risk, the consumer could negotiate a particular policy but might fail to find any insurer, in which case the consumer is left to retain or avoid the risk (see Chapter 10).

Organizational Categories

Organizations conventionally categorize risks by the organizational level that is subject to them or should be responsible for them. Although many different types of organizations can be identified, they generally recognize at least three levels, even though they use terms differently and sometimes incompatibly (see Table 3.3). Thus, all stakeholders should declare their understanding of categories, if not agree upon a common set.

We could differentiate risks within an organization by level (as in Table 3.3) or by the assets or systems affected by those risks. Table 3.4 shows how different authorities have categorized these risks; I have attempted to align similar categories.

Table 3.3 Organizational Levels, by Different Types of Organization

	Typical organization	British standard organization (BSI, 2000, p. 13)	British official or private organization (AIRMIC, ALARM, and IRM, 2002, p. 6)	British governmental organization (Cabinet Office, February 2013)	United States official organization	Military organization (for instance: MOD, 2009, August 2011, and November 2011)
Highest level	Corporate	Strategic/Top management	Strategic	Strategic or gold	Strategic	Strategic
Middle level	Division or Department	Middle management	Project/Tactical	Tactical or silver	Program	Operational
Lowest level	Group, Unit, or Team	Operational	Operational	Operational or bronze ("hands-on work")	Project or Operation	Tactical

Table 3.4 Areas of Risk Within the Organization, as Listed by Different Authorities, With Similar Areas Aligned

Waring and Glendon (1998, p. 7)	British Standards Institution (2000, p. 14)	Business Continuity Institute, National Counterterrorism Security Office, and London First (UK BCI 2003)	British Treasury (2004, p. 17)	Australian/New Zealand and ISO (2009a, p. 4)
-	-	-	-	Stakeholder relations
-	-	-	-	Structure
Objectives	-	-	Change (new policies, new projects, change programs, targets)	Policies, objectives, and strategies
Culture	-	-	-	Culture
Resources	People	Personnel	Operational (service or project delivery, capacity and capability, and risk management performance and capability)	Capabilities (resources and knowledge)
	Finance	-		
	Infrastructure and physical plant	Physical assets		
-	-	Systems		Information systems

Levels

Like security, risks can be categorized through a hierarchy of levels, say from the global level down to the personal (see Chapter 2).

Most organizations distinguish at least their internal risks from the external risks. The Australian/New Zealand and ISO standard prescribes, as the first step in managing risks, establishing both the organization's goals and other *internal* parameters and the parameters of the *external* environment. The external environment has at least 4 levels: international, national, regional, and local (ISO, 2009a, p. 4).

Higher Functional Types

Some authorities have offered basic universal categories that could be applied to anything, within or without the organization, up to the global level. Many authorities essentially agree on these categories, although the terms vary. Table 3.5 shows the different categories recommended by these different authorities, with similar categories aligned.

For instance, the International Risk Governance Council (2008, p. 6) recognizes 4 categories of risk (natural, technological, economic, and environmental). The World Economic Forum, in its latest annual report (Global Risks 2013), identifies 50 global risks across 5 categories: economic, environmental,

Table 3.5 Higher Categories of Risk, as Described or Prescribed by Different Authorities

Australian/ New Zealand and ISO, 1995–2009	**Waring and Glendon (1998, p. 7)**	**UK Treasury (2004, p. 17)**	**UK MOD (January 2010, p. 6)**	**PRINCE2®, 1996–2009**	**World Economic Forum (2013)**
Environmental	Climatic	Environmental	Resource and environment	Environmental	Environmental
Political	Political	Political	Geopolitical	Political	Geopolitical
Legal and regulatory	-	Legal and regulatory	-	Legal and regulatory	-
Socio-cultural	-	Socio-cultural	Social	-	Societal
Economic	Economic	Economic	Economic	Economic, financial, and market	Economic
-	-	-	-	Strategic and commercial	-
Internal	Organizational	Operational	-	Organizational, managerial, and human factors	-
Technological	Technological	Technological	Science and technology	Technical, operations, and infrastructure	Technological

geopolitical, societal, and technological. The Australian/New Zealand and ISO (2009a, p. 4) standard lists 6 categories (natural and competitive environmental, political, legal and regulatory, economic, sociocultural, and technological). PRINCE2® offers 7 categories and 60 subcategories. Another source on project management listed 10 categories and 64 subcategories (Heerkens, 2002, p. 146). A typical government department or large commercial organization would identify even more subcategories.

Simple Statistical Calculations and Parameters

This section describes the different ways to mathematically calculate risk, predictable return, expected return, Program Evaluation and Review Technique (PERT) expected return, range of contingencies, the range of returns, and risk efficiency.

Formulae for Risk

Risk, as defined here in its simplest qualitative form, is easy to formulate mathematically as the product (Risk) of probability (p) and the return (R), or: $Risk = p \times R$.

The formulations of risk can be made more complicated by adding exposure or vulnerability or even the hazard or threat. Different formulae produce risk by multiplying: frequency by vulnerability (BSI, 2000, pp. 20–21); threat by vulnerability (Humanitarian Practice Network, 2010, p. 28); hazard by vulnerability, in the context of natural risks (Wisner, Blaikie, Cannon, & Davis, 2004, pp. 49, 337); hazard, vulnerability, and incapacity, in the context of natural disasters (UN ISDR, 2009, p. 4; Public Safety Canada, 2012, p. 26); exposure, likelihood, and returns (Waring & Glendon, 1998, pp. 27–28); or vulnerability, threat, and returns, in the context of terrorism (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006).

Managers of natural risks, especially environmental risks and health risks, are more likely to use and prescribe formulae that multiply: hazard by vulnerability; hazard by exposure; hazard by vulnerability by exposure; or hazard by vulnerability by incapacity. Notional examples of appropriate or effective qualitative formulations of hazard and vulnerability (or exposure) are listed below:

- One person carrying a communicable pathogen coinciding with a person without immunity will lead to another infected person.
- The proportion of the population with communicable diseases multiplied by the number of uninfected but coincident and vulnerable persons gives a product indicating the number of newly infected persons (ignoring subsequent infections by newly infected persons).
- The number of people who are both exposed to a drought and lack reserves of food is the number of people who would starve without external aid.
- Coincidence between unprotected populations and armed invaders indicates the populations that will be harmed or displaced.
- The rate of crime in an area multiplied by the population in that area gives the number of people eligible for victims-of-crime counseling.
- If terrorists attack site *S* with an incendiary projectile and site *S* is both undefended against the projectile and flammable, then site *S* would be destroyed.

These formulae are justifiable anywhere where the event or returns are predictable given coincidence between a particular hazard and one or all of vulnerability, exposure, or incapacity. None of

hazard, vulnerability, or incapacity necessarily includes probability, although uncertainty may be implicit in the assessment of a particular hazard or vulnerability (a higher rating of the hazard suggests more likely coincidence with the vulnerability; a higher rating of the vulnerability suggests a more likely failure of defenses).

Predictable Return or Event

In truth, given the formal logic in some of the formulae above that formally ignore probability, the product is a predictable return rather than an expected return (the commonest formulation of risk; see below).

In some formulae, the product is a predictable event, not a predictable return. For instance, Public Safety Canada (2012, p. 26) defines "a disaster" as a product of hazard, vulnerability, and incapacity. The disaster is a predictable event, given the presence of hazard, vulnerability, and incapacity.

Expected Return

Risk, in its simplest mathematical form, is the product of probability and return. If only one return were possible, this formula would be the same as the formula for the *expected return*. When we have many possible returns, the expected return is the sum of the products of each return and its associated probability. In statistical language, the expected return is a calculation of the relative balance of best and worst outcomes, weighted by their chances of occurring (or the weighted average most likely outcome). The mathematical formula is:

Figure 3.1 The Typical Formula for the Expected Return

$$ER = {}^{N}\Sigma_{i=1} (P_i \times R_i)$$

where:

ER = expected return

N = total number of outcomes

P_i = probability of individual outcome

R_i = return from individual outcome

For instance, if we estimate only two possible returns (either a gain of $20 million with a probability of 80% or a loss of $30 million with a probability of 20%) the expected return is 80% of $20 million less 20% of $30 million, or $16 million less $6 million, or $10 million.

Note that the expected return is not necessarily a possible return. In the case above, the expected return ($10 million) is not the same as either of the possible returns (+$20 million or –$30 million). The expected return is still useful, even when it is an impossible return, because it expresses as one number a weighted average of the possible returns. This bears remembering and communicating, because consumers could mistakenly assume that you are forecasting the expected returns as a possible return or even the predicted return.

The expected return does not tell us the range of returns. The expected return might be a very large positive value that we desire, but the range of returns might include very large potential negative returns. Imagine that we expect a higher profit from option *A* than option *B*, but the range of returns for option *A* extends to possible huge losses, while the range of returns for option *B* includes no losses. Risk averse audiences would prefer option *B*, but the audience would be ignorant of option *B*'s advantages if it received only the expected return. Hence, we should always report the expected return and the range of returns together.

Having said that, we need to understand that best or worst outcomes may be very unlikely, so the range of returns can be misleading too. Ideally, we should report the probabilities of the worst and best outcomes, so that the audience can appreciate whether the probabilities of the worst or best outcomes are really sufficient to worry about. We could even present as a graph the entire distribution of returns by their probabilities. Much of this ideal is captured by *risk efficiency*, as shown below.

Program Evaluation and Review Technique (PERT) Expected Return

If we identify many potential outcomes, then a calculation of the expected return might seem too burdensome, at least without a lot of data entry and a statistical software program. In that case, we could choose a similar but simpler calculation prescribed by the Program Evaluation and Review Technique (PERT), a project management technique originating from the US Navy. In this formula, we include only the worst, best, and most likely outcomes, and we weight the most likely outcome by a factor of 4.

The main problems with the PERT expected return are that the calculation excludes all possible returns except the worst, best, and best likely and the actual probabilities of each outcome.

The PERT formula may be preferable to the typical formula of expected return if consumers want to acknowledge or even overstate the most extreme possible outcomes.

Range of Contingencies

Many planners are interested in estimating the range of potential contingencies, where a contingency (also a scenario) is some potential event. Normally, planners are interested in describing each contingency with an actor, action, object, returns, space, and time. Such contingencies are not necessarily statistically described (they could be qualitatively described) but at least imply estimates of potential returns and can be used to calculate risk statistically.

Figure 3.2 PERT's Formula for the Expected Return

$$ER = (O + 4M + P) \div 6$$

where:

ER = expected return

O = the most optimistic return

M = the most likely return

P = the most pessimistic return

When lots of contingencies are possible, good advice, similar to PERT's advice, is to prepare to meet the likeliest contingencies and the worst contingencies (although judgments should be made about which of the negative contingencies has a high enough probability to be worth preparing for) and to shape the future toward the best contingency. Preparing in this way is often called contingency planning, scenario planning, or uncertainty sensitive strategic planning (Davis, 2003). However, judgments should be made about whether the worst and best contingencies are likely enough to be worth preparing for.

Range of Returns

The range of returns is the maximum and minimum returns (or the best and worst returns). Sometimes the difference between them is expressed, too, but the difference is not the same as the range. For instance, the range of returns from a project might be assessed from a profit of $2 million to a loss of $1 million—a difference of $3 million.

The range of returns is useful for decision makers who want to know the best and worst possible returns before they accept a risk and is useful for planners who must plan for the outcomes.

The difference (between the maximum and minimum or best and worst outcomes) is often used as an indicator of uncertainty, where a narrower difference is easier for planning. The difference is used as an indicator of exposure, too (in the financial sense, exposure to the range of returns). The statistical variance and standard deviation of all estimated returns could be used as additional indicators.

However, uncertainty is not measured directly by either the range of returns or the difference; also, the maximum and minimum returns may be very unlikely. Thus, the maximum and minimum returns should be reported together with the probabilities of each. You should also report the most likely return too. Indeed, PERT advocates reporting the most likely return as well as the worst (or most pessimistic) return and the best (or most optimistic) return.

Risk Efficiency

Some people have criticized the expected return for oversimplifying risk assessment and potentially misleading decision makers: "The common definition of risk as *probability multiplied by impact* precludes consideration of risk efficiency altogether, because it means risk and expected value are formally defined as equivalent" (Chapman & Ward, 2003). These critics prescribed measurement of the "adverse variability relative to expected outcomes, assessed for each performance attribute using comparative cumulative probability distributions when measurement is appropriate" (Chapman & Ward, 2003, p. 48).

This sounds like a complicated prescription, but the two criteria for risk efficiency are simple enough: the expected return should be preferable (either a smaller negative return or a larger positive return); and the range of returns should be narrower (sometimes we settle for a smaller maximum negative return or a larger minimum positive return).

By these criteria, an option would be considered preferable if its maximum negative return is lowest, the range of returns is narrowest, and the expected return is more positive. For instance, imagine that our first option offers a range of returns from a loss of $1 million to a gain of $1 million with an expected return of $0.5 million, while the second option offers a range of returns from a loss of $2 million to a gain of $20 million with an expected return of $0.25 million. The first option is more risk efficient, even though the second option offers a higher maximum positive return.

Analyzing and Assessing Risks

The section discusses how you can analyze and assess risks. The subsections below discuss the importance of risk analysis and assessment, distinguish risk analysis from risk assessment, describe risk analysis, describe risk assessment, and introduce the different available external sources of risk assessments.

Importance

Risk analysis and assessment are important because if we identify the various things that contribute to the risks then we could control each of these things and raise our security. As one author has advised businesses in response to terrorism, "risk assessment and risk analysis are not optional luxuries" (Suder, 2004, p. 223). Another author has advised project managers to be intellectually aggressive toward the analysis of security and risk.

> In addition, be on the alert for new threats. Unfortunately, however, new threats will not necessarily be obvious. You should always be "looking for trouble." Be skeptical, aggressive, and relentless in your quest to uncover potential problems. As the saying goes, if you don't manage risk, it will manage you! (Heerkens, 2002, p. 151)

Placing Risk Analysis and Risk Assessment

Over the last fifteen years, increased awareness of risks and increased attention to security have discredited prior norms of analysis and assessment and suggested a requirement for more attentive risk analysis and assessment.

Given the increased salience of security and risk over the last two decades, we might expect rapid maturation of their analysis and assessment, but an academic investigation of different methods for assessing health, natural, and crime risks found that they "share some commonalities, but also have many differences" (Kennedy, Marteache, & Gaziarifoglu, 2011, p. 45). Authorities are either surprisingly vague about analysis and assessment, use the terms interchangeably, use terms that are clearly incompatible with the practices, or discourage formal methods of assessment in favor of more intuitive assessment (see Pedagogy boxes 3.5 and 3.6 below). For instance, NATO does not define them at all, the Humanitarian Practice Network (2010, p. xviii) defines risk assessment and risk analysis interchangeably, and the ISO uses *risk analysis* illiterately to mean risk assessment, while using *risk identification* to mean risk analysis.

To resolve this incompatibility, we need to go back to semantic analysis. Semantic analysts have identified a class of verbs that, when used in connection with risk, "represent the actor's cognitive awareness: know the risk, understand the risk, appreciate the risk, calculate the risks" (Fillmore & Atkins, 1992, p. 86). This description is a neat prescription for a process of analyzing and assessing risks, where knowing (identifying) and understanding the risks are parts of risk analysis, while appreciating and calculating the risks are parts of risk assessment:

1. Analyze the risks:
   a. Identify the risks.
   b. Understand the risks by relating them to their sources (see Chapter 4).

2. Assess the risks:
   a. Appreciate the associated likelihood and return of each risk.
   b. Calculate the relative scale, level, or rank of the risks.

This prescription is more literal and simpler than most other prescriptions (see below).

Risk Analysis

Risk analysis helps to identify and understand the risks ahead of risk assessment (appreciating and calculating the risk), which in turn is a practical step toward choosing which negative risks should be controlled and which positive risks should be pursued and how to communicate our risk management.

Analyzing the risk involves identifying the risk and disaggregating the risk from its source to its potential returns. (Diagrammatic help for analyzing risk is shown in Figure 4.3.) A proper analysis allows us to assess the likelihood of each part of the chain; if we had not assessed the risks, we could hardly imagine either controlling all the actual risks or efficiently choosing the most urgent risks to control. Poor analysis and assessment of risk leads to mismanagement of risks by, for instance, justifying the allocation of resources to controls on misidentified sources of risk or on minor risks. Better analysis of risk would not prevent political perversities, but would counter poor analysis. Consider current counter-terrorism strategy, which involves terminating the causes of terrorism. Tracing the causes means careful analysis of the risk through its precursors to its sources. If the analysis is poor, government would end up terminating something that is not actually a source or cause of terrorism.

Pedagogy Box 3.5 Other Definitions and Practices of Risk Analysis

Unfortunately, most authorities do not use the term *risk analysis* literally. Almost all refer to risk assessment but few refer to risk analysis; their references to risk analysis tend to mean risk assessment, while they use *risk identification* to mean literal risk analysis. In some standards, most importantly the Australian/New Zealand and ISO standard (2009, p. 6) and its many partial adherents (such as Public Safety Canada, 2012, and AIRMIC, ALARM, and IRM, 2002), *risk analysis* is an explicit step in the recommended process for managing risks. The Australian/New Zealand standard, the ISO, and the Canadian government each promise that risk analysis "provides the basis for risk evaluation and decisions about risk treatment." They define risk analysis as the "process to comprehend the nature of risk and to determine the level of risk," but this is risk assessment. Their *risk identification* ("the process of finding, recognizing, and recording risks") sounds more like *risk analysis*. The Canadian government refers to *hazard identification* as "identifying, characterizing, and validating hazards," which again sounds like analysis, and describes "identification" as one part of "assessment" (Public Safety Canada, 2012, p. 49). Some project managers refer to *risk identification* when they clearly mean *risk analysis*—they properly schedule it before *risk assessment*, but add *risk analysis* as a third step, ranking risks by our "concern" about them (Heerkens, 2002, p. 143).

Similarly, both the British Treasury and the Ministry of Defense have defined *risk analysis* as "the process by which risks are measured and prioritized," but this is another definition that sounds more like risk assessment. The British Civil Contingencies Secretariat ignores risk analysis and provides a more operational definition of assessment, where analysis is probably captured under "identifying" risks.

Risk Assessment

According to the semantic analysis above, all a risk assessment needs to do, after a risk analysis, is

a. Appreciate the associated likelihood and return of each risk

b. Calculate the relative scale, level, or rank of the risks

Risk assessment can be informal, subconscious, and routine. Some authors have pleaded for more insightful understanding rather than conventional wisdom or generalizable models. Molak writes, "The thought process that goes into evaluating a particular hazard is more important than the application of some sophisticated mathematical technique or formula, which often may be based on erroneous assumptions or models of the world" (1997, p. 8). According to Bracken, Bremmer, and Gordon, "Risk management is about insight, not numbers. It isn't the predictions that matter most but the understanding and discovery of the dynamics of the problems" (2008, p. 6).

Risk assessment is not just a formal step in a prescribed process but is something we do all the time. When you choose to walk across a street or enter a neighborhood, you have assessed the risks—however unconsciously or imperfectly. That process is often termed *dynamic risk assessment*. Although these skills include instinctive, automatic, and informal skills, they are subject to description and training.

Pedagogy Box 3.6 Other Definitions and Practices of Risk Assessment

United Nations

"Risk assessment is . . . a methodology to determine the nature and extent of risk by analyzing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods, and the environment on which they depend" (UN ISDR, 2009, p. 11).

United States

"Risk assessment means a process or method for evaluating risk associated with a specific hazard and defined in terms of probability and frequency of occurrence, magnitude and severity, exposure, and consequences" (FEMA, 1997, p. xxv). For the GAO (2005, p. 110), risk assessment is "the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability, and consequences. A risk assessment may include scenarios in which two or more risks interact to create a greater or lesser impact. A risk assessment provides the basis for the rank ordering of risks and for establishing priorities for applying countermeasures." For DOD (2010, p. 269), risk assessment is "the identification and assessment of hazards."

Australian/New Zealand (2009) and ISO (2009a)

The Australian/New Zealand and ISO's definition of risk assessment ("the overall process of risk identification, risk analysis, and risk evaluation") is actually an operational definition of the process of assessing risks through three steps (which are also the second to fourth steps within a 7-step process of risk management: see Chapter 8):

1. Risk identification ("the process of finding, recognizing, and recording risks")
2. Risk analysis ("a process to comprehend the nature of a risk and to determine its level")
3. Risk evaluation ("the process of comparing the results of risk analysis with risk criteria to determine whether a risk and/international relations its magnitude is acceptable or tolerable")

Canadian

The Canadian government accepts the ISO's definition and process of risk management, but from October 2009 to October 2011 the Canadian government, with advice from the U.S., British, and Dutch governments, started the development of a federal method (All Hazards Risk Assessment process; AHRA), based on the first steps of the ISO process:

1. Setting the context: "a comprehensive understanding of the strategic and operating context of an organization," using its plans, environmental/situational assessments, and intelligence
   a. to "identify risk themes, defined as activities or phenomena of a particular interest to an institution"; and
   b. to produce "analysis" of future hazards and threats within the risk themes.
2. Risk identification: "the process of finding, recognizing, and recording risks," producing
   a. "a list of identified top priority threats and hazards (or risks)" by institution; and
   b. scenarios for each potential event.
3. Risk analysis: "to understand the nature and level of each risk in terms of its likelihood and impact."
4. Risk evaluation: "the process of comparing the results of risk analysis with risk criteria to determine whether a risk and/or its magnitude is/are acceptable or tolerable" (Public Safety Canada and Defence Research & Development Canada, February 2013).

(The published AHRA actually described the first 5 steps of the ISO's 7-step risk management process, but the fifth is the treatment or control of the risks and is clearly not part of risk assessment.)

British

The glossaries issued by the Treasury and MOD each defined risk assessment as "the overall process of risk analysis and risk evaluation," where *risk analysis* is "the process by which risks are measured

(Continued)

(Continued)

and prioritized" and risk evaluation is "the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels[,] or other criteria." Each department subsequently developed *risk assessment* as, respectively, "the evaluation of risk with regard to the impact if the risk is realized and the likelihood of the risk being realized" (Treasury, 2004, p. 49) or the "overall process of identifying, analyzing[,] and evaluating risks to the organization. The assessment should also look at ways of reducing risks and their potential impacts" (MOD, November 2011).

The Civil Contingencies Secretariat defined risk assessment as "a structured and auditable process of identifying potentially significant events, assessing their likelihood and impacts, and then combining these to provide an overall assessment of risk, as a basis for further decisions and action" (Cabinet Office, February 2013).

Humanitarian Practice Network

Risk assessment (used interchangeably with risk analysis) is "an attempt to consider risk more systematically in terms of the threats in the environment, particular vulnerabilities and security measures to reduce the threat or reduce your vulnerability" (Humanitarian Practice Network, 2010, p. xviii).

IRGC

The International Risk Governance Council's *risk governance framework* refers to both "analysis" and "understanding" but does not specify these steps. Its separate process of managing risk starts with a step known as *risk preassessment*—"early warning and 'framing' the risk in order to provide a structured definition of the problem and how it may be handled. Pre-assessment clarifies the various perspectives on a risk, defines the issue to be looked at, and forms the baseline for how a risk is assessed and managed." The "main questions" that the assessor should ask are listed as follows:

- What are the risks and opportunities we are addressing?
- What are the various dimensions of the risk?
- How do we define the limits for our evaluations?
- Do we have indications that there is already a problem? Is there a need to act?
- Who are the stakeholders? How do their views affect the definition and framing of the problem?
- What are the established scientific/analytical tools and methods that can be used to assess the risks?
- What are the current legal/regulatory systems and how do they potentially affect the problem?
- What is the organizational capability of the relevant governments, international organizations, businesses and people involved? (IRGC, 2008, pp. 8–9)

The second step of the IRGC's 5-step process of managing risk is *risk appraisal*, which starts with "a scientific risk assessment—a conventional assessment of the risk's factual, physical, and measurable

characteristics including the probability of it happening." The main questions that the assessor should ask are below:

- What are the potential damages or adverse effects?
- What is the probability of occurrence?
- How ubiquitous could the damage be? How persistent? Could it be reversed?
- How clearly can cause-effect relationships be established?
- What scientific, technical, and analytical approaches, knowledge, and expertise should be used to better assess these impacts?
- What are the primary and secondary benefits, opportunities, and potential adverse effects? (IRGC, 2008, p. 10)

Unofficial

Risk assessment is "the process of gauging the most likely outcome(s) of a set of events, situations[,] or options and the significant consequences of those outcomes" (Waring & Glendon, 1998, p. 21), "the combination of risk identification and risk quantification. The primary output of a risk assessment is a list of specific potential problems or threats" (Heerkens, 2002, p. 143), or "a consideration of the probabilities of particular outcomes, both positive and negative" (Kennedy & Van Brunschot, 2009, p. 4).

Crime Risk Assessment

Criminologists have prescribed the following questions for assessing risks:

- What type of threat or hazard are we facing?
- What types of data are needed?
- What are the sources of information available?
- What is the probability that the event would occur?
- How vulnerable are we?
- How exposed are we?
- How does information flow from the local to a higher level? (Kennedy, Marteache, & Gaziarifoglu, 2011, p. 34)

Dynamic Risk Assessment in Britain

In 1974, the British Parliament passed the Health and Safety at Work Act, which established the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE) as responsible for the regulation of almost all the risks to health and safety arising from work. After a surge in deaths of firefighters in the late 1980s and early 1990s, the HSE served several improvement notices on the firefighting service, amounting to an order for better risk assessment. The Home Office (1997) recommended a

(Continued)

(Continued)

focus on the safety of personnel. The Fire Service Inspectorate (1998) agreed and ordered firefighters to perform a risk assessment before all deployments; the Inspectorate suggested that standard operating procedures could be developed for predictable scenarios—what became known as a "Dynamic Risk Assessment." The Civil Contingencies Secretariat defines "dynamic risk assessment" as a "continuing assessment appraisal, made during an incident or emergency, of the hazards involved in, and the impact of, the response" (Cabinet Office, February 2013).

Acknowledging the dynamic relationship between the emergency and firefighter, the Fire Service Inspectorate (1998) formalized a simple process:

1. Evaluate the situation, tasks, and persons at risk;
2. Select systems of work;
3. Assess the chosen system of work;
4. Assess whether the risks are proportional to the benefits:
   a. If yes, proceed with tasks.
   b. If no, evaluate additional control measures and return to step.

Some British police forces adopted the same model, particularly after the HSE prosecuted the Metropolitan Police for breaches of health and safety. However, increasingly police complained that Dynamic Risk Assessment was impractical, while some blamed health and safety rules for their reluctance to take risks in order to protect the public (such as when community police officers watched a civilian drown while they awaited rescue equipment). The HSE (2005) subsequently "recognized that the nature of policing necessitates police officers to respond to the demands of unpredictable and rapidly changing situations and reliance solely on systematic risk assessment and set procedures is unrealistic."

Sources of Risk Assessments

This section introduces the main available external sources of risk assessments: subject matter experts; structured judgments; and systematic forecasts.

Subject Matter Experts

External experts are useful for checking for external agreement with our internal analysis and assessment or for sourcing more expert assessments than we could source internally. Unfortunately, most risk assessments rely solely on surveys of other people, due to insufficient time, capacity, or (frankly) motivation for proper analysis and assessment, and the expertise of these respondents is often less than claimed.

The main problem with any survey is that objective experts are rarer than most people realize. Generally, procurers and surveyors report that they have surveyed *experts* or *subject-matter experts*,

but do not measure or report expertise. For Public Safety Canada (2012, p. 90), which prescribes surveys of experts as complementary to objective evidence, a *subject-matter expert* is "a person who provides expertise in a specific scientific or technological area or on a particular aspect of a response."

Selection of experts involves choices: the more respondents, the more diversity of opinion, but adding more respondents also suggests wider recruiting of inferior experts. Our statistical confidence in the average response increases as we survey more people, although surveying more nonexperts or biased experts would not help.

Subject-matter expertise can suggest disengagement from wider knowledge. Probably everybody is subject to biases, and consumers prefer agreeable respondents. Even experts are subject to these biases, as well as political and commercial incentives.

For commercial, political, and personal reasons, many supposed experts are just the cheapest or most available or friendliest to the procurer. At the highest levels of government, often assessments of risks are made by informal discussions between decision makers and their closest friends and advisers, contrary to rigorous official assessments. Politicians often are uncomfortable accepting influence without political rewards or with methods that they do not understand. This dysfunction partly explains the George W. Bush administration's genuine confidence in its assessments in 2003 of the threats from the regime of Saddam Hussein and the opportunities from invading Iraq.

Political and commercial incentives help to explain the sustainment of poorly accredited academic experts or think tanks. In recent years, public confidence in experts of many types has been upset by shocks such as financial crises and terrorist attacks, suggesting we should lower our expectations or be more diligent in choosing our experts. For instance, in tests, most political experts performed little better than random when forecasting events five years into the future. Confident experts with deep, narrow knowledge ("hedgehogs" in Isaiah Berlin's typology of intellectuals) were less accurate than those with wide and flexible knowledge ("foxes"), although even foxes were not usefully accurate in forecasting events years into the future (Tetlock, 2006). Political scientists have a poor reputation for forecasting, perhaps because the phenomena are difficult to measure, they rely on small populations of data, they reach for invalid correlates, or they rely on unreliable judgments (unreliability may be inherent to political science if only because the subjects are politicized). Consequently, political scientists are highly polarized between different methods. While conscientious scientists attempt to integrate methods in order to maximize the best and minimize the worst, many political scientists form isolated niches (McNabb, 2010, pp. 15–28). Methods, data, and judgments are worst in the important fields of international security, war studies, and peace studies. Similarly, economists have received deserved criticism for their poor awareness of financial and economic instability in recent years.

All this illustrates the obvious principle that the risk assessor should be diligent when choosing experts. This is not to say that we should doubt all experts but that we should be more discriminating than is typical. We should carefully select the minority of all experts, even at the best institutions, who are objective, evidence-based, practical interdisciplinary thinkers.

Structured Judgments

We can structure the survey in more functional ways, as described in subsections below: Delphi survey; ordinal ranking; and plots of likelihood and returns.

Delphi Survey

The survey itself can be structured in more reliable ways. The least reliable surveys are informal discussions, particularly those between a small number of people under the leadership of one person, such as those commonly known as focus groups. Informal discussions tend to be misled by those most powerful in the perceptions of group members and by mutually reactionary, extreme positions.

Delphi surveys encourage respondents away from narrow subjectivity by asking them to reforecast a few times, each time after a revelation of the previous round's forecasts (traditionally only the median and interquartile range are revealed, thereby ignoring outliers). Interpersonal influences are eliminated by keeping each respondent anonymous to any other. This method helps respondents to consider wider empirical knowledge while discounting extreme judgments and to converge on a more realistic forecast. It has been criticized for being nontheoretical and tending toward an artificial consensus, so my own Delphi surveys have allowed respondents to submit a written justification with their forecasts that would be released to all respondents before the next forecast.

Ordinal Ranking

The respondent's task can be made easier by asking the respondent to rank the risk on an ordinal scale, rather than to assess the risk abstractly. The Canadian government refers to *risk prioritization* as "the ranking of risks in terms of their combined likelihood and impact estimates" (Public Safety Canada, 2012, p. 84). Essentially a risk ranking is a judgment of one risk's scale relative to another. Fewer ranks or levels (points on an ordinal scale) are easier for the respondent to understand and to design with mutually exclusive coding rules for each level. Three-point or 5-point scales are typical because they have clear middle, top, and bottom levels. More levels would give a false sense of increased granularity as the boundaries between levels become fuzzy.

Plotting Likelihood and Returns

A scheme for surveying more thoughtful assessments of risk would ask respondents to plot different types of risk in a single matrix by risk's two unambiguous multiples (likelihood and returns) (see Figure 3.3).

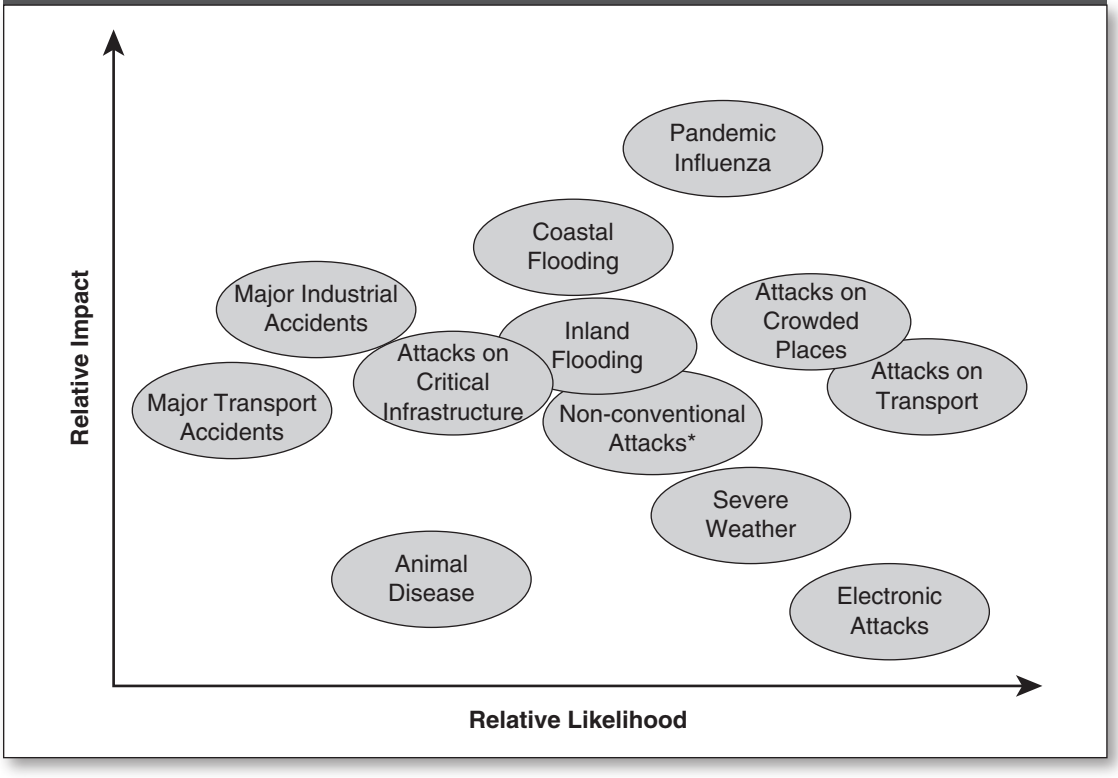
Indeed, the World Economic Forum (2013, p. 45) gives respondents a list of risks and asks them to rate both the likelihood and the impact (each on a 5-point scale). The World Economic Forum is able to calculate the risks for itself as a product of likelihood and impact. In its report, it presents the average responses for each risk's likelihood and impact on bar charts and as plots on a two-dimensional graph similar to that shown in Figure 3.3.

Naturally, given the opportunity, an even more accurate assessment would involve asking experts on the likelihoods (see Chapter 6) and other experts on the returns (see Chapter 7), from which we could calculate the risk.

Systematic Forecasts

In the 1990s, governments and supranational institutions and thence think tanks took more interest in producing their own forecasts of future trends and events. Initially, they consulted internal staff or external "futurists" and others whose opinions tended to be highly parochial. In search of more control, some have systematized forecasts that they might release publicly. These forecasts are based largely on expert judgments, but are distinguished by some attempt to combine theoretical or empirical review, however imperfectly.

Figure 3.3 A Risk Plot: Different Scenarios Plotted by Impact and Likelihood



SOURCE: U.K. Cabinet Office, August 2008.

For instance, since 1997 the U.S. National Intelligence Council has published occasional reports (around every four years) on *global trends* with long horizons (inconsistent horizons of 13 to 18 years). In 1998, the British government's Strategic Defense Review recommended similar forecasts, so the Ministry of Defense established what is now the Development, Concepts and Doctrine Center, which since 2001 has published occasional reports on *global strategic trends* with a time horizon of 30 years (for the MOD, January 2010, p. 6, a trend is "a discernible pattern of change"). Annually since 2004, the British executive has produced a *National Risk Assessment* with a time horizon of five years—the published versions (since 2008) are known as "National Risk Registers of Civil Emergencies." In 2010, it produced a *National Security Risk Assessment* by asking experts to identify risks with time horizons of 5 and 20 years—this remains classified, but is summarized in the National Security Strategy (Cabinet Office, 2010, p. 29, 37; Cabinet Office, July 2013, pp. 2–4). Since 2011, the Canadian government has prescribed annual forecasts of "plausible" risks within the next five years, *short-term*, and 5 to 25 years in the future, *emerging* (Public Safety Canada and Defense Research and Development Canada, February 2013, p. 11). Since the start of 2006, the World Economic Forum has published annual forecasts of *global risks* (not just economic risks) with a horizon of 10 years.

Some think tanks are involved in official forecasts as contributors or respondents or produce independent forecasts with mostly one-year horizons. For instance, since 2008 the Strategic Foresight

Initiative at the Atlantic Council has been working with the U.S. National Intelligence Council on *global trends*. Since March 2009, around every two months, the Center for Preventive Action at the Council on Foreign Relations has organized discussions on plausible short- to medium-term contingencies that could seriously threaten U.S. interests; since December 2011, annually, it has published forecasts with a time horizon through the following calendar year. Toward the end of 2012, the Carnegie Endowment for International Peace published its estimates of the ten greatest international "challenges and opportunities for the [U.S.] President in 2013."

Official estimates are not necessarily useful outside of government: officials prefer longer term planning that is beyond the needs of most private actors; they also use intelligence that falls short of evidence; the typical published forecast is based on mostly informal discussions with experts. Some experts and forecasts refer to frequency or trend analysis or theory, but too many do not justify their judgments. Both the U.S. and British governments admit to consulting officials, journalists, academics, commentators, and business persons, but otherwise have not described their processes for selecting experts or surveying them. The Canadian government has been more transparent:

> Generally, the further into the future forecasts go, the more data deprived we are. To compensate for the lack of data, foresight practitioners and/or futurists resort to looking at trends, indicators etc. and use various techniques: Technology Mapping; Technology Road-Mapping; Expert Technical Panels, etc. These are alternate techniques that attempt to compensate for the uncertainty of the future and most often alternate futures will be explored. Federal risk experts can get emerging and future insights and trend indicators through community of practice networks such as the Policy Horizons Canada (http://www.horizons.gc.ca) environmental scanning practice group. (Public Safety Canada and Defense Research and Development Canada, February 2013, p. 11)

The World Economic Forum's survey is the most transparent: it asks respondents to assess, on a scale from 1 to 5, the likelihood of each of 50 possible events occurring within the next ten years. Additionally, it asked respondents to pick the most important risk (center of gravity) within each of the 5 categories of risk. It also asked respondents to link pairs of related risks (at least 3, no more than 10 such pairs). It used the results to identify the most important clusters of related risks, and then it explored these clusters through direct consultation with experts and focus groups.

SUMMARY

This chapter has:

- defined risk,
- explained how qualitatively to describe a risk more precisely and usefully,
- shown you different ways to categorize risks, including by
  - negative and positive risks,
  - pure and speculative risks,
  - standard and non-standard risks,

  - organizational categories,
  - levels, and
  - higher functional types,
- given you alternative ways to calculate risk and its parameters, including:
  - risk, by different combinations of probability, return, hazard, vulnerability, and exposure,
  - predictable return,
  - expected return,
  - PERT expected return,
  - range of contingencies,
  - range of returns, and
  - risk efficiency,
- shown how to analyze risks,
- shown how to assess risks, and
- introduced available external sources of risk assessments.

QUESTIONS AND EXERCISES

1. Identify what is good or bad in the different definitions of risk (collected earlier in this chapter).
2. Calculate the expected returns in each of the following scenarios:
   a. We forecast a 50% probability that we would inherit $1 million.
   b. The probability of a shuttle failure with the loss of all six passengers and crew is 1%.
   c. The probability of terrorist destruction of site *S* (value: $100 million) is 20%.
   d. If the project fails, we would lose our investment of $1 million. The probability of failure is 10%.
   e. One percent of our products will fail, causing harm to the user with a liability of $10,000 per failure. We have sold 100,000 products.
3. What are the expected returns and range of returns in each of the scenarios below?
   a. A military coalition has offered to arm an external group if the group would ally with the coalition. Survey respondents forecast a 60% probability that the group would stay loyal to the coalition. The group currently consists of 1,000 unarmed people.
   b. The coalition must choose between two alternative acquisitions: an off-road vehicle that could avoid all roads and therefore all insurgent attacks on road traffic, which account for 40% of coalition casualties; or an armored vehicle that would protect all occupants from all insurgent attacks. However, experts estimate a 20% probability that the insurgents would acquire a weapon to which the armored vehicle would be as vulnerable as would any other vehicle.
   c. The police claim that an investment of $1 million would double their crime prevention rate. Another authority claims that an investment of $1 million in improvements to electricity generation would enable street lights at night, which would triple crime prevention. Experts estimate the probability of success as 60% in the case of the police project, 50% in the case of the electricity project.

4. Consider your answers to question 3. In each scenario, how could you describe one option or alternative as risk efficient?
5. Describe the risks in the scenarios in questions 2 and 3.
6. Categorize the risks in the scenarios in questions 2 and 3.
7. What is the difference between the normal formula of expected return and the PERT expected return?
8. What are the advantages and disadvantages of asking experts to assess risk's level or rank?