CHAPTER

10

Controls and Strategies

This chapter explains controls and strategies—the actual things under our control that affect our risks. The two main sections of this chapter define control and explain when and why controls are applied to risks and define strategy and explain when and why to choose between available strategies in response to risk.

Control

This section defines control, explains how to separate tolerable from intolerable risks that you should control, explains the trade-off between intolerability and practicality, explains why sometimes even tolerable risks are controlled, and explains why different stakeholders can have different levels of tolerance and control at the same time.

Defining Control

A control is anything that was intended to or effectively does reduce a risk (see Table 10.1 for official definitions). If a control reduces a risk, the precontrol state of the risk is usually known as the *inherent risk*, while the postcontrol state is usually known as the *residual risk*.

The control is not necessarily an absolute solution to the risk. It may reduce a risk to a still intolerable level or to an only temporarily tolerable level. Consequently, good risk management processes prescribe monitoring the risk, even after control.

Establishing Tolerable Risks

Most authorities and standards prescribe the establishment of a risk tolerability threshold, below which a negative risk is tolerable and above which it should be controlled.

Since stakeholders, managers, and risks are diverse, authorities and standards normally leave users to find their own tolerability threshold and do not prescribe where the threshold should fall, although project managers have been advised to tolerate risks that score less than 30–40 on a 100-point scale (Meerkens, 2002, p. 148). In international security, some writers imply that strategists should not tolerate

Table 10.1 Official Definitions Relating to Risk Controls and Strategies

	Australian and New Zealand Joint Technical Committee (2009); International Organization for Standardization (2009a)	**U.K. Treasury (2004)**	**U.K. MOD**	**U.K. Civil Contingencies Secretariat (U.K. Cabinet Office, 2013)**	**Public Safety Canada (2012)**
Control	"a measure that is modifying risk," including a "process, policy, device, practice, or other actions which modify risk."	"any action . . . taken to manage risk"; an internal control is "any action, originating within the organization, taken to manage risk" (p. 50).	"any action taken by management to enhance the likelihood that established objectives and goals will be achieved" (2009a); "The coordination of activity, through processes and structures that enable a commander to manage risk and deliver intent" (2009b, p. 234).	A risk control is "measures to reduce the likelihood of an emergency occurring from a given risk, and/or implement measures to mitigate the impacts of that emergency should arise." A control is "the application of authority, combined with the capability to manage resources, in order to achieve defined objectives."	-
Treatment	"a process to modify risk"	-	-	"process of determining those risks that should be controlled (by reducing their likelihood and/or putting impact mitigation measures in place) and those that will be tolerated at their currently assessed level" (countermeasures are "precautionary actions to protect the public")	"the process of developing, selecting, and implementing risk control measures"

	Australian and New Zealand Joint Technical Committee (2009); International Organization for Standardization (2009a)	U.K. Treasury (2004)	U.K. MOD	U.K. Civil Contingencies Secretariat (U.K. Cabinet Office, 2013)	Public Safety Canada (2012)
Capability	-	-	-	"a demonstrable ability to respond to and recover from a particular threat or hazard"	"a combination of resources that provides the means to prevent, protect against, respond to, and recover from emergencies, disasters, and other types of incidents. In capability-based planning, a capability includes the following elements: planning, organization, equipment and systems, training, and exercises, evaluations, and corrective actions"
Strategy	effectively the same as risk treatment	"the overall organizational approach to risk management as defined by the Accounting Officer and/or Board" (p. 50)	Risk mitigation is "reduction of the exposure to, probability of, or loss from risk" (2011c).	"the level (above tactical level and operational level) at which policy, strategy and the overall response framework are established and managed"	("strategic emergency management plan") "an overarching plan that establishes a federal government institution's objectives, approach, and structure for protecting Canadians and Canada from threats and hazards in their areas of responsibility and sets out how the institution will assist with coordinated emergency management" (p. 90)

(Continued)

Table 10.1 (Continued)

	Australian and New Zealand Joint Technical Committee (2009); International Organization for Standardization (2009a)	U.K. Treasury (2004)	U.K. MOD	U.K. Civil Contingencies Secretariat (U.K. Cabinet Office, 2013)	Public Safety Canada (2012)
Inherent risk	-	"the exposure arising from a specific risk before any action has been taken to manage it" (p. 49)	"the risk found in the environment and in human activities that is part of existence" (2009a) (note: this conflates pure risks or natural risks)	-	-
Residual risk	"the risk remaining after risk treatment"	"the level of risk remaining after internal control has been exercised [and] the exposure in respect of that risk" (p. 9); "the exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective" (p. 49).	"the remaining level of risk after risk control measures have been implemented" (2009)	-	"risk that remains after implementing risk mitigation measures" (p. 80)

negative risks until their probabilities approach zero, given the high negative returns of strategic failure in international war:

> [A]ny strategic argument which seeks to direct and inform practice needs to satisfy certain conditions so that the desired end is, in fact, achieved by the means recommended and employed. The rationality of such arguments does not depend upon making out a plausible or acceptable case for the recommended action, but in showing that the result is either highly probable or certain. (Reynolds, 1989, p. 29)

Visually, identifying tolerable risks involves assessing the risks, assessing our tolerability level or threshold, and plotting the risks on a linear scale, where risks higher or lower than the threshold would be intolerable (see Figure 10.1).

However, individually tolerable risks could interact or vector together as a single *compound risk* that is intolerable. For instance, we could choose to assess criminals individually and find their associated risks tolerable, but if those criminals were to cooperate or to be analyzed as a homogenous group, then the risks associated with the group might become intolerable.

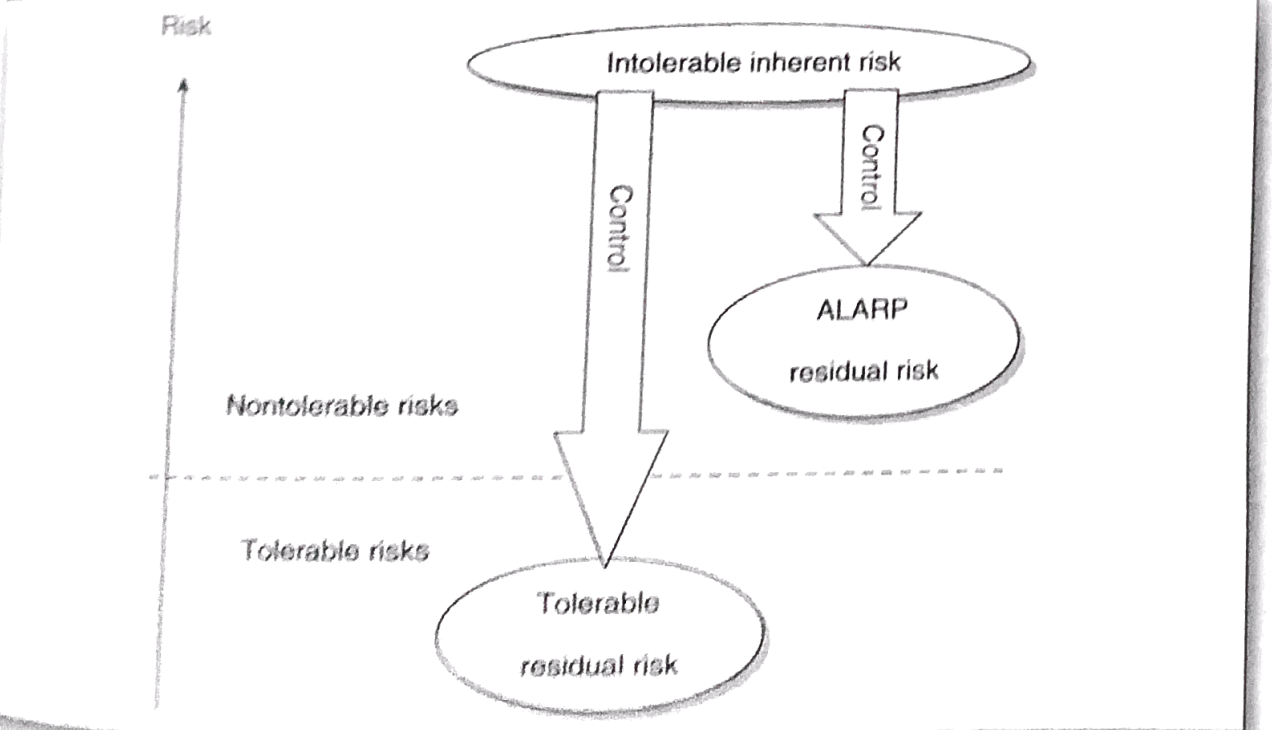
Pedagogy Box 10.1 Prescriptions for Establishing Tolerability

The Australian/New Zealand and ISO standards (International Organization for Standardization, 2009a, p. 8) prescribe in their risk management process a step termed *risk evaluation*—meaning "the process of comparing the result of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable." (The Canadian government too follows the definition and the process.)

The International Risk Governance Council (IRGC) (2008, p. 6) prescribed a step called *characterization and evaluation* (separating tolerable from intolerable risks).

The Humanitarian Practice Network (2010) describes the "threshold of acceptable risk" as "the point beyond which the risk is considered too high to continue operating; [it is] influenced by the probability that an incident will occur, and the seriousness of the impact if it occurs" (p. xix).

Figure 10.1 Conceptualizing Inherent and Residual Risks



Intolerability Versus Practicality

Ideally, we would seek to control intolerable risks until the residual risk is tolerable. However, sometimes the controls would be impractical or unjustifiably burdensome, in which case risk managers might accept a residual risk level that is higher than the tolerability level. If so, on practical grounds, they would effectively tolerate a level of risk that they would not tolerate otherwise. This level is described sometimes as the ALARP (as low as reasonably practical) level. Some authors talk of a constant "risk balance" or "security dynamic"—a balance between our tolerance of the risks, our resources available to control the risks, and our values (Van Brunschot & Kennedy, 2008, pp. 12–13).

Naturally, the ALARP level could be used unscrupulously to justify a multitude of sins, such as laziness or meanness, but ALARP levels are everywhere, even though most are unadmitted. For instance, law enforcement authorities ideally would like to eliminate crime, but they would need to track every activity of every person, which would be impractical, unethical, and stressful. In effect, some level of crime becomes "acceptable" (Kennedy & Van Brunschot, 2009, p. 4). Similarly, regulation of transport systems seeks to promote but not to guarantee safety; otherwise the transport systems would grind to a halt under the burden of inspections and reports.

Pedagogy Box 10.2 ALARP Food Risks

Since 1995, the Food and Drug Administration (FDA), which oversees the safety of most foods, medical devices, and medical drugs in the United States, has published a tolerability level for insect parts in food, even though surveys of food consumers show that most consumers, rhetorically at least, would not knowingly tolerate any insect parts in food. In effect, the FDA regards its "food defect action levels" (such as more than 75 insect parts per 50 grams of flour or more than 60 insect parts per 100 grams of chocolate) as ALARP levels: "The FDA set these action levels because it is economically impractical to grow, harvest, or process raw products that are totally free of non-hazardous, naturally-occurring, unavoidable defects" (U.S. FDA, 2005).

Tolerance of an ALARP level could introduce new risks, such as potential collapse of public confidence in the authority that tolerated the ALARP level before some associated public shock revealed such tolerance to the public. For instance, from 2004 to 2007, U.S. consumers were shocked by a series of revelations of meat from diseased livestock in the human food chain. Effectively, authorities had knowingly tolerated diseased meat in the food chain, while most consumers had been unaware. In 2009, new U.S. federal laws took effect that outlawed diseased meat from being passed for human consumption. In 2012, British consumers were shocked by revelations that meats routinely sold in supermarkets, fast food outlets, and restaurants as beef had been identified genetically as horse meat, mostly from continental European sources, causing a collapse in confidence in European-wide regulation of food labelling.

Controlled Tolerable Risks

Sometimes, scrupulous authorities assess a risk as tolerable but are forced to control it anyway by outside stakeholders, sometimes for unnecessary reasons. For instance, a natural risk manager might have assessed the chance of a hurricane as tolerably low and allocated most resources to control the much

higher chance of drought, but the public in an unaffected region could become alarmed by a hurricane in a neighboring region and demand observable defenses against hurricanes, even if neighboring risks were unrelated.

Pedagogy Box 10.3 Controlled Tolerable Food Risks

Consumers of food tend to be alarmed by harmless and even nutritious "defects" (such as insect parts) that they could see in their food, more than by harmful and nonnutritious defects (such as artificial pesticides and hormones and natural diseases) that they cannot see. Consequently, consumers demand food that has fewer observable defects than the FDA specifies, but this encourages food suppliers to use more pesticides in order to reduce insects—thereby increasing the risks associated with pesticides. This is a trend that the FDA discourages: "It is FDA's position that pesticides are not the alternative to preventing food defects. The use of chemical substances to control insects, rodents, and other natural contaminants has little, if any, impact on natural and unavoidable defects in foods" (U.S. FDA, 2005).

Incompatible Tolerability

Sometimes different stakeholders effectively work alongside each other with different tolerability levels. For instance, during recent multinational coalition operations in Afghanistan (since 2001), Iraq (since 2003), and other countries, soldiers from developed countries have been instructed not to travel without armed or armored protection, while indigenous personnel were issued inferior levels of protection, and some "third-party" nationals in the employ of civilian contractors were expected to work without any protection at all.

These incompatible tolerability levels reflect the different risk sensitivities within each national culture and organizational culture, and the different practical constraints on each actor's controls.

In some cases, incompatible sensitivities or controls may not matter to cooperative operations, but they could interfere with interoperability. For instance, in Afghanistan and Iraq, foreign personnel often were forbidden from entering high-risk areas that local personnel had been ordered to enter, while local personnel often demanded equipment of the same survivability as used by foreign troops. Similarly, local personnel often accused foreign personnel of deferring too readily to remote strike weapons, such as air-to-ground missiles launched from aircraft, that sometimes cause collateral civilian casualties, while foreign personnel often accuse local personnel of lacking care in the use of their portable firearms against civilians misidentified as enemies.

Strategies

This section defines risk management strategies, describes existing prescribed strategies, describes the 6 "T" strategies, and combined or balanced strategies.

Defining Strategy

A *risk management strategy* is any purposeful response to insecurity or risk; the strategy might be emergent or subconscious, but must aim to affect security or risk. The strategy is usefully distinguished

from the controls—the particular actions used to change a particular risk, such as a guard acquired as part of a protective strategy. (Many authorities on risk management have offered a set of recommended responses to risk or approaches to security that they usually term *treatments*, *approaches*, *responses*, or *strategies*. Unfortunately, many authorities use these terms interchangeably for strategy or control.)

Pedagogy Box 10.4 Other Definitions of Risk Management Strategies

Some risk management standards refer to *approaches* toward security or managed risks. Some private commentators use both terms (*strategy* and *approach*) (Van Brunschot & Kennedy, 2008, pp. 165–166). The Humanitarian Practice Network is unusual for talking about both *risk management strategies* and *security strategies*. It defines (2010) a *security strategy* as "the overarching philosophy, application of approaches, and use of resources that frame organization security management" (p. xviii). Business managers, grounded in marketing strategies and corporate strategies, are comfortable referring to any purposeful response as a risk management strategy (Branscomb & Auerswald, 2001, Chapter 4).

The ISO prescribes seven strategies but does not define strategy, although it seems to regard "risk treatment" ("a process to modify risk") as inclusive of strategy. The Canadian government follows ISO, with some reservations.

The British Standards Institution has largely followed the ISO, but the British government has not ordered departments to follow any common standard. The British Treasury (2004) defines a risk management strategy as "the overall organizational approach to risk management as defined by the Accounting Officer and/or Board" (p. 50). The British Ministry of Defense (2011c) has definitions of military strategy but none of risk management strategy, although it defines "risk mitigation" as "reduction of the exposure to, probability of, or loss from risk" (pp. 6–7).

Strategy is well defined in military contexts. For instance, the United States Department of Defense (DOD) dictionary (2012b) defines it as "a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objective." Nevertheless, military strategists traditionally have not mentioned risk directly, although they routinely refer to security. In the last two decades, many governments have introduced risk management as a supplement or alternative to traditional security and defense strategies. For instance, in 2001, the DOD published a Quadrennial Defense Review with a declaration that "managing risks is a central element of the defense strategy" (p. 57). Some academics have encouraged or noticed the shift: "Strategy is no longer a question of defeating concrete threats in order to achieve perfect security; it has instead become a way of managing risks" (Rasmussen, 2006, p. 11). Nevertheless, the DOD has no definition of risk management strategy or security strategy, although the U.S. Defense Acquisition University prescribes strategies for managing acquisition projects and other departments routinely list strategies for managing security in certain domains, such as counter-terrorism.

Existing Strategies

The Australian/New Zealand standard (since 1995) and ISO (International Organization for Standardization, 2009a, pp. 9–10) offer a set of seven strategies that has proved most appealing, but not perfect, partly because some of the seven strategies overlap (see Table 10.2). For instance, *retaining* the risk is written to include both negative and positive risks, which overlaps with *pursuing* a positive risk. Similarly, *changing the consequences* involves mostly controlling the consequences of a potential event, but, as written, includes also the retention of financial reserves, which would not directly control the consequences at all and is better placed as a substrategy of *retaining* the risk. The ISO standard is followed by the Canadian government, among others, but the Canadian government is dissatisfied with the ISO strategies and recently (2013) published a cursory development, which remains ongoing.

Trade associations tend to follow the ISO, otherwise prescriptions tend to be contradictory. For instance, the Humanitarian Practice Network (2010, pp. 28, 50, 55) identified three risk management strategies, three overlapping security strategies, and two variations of the risk management strategies, for eight overlapping approaches that actually shake out as substrategies to three of the seven strategies offered by the ISO (see Table 10.2).

Similarly, two criminologists have categorized just three strategies/approaches (*prepare and make ready, respond, recover and prevent*), within which they conflated many competing optional approaches. For instance, within "*preparedness and readiness*" they effectively conflated transferring risks, avoiding risks, defending against threats, and preventing negative events—each of which is different to preparing or making ready for an event. The only natural separation between "*preparing*" and "*responding*" is chronological (you should prepare to respond to an attack in case it happens; it if happens you should respond). Finally, "*recover and prevent*" included an optional approach ("*prevent*") that naturally belonged in the first stage but was mentioned in all three stages. Fairly, they admitted "some degree of slippage with respect to the notions of preparedness and prevention" (Van Brunschot & Kennedy, 2008, p. 184).

Official authorities have tended to focus their risk management strategies on project risks, such as the U.S. Defense Acquisition University's four uncontentious strategies (*avoid*; *control*; *accept*; *transfer*). Other official authorities are focused on security strategies such as *preparedness*, *resilience*, *continuity*, and any other of a total of nine synonyms that largely mean *controlling the negative consequences* (see below) of a potential event—which is only one of the seven strategies offered by the ISO.

The Institute of Chartered Accountants of England and Wales (Turnbull, 1999) suggested four effective strategies (see Table 10.2), which were most influential on British government. Subsequently, the Treasury prescribed (and most other departments adopted) five risk management strategies known as the "five Ts" (U.K. Ministry of Defense [MOD], 2011c, pp. 6–7). The British government's project management standard (PRINCE2) follows similar strategies but knows them by other words. These five Ts also contain impractical overlaps and separations. For instance, *treating* and *terminating* risks involve essentially the same activities—terminating the risk would be the ultimate effect of perfectly treating the risk.

The Six "T" Strategies

Clearly, the current offerings are dissatisfactory. The authoritative prescriptions do not agree on even the number of strategies. Some of their strategies align neatly, but some contain substrategies that are placed under different strategies by different authorities. Some strategies are separated but are really

variations of each other. Some offerings are very narrow. Most surprising, no authority admits *diversification*, a routine strategy in many domains, especially finance. Similarly, no authority explicitly admits the possibility of *turning* a risk from negative to positive.

Semantic analysts have identified in general use a class of verbs (such as *avoid*, *reduce*, *minimize*, and *eliminate*) representing human attempts to change risk. They identified another class of verbs (such as *incur*, *entail*, *offer*, and *involve*) representing the object's situational or voluntary relationship with the risk. A final class of verbs (such as *assume*, *face*, *shoulder*, and *bear*) represents a victim's relationship with the risk (Fillmore & Atkins, 1992, pp. 86–87). These words suggest a minimum of three strategies: treat—which sometimes extends to terminate, take, and tolerate.

Combining these observations, I offer six "Ts" (tolerate, treat—which sometimes extends to terminate, turn, take, transfer, and thin the risk), rationalizing the competing prescriptions, with a more practical taxonomy and due emphasis on strategies that are usually conflated or forgotten. The sections below explain these six strategies.

Tolerate

The strategy of toleration might be known elsewhere as one of *assumption* or *acceptance*, but these terms are often confused with *taking* the risk, which implies pursuit of a positive risk (see below).

Tolerating the risk would eschew any control on the risk (although this should not imply forgetting about the risk). We could choose to tolerate the risk, even if it were higher than our threshold for intolerability, if we were to decide that the benefit of controlling the risk would not be justified by the cost of controlling the risk.

Tolerating the risk means eschewing any additional control but is not the same as eschewing any management of the risk. Tolerating the risk should imply either watching or retaining the risk, either of which might be treated elsewhere as a separate strategy but is properly treated as an option within the strategy of tolerating the risk, as described in subsections below.

Watch

While we tolerate a risk, we should watch the risk in case the risk changes. Such a watch implies, in practice, periodic reassessment of the risk level. If the risk were to fall, we would feel more justified in tolerating the risk. If the risk were to rise, we should consider a new strategy (probably *treat* the risk).

Retain

A strategy of "retaining the risk" implies that the owner of the risk is holding or building reserves against the potential negative returns. For instance, if we feared a poor harvest and could not find or afford an insurer or donor who would promise to supply any shortfall in our supply of food, we should build reserves of food. Similarly, if we invest in a new commercial venture but decide that insurance against financial failure would be too costly, we should hold or build financial reserves that could pay for the costs of failure. Retaining the risk is the main alternative to *transferring* the risk to some outside actor (such as an insurer or partner).

Treat (and Sometimes Terminate)

If we were to decide that we could not tolerate a risk, we should treat the risk. Treating the risk means the application of some control to a risk in order to reduce the risk, ideally to a tolerable level, possibly until

we terminate the risk. A strategy of termination includes *prevention* of things like the threat's intent or capabilities or our exposure to threats (see below). Prevention might be defined elsewhere as treating the risk (see, for instance, Heerkens, 2002, p. 150), but prevention implies termination of the risk.

Opportunities to terminate the risk are often forgotten in the haste to prevent the risk growing. Termination is attractive because we could eliminate the risk entirely. This outcome would comply with the adage "prevention is better than cure" and with the commercial manager's desire for the most efficient strategy, but not if the burden of treatment becomes prohibitive. The burden may persuade us to accept a technically intolerable residual risk, but one as low as reasonably practical (ALARP).

As described in the four subsections below, treating or terminating the risk can be achieved in four main ways: reducing our exposure to the source; reducing the source's threatening intent; reducing the source's threatening capabilities; or reducing the potential negative effects of an event. For instance, we could park our car outside of the area where car thieves operate (reducing exposure), equip the car with an alarm that discourages attempts to break into the car (controlling the threat's intent), acquire windows that resist break-ins (controlling the threat's capabilities), or use our least valuable car (controlling the negative effects).

Pedagogy Box 10.5 Official Definitions of Prevention

The UN Office for International Strategy for Disaster Reduction (ISDR) (2009) defined *prevention* in only this sense (as "the outright avoidance of adverse impacts of hazards and related disasters") (p. 9). Similarly, the UN Department of Humanitarian Affairs (DHA) (1992) defined prevention as "encompassing activities designed to provide permanent protection from disasters. It includes engineering and other physical protective measures, and also legislative measures controlling land use and urban planning."

U.S. Department of Homeland Security (DHS) (2009) defines prevention as "actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects" (p. 110).

The Canadian government defines prevention as "actions taken to eliminate the impact of disasters in order to protect lives, property, and the environment, and to avoid economic disruption." A *preventive control* is "a plan or process that enabled an organization to avert the occurrence or mitigate the impact of a disruption, crisis, or emergency" (Public Safety Canada, 2012, p. 73).

Reduce Exposure

Reducing our exposure to the sources of risk would reduce their opportunities to harm us. Reducing exposure involves any of four sub-strategies: deferring our exposure to the sources; avoiding exposure; withdrawing from exposure; or containing the hazard.

Defer

We could choose to defer our acceptance of the risk. The word *defer* implies that we are not currently exposed to the risk but that we reserve the option to undertake the risk at a later point. For instance, we could decide that an investment is too negatively risky this year, so we could defer a review of the decision to next year in case the risk might have changed to a state that is worth pursuing.

Avoid

The word *avoid* implies that we want to do something without exposing ourselves to a negative risk. For instance, we could decide that we should intervene in a lawless area in order to terminate the threats at their geographical source—this is a strategy of termination. An alternative strategy is to intervene in the area whenever the threats are not present, perhaps in order to build local capacity or provide humanitarian aid—this strategy is one of avoidance.

Pedagogy Box 10.6 Canadian Definition of Risk Avoidance

The Canadian government defines *risk avoidance* as "an informed decision to avert or to withdraw from an activity in order not to be exposed to a particular risk" (Public Safety Canada, 2012, p. 82).

Withdraw

A strategy of withdrawing from the risk implies that we are currently exposed to the risk, but we choose to stop our exposure to the risk. For instance, we could be operating in some city where the chance of political violence rises to an intolerable level, at which point one of our choices is to move somewhere else.

Contain

Containing the hazard could be achieved by preventing the hazard from reaching us, or preventing ourselves from coinciding with the hazard. For instance, if a flood were to reach us it would be a threat, but if we could construct some diversion or barrier the flood would not reach us. Similarly, a river that routinely floods a narrow valley could be dammed. Similarly, a criminal could be detained.

Sometimes, containment temporarily contains a hazard until it returns to its threatening state. Worse, containment could strengthen the hazard. For instance, detention of criminals is criticized for bringing criminals together where they can further radicalize and prepare each other for further crime, without providing opportunities for renunciation of crime or the take up of lawful employment. Indeed, more criminals return to crime after detention (this return is known as *recidivism*) than return to lawfulness.

Sometimes, an attempt to contain a hazard might reduce the frequency of minor events but not all events. For instance, a dam would terminate minor floods, but if flood waters could overflow the dam then we would have less frequent but more catastrophic floods.

Some strategies of containment have costs that are underassessed by the author of the strategy: often the domain, such as flood prevention, in which the risk manager is working, is imperfectly competitive with the domain, such as natural biodiversity, that suffers the costs of the measures. For instance, from the environmentalist's perspective, damming a valley is likely to damage its natural environment in ways that are not justified by the decreased chance of flooding in the town.

Reduce Intent

Since a threat necessarily must have intent and capability to harm us, we could keep a hazard in its hazardous state or return a threat to it hazardous state by terminating the source's threatening intent.

The three main substrategies are reduce the causes of the activation of such intent; deter intent; and reform intent.

Reduce the Causes of Activation

The causes of the threat include the activation of the hazard into a threat. Prevention of the causes would prevent the threat from arising from the hazard.

Prevention is particularly appropriate in domains such as preventable diseases: helping people to give up behaviors such as smoking is far cheaper than treating smokers for lung cancer; vaccinating against a pathogen is ultimately cheaper than treating the diseases caused by the pathogen. Similarly, prevention of climate change would be more effective and efficient (1% to 2% of global GDP until 2050) than treating the effects (5% to 10% of global GDP until 2050) (Swiss Re, 2013, p. 13). Similarly, preventing human hazards from acquiring the intent or capabilities to behave as terrorists is more efficient than defending every potential target from every potential threat.

Prevention is attractive in international relations, too, where the negative returns can be enormous. For instance, the British government has long advocated for more international cooperation in the assessment and control of potential conflicts.

> More effective international responses to reduce risks of instability—and thereby prevent crises—are possible. Prevention is much more humane and far less costly than crisis response . . . The underlying causes of conflict need to be tackled . . . In many cases, the suppression of violent crises has not addressed the dynamics of tension or political conflict, and thus has not reduced the risks of future armed conflict. (U.K. Prime Minister's Strategy Unit, 2005, pp. 4, 22)

However, proactive control of some causes of activation may activate other threats. The British government's high-minded advocacy in 2005 for more international cooperation in the assessment and control of international risks looked hypocritical after the largely bilateral U.S.-British invasion of Iraq in 2003, which stimulated an insurgency there and vengeful terrorism at home, such as when four British Muslims killed themselves and 52 others in suicide bombings on public transport in London, July 7, 2005, having recorded messages that blamed British foreign policy.

Pedagogy Box 10.7 Reducing the Causes and Sources of Disease

"Most scientific and health resources go toward treatment. However, understanding the risks to health is key to preventing disease and injuries. A particular disease or injury is often caused by more than one risk factor, which means that multiple interventions are available to target each of these risks. For example, the infectious agent Mycobacterium tuberculosis is the direct cause of tuberculosis; however, crowded housing and poor nutrition also increase the risk, which presents multiple paths for preventing the disease. In turn, most risk factors are associated with more than one disease, and targeting those factors can reduce multiple causes of disease. For example, reducing smoking will result in fewer deaths and less disease from lung cancer, heart disease, stroke, chronic respiratory disease, and other conditions. By quantifying the impact of risk factors on diseases, evidence-based choices can be made about the most effective interventions to improve global health" (World Health Organization, 2009, p. 1).

Deter

Deterring the threat means dissuading the hazard from becoming a threat. For instance, most national efforts to build military capacity are explicitly or effectively justified as deterrent of potential aggressors. So long as potential aggressors are deterred, they remain in a hazardous state and do not reach a threatening state.

Deterring the threats would reduce the frequency of negative events. For instance, at physical sites, security managers often seek to draw attention to their alarms, cameras, and guards in order to increase the chances that the potential threat would observe these measures and be deterred. However, encouraging observation of our defensive measures could help the potential threat to discover vulnerabilities, such as fake alarms, misdirected cameras, and inattentive guards. For the purpose of deterrence, ideally, defensive vigilance and preparedness should be observable without being counter-able.

We could seek to detain or kill or otherwise punish people for having the intent to harm. This action may reduce the threat's capabilities directly and deter others from becoming similar threats, although sometimes punishment (particularly in counter-terrorism) becomes vengeful rather than purposefully deterrent.

Pedagogy Box 10.8 Another Definition of Deterrence

The Humanitarian Practice Network (2010, pp. xvi, 55) recognizes a "deterrence approach" as a "security strategy" or "an approach to security that attempts to deter a threat by posing a counter-threat, in its most extreme form through the use of armed protection."

Reform

We could also seek to reform or turn around someone's harmful intent. Postdetention programs, such as supervision by parole officers and suspended sentences, seek to reduce recidivism mainly by containment and deterrence, but some programs include mandatory participation in seminars and such like that aim to reform the former prisoner's intent. Much counter-terrorism since the 2000s is focused on persuading people that terrorism is morally wrong, to renounce terrorism, and to speak out against terrorism.

Reduce Capabilities

Reducing threatening capability involves controlling the hazard's acquisition of capability or reducing the threat's acquired capabilities.

Counter the Acquisition of Capabilities

Preventing the potential aggressor from acquiring the capabilities to threaten us is the objective behind the many strategies called "counter-proliferation," which aim to reduce the supply of arms to hazardous actors (such as unfriendly states, insurgents, and terrorists). Countering acquisition is easy to confuse with containing the hazard but is not the same strategy. For instance, while seeking confirmation as U.S. Secretary of State, Senator John Kerry told the Senate's Foreign Relations Committee (January 24, 2013) about

current U.S. strategy toward Iranian nuclear weaponization: "We will do what we must do to prevent Iran from obtaining a nuclear weapon, and I repeat here today, our policy is not containment [of a threat]. It is prevention [of acquisition], and the clock is ticking on our efforts to secure responsible compliance."

Given that a group's capabilities include personnel, this strategy could focus on countering the group's recruitment.

Reduce Acquired Capabilities

Once the threat has acquired threatening capabilities, we could aim to reduce those capabilities by removing, damaging, or destroying them. For instance, law enforcement involves confiscating weapons, war involves attacks on enemy arms and the supply chain, and health care includes destruction of pathogens, toxins, and other sources of health risks.

Sometimes personnel are targeted in order to reduce threatening capabilities. Counter-terrorism sometimes includes campaigns to persuade people to separate from terrorist groups. An alternative is to kill them. A terrorist who has already attacked and is not dissuadable or detainable is more justifiably killed. However, prevention of terrorism has too often involved extra-judicial killing of terrorist hazards, rather than containing, deterring, or reforming the sources, and has often generated new grievances. In fact, terrorist groups, particularly religious terrorist groups, are more cohesive and motivated after lethal attacks on them, even if their capabilities are degraded (Post, 1987). If we were to fail to kill the leader of a group that is still in a hazardous state (it had not chosen to threaten us), we would provide the leader with justifiable intent to retaliate against us. Even if the leader had chosen to be a threat already, killing the target erodes the rule of law and encourages similar actions against our own leaders.

Controlling Negative Effects

We could control or reduce the negative effects that would arise from a potential event. Termination of the risk would be achieved if we went so far as to prevent any negative effects from the threat's capabilities. For instance, imagine that a criminal leader has chosen to threaten us and orders the criminal gang to take up small arms against us. If we were to acquire for all our assets a material armor that is perfectly proof against small arms (and we were to ban all unarmored activities), our operations would become invulnerable to small arms. As long as the criminal gang does not acquire weapons that threaten our armor, and the armor works perfectly, we would have prevented all risks associated with that gang. In theory, the gang could innovate a threat to our defenses, a reminder that we should watch risks for change.

Controlling the negative effects is a strategy that could be known by many other words that are more precise, such as *defense, deterrence, protection*, and *preparedness*. Defense, as the capacity to defeat the attack, is focused on reducing the likelihood of a successful attack, as is deterrence. Some defensive measures, like most forms of preparedness, are focused on reducing the negative returns of an attack. For instance, guards could be employed to prevent human threats from attacking more vulnerable or valuable things, such as interior personnel and assets, and to deter any attacks in the first place—in either case, their effect is to reduce the likelihood of a successful attack. Other acquisitions, such as the armor worn on the bodies of the guards, are acquired more to reduce the negative effects of any attack than to reduce the likelihood of an attack.

The strategy of controlling the negative effects is known by (unfortunately) nine other terms that are highly synonymous but rarely admit their common objective or the existence of other synonyms,

and are often poorly defined: protecting the targets, preparing to defend or protect against the threat, planning for contingencies, mitigating the negative returns, managing consequences, building resilience against disruption, responding to the event, continuing operations despite the event, or recovering from the event.

Protection

For the U.S. DHS (2009), *protection* is the "actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP [National Infrastructure Protection Plan], protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident" (p. 110).

For the British Civil Contingencies Secretariat, *civil protection* is "organization and measures, under governmental or other authority, aimed at preventing, abating or otherwise countering the effects of emergencies for the protection of the civilian population and property" (U.K. Cabinet Office, 2013).

For the Humanitarian Practice Network (2010, pp. xviii, 55, 71) the *protection approach* is "a security strategy" or "approach to security" that "emphasizes the use of protective devices and procedures to reduce vulnerability to existing threats, but does not affect the level of threat." It later added that reducing vulnerability under this approach can be done "in two ways, either by hardening the target or by increasing or reducing its visibility," but the latter reduces the likelihood not the returns.

Preparedness

For the UN, *preparedness* is the "activities designed to minimize loss of life and damage, to organize the temporary removal of people and property from a threatened location and facilitate timely and effective rescue, relief and rehabilitation" (UN DHA, 1992) or "the knowledge and capacities developed by governments, professional response and recovery organizations, communities, and individuals to effectively anticipate, respond to, and recover from, the impacts of likely, imminent, or current hazard events or conditions" (UN ISDR, 2009, p. 9).

For U.S. Federal Emergency Management Agency (FEMA) (1992) preparedness is "those activities, programs, and systems that exist prior to an emergency that are used to support and enhance response to an emergency or disaster." For U.S. DHS (2009), preparedness is the

> activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents. (p. 110)

For the British Civil Contingencies Secretariat, preparedness is the "process of preparing to deal with known risks and unforeseen events or situations that have the potential to result in an emergency" (U.K. Cabinet Office, 2013).

Contingency and Scenario Planning

The term *contingency planning* literally means planning to meet different contingencies (future issues), although it is sometimes used to mean preparedness (for instance, Heerkens, 2002, p. 150).

For the UN, contingency planning is "a management tool used to ensure that adequate arrangements are made in anticipation of a crisis" (UN Office for the Coordination of Humanitarian Affairs [OCHA], 2003) or "a management process that analyses specific potential events or emerging situations that might threaten society or the environment and establishes arrangements in advance to enable timely, effective, and appropriate responses to such events and situations" (UN ISDR, 2009, p. 3). For the Humanitarian Practice Network (2010, p. xv) contingency planning is "a management tool used to ensure adequate preparation for a variety of potential emergency situations," while *scenario planning* is "forward planning about how a situation may evolve in the future, and how threats might develop [and] reviewing the assumptions in plans and thinking about what to do if they do not hold."

For Public Safety Canada (2012) a *contingency plan* is "a plan developed for a specific event or incident" (p. 17).

For the British Civil Contingencies Secretariat, a contingency is the "possible future emergency or risk that must be prepared for," a contingency plan is a "plan prepared by a particular authority specifying the response to a potential incident within its area of jurisdiction," and a civil contingency planning is "civil protection provisions made for the preparation and planning of a response to and recovery from emergencies" (U.K. Cabinet Office, 2013). For the MOD (2009b) a contingency plan is "a plan which is developed for possible operations where the planning factors have identified or can be assumed. This plan is produced in as much detail as possible, including the resources needed and deployment options, as a basis for subsequent planning" (p. 234).

Mitigation

For the UN, *mitigation* is the "measures taken in advance of a disaster aimed at decreasing or eliminating its impact on society and environment" (UN DHA, 1992) or "the lessening or limitation of the adverse impacts of hazards and related disasters" (UN ISDR, 2009, p. 8).

For the U.S. government, mitigation is "any action taken to eliminate or reduce the long-term risk to human life and property from hazards" (U.S. FEMA, 1999), "ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident" (U.S. DHS, 2009, p. 110), or "the capabilities necessary to reduce loss of life and property by lessening the impact of disasters" (U.S. DHS, 2011).

For Public Safety Canada (2012), it is the "actions taken to reduce the impact of disasters in order to protect lives, property, and the environment, and to reduce economic disruption" (p. 63).

"Mitigation . . . aims at reducing the negative effects of a problem" (Heerkens, 2002, p. 150).

Consequence Management

Consequence management sounds much like mitigation. The Canadian government defines *consequence management* as "the coordination and implementation of measures and activities undertaken to alleviate the damage, loss, hardship, and suffering caused by an emergency. Note [that] consequence management also includes measures to restore essential government services, protect public health, and provide emergency relief to affected governments, businesses, and populations" (Public Safety Canada, 2012, p. 17). The British Civil Contingencies Secretariat defines consequence management as the "measures taken to protect public health and safety, restore essential services, and provide emergency relief to governments, businesses, and individuals affected by the impacts of an emergency" (U.K. Cabinet Office, 2013).

Resilience is "the ability of a system, community, or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. Comment: Resilience means the ability to 'resile from' or 'spring back from' a shock" (UN ISDR, 2009, p. 10).

Resilience is the "adaptive capacity of an organization in a complex and changing environment" (International Organization for Standardization, 2009a, p. 11).

The U.S. DHS (2009) defined resilience as "the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions" (p. 111).

In Britain, "resilience reflects how flexibly this capacity can be deployed in response to new increased risks or opportunities" (U.K. Prime Minister's Strategy Unit, 2005, p. 38), the "ability of a community, services, area, or infrastructure to detect, prevent, and, if necessary, to withstand, handle and recover from disruptive challenges" (U.K. Cabinet Office, 2013), or is the "ability of an organization to resist being affected by an incident" (U.K. MOD, 2011c, p. Glossary-3). *Community resilience* is "communities and individuals harnessing local resources and expertise to help themselves in an emergency in a way that complements the response of the emergency services" (U.K. Cabinet Office, 2013).

In Canada, resilience is "the capacity of a system, community, or society to adapt to disruptions resulting from hazards by persevering, recuperating, or changing to reach and maintain an acceptable level of functioning" (Public Safety Canada, 2012, p. 80).

Recently, the World Economic Forum asserted the greater importance of "national resilience" to "global risks."

> In the wake of unprecedented disasters in recent years, "resilience" has become a popular buzzword across a wide range of disciplines, with each discipline attributing its own working definition to the term. A definition that has long been used in engineering is that resilience is the capacity for "bouncing back faster after stress, enduring greater stresses, and being disturbed less by a given amount of stress". This definition is commonly applied to objects, such as bridges or skyscrapers. However, most global risks are systemic in nature, and a system—unlike an object—may show resilience not by returning exactly to its previous state, but instead by finding different ways to carry out essential functions; that is, by adapting. For a system, an additional definition of resilience is "maintaining system function in the event of disturbance". The working definition of a resilient country for this report is, therefore, one that has the capability to 1) adapt to changing contexts, 2) withstand sudden shocks and 3) recover to a desired equilibrium, either the previous one or a new one, while preserving the continuity of its operations. The three elements in this definition encompass both recoverability (the capacity for speedy recovery after a crisis) and adaptability (timely adaptation in response to a changing environment). (World Economic Forum, 2013, p. 37)

The World Economic Forum chose to break down resilience into three characteristics (robustness, redundancy, resourcefulness) and two measures of performance (response, recovery).

a. "Robustness incorporates the concept of reliability and refers to the ability to absorb and withstand disturbances and crises. The assumptions underlying this component of resilience are that: 1) if fail-safes and firewalls are designed into a nation's critical networks, and 2) a

nation's decision-making chains of command become more modular in response to changing circumstances, then potential damage to one part of a country is less likely to spread far and wide."

b. "Redundancy involves having excess capacity and back-up systems, which enable the maintenance of core functionality in the event of disturbances. This component assumes that a country will be less likely to experience a collapse in the wake of stresses or failures of some of its infrastructure, if the design of that country's critical infrastructure and institutions incorporates a diversity of overlapping methods, policies, strategies or services to accomplish objects and fulfill purposes."

c. "Resourcefulness means the ability to adapt to crises, respond flexibly and—when possible—transform a negative impact into a positive. For a system to be adaptive means that it has inherent flexibility, which is crucial to enabling the ability to influence of resilience. The assumption underlying this component of resilience is that if industries and communities can build trust within their networks and are able to self-organize, then they are more likely to spontaneously react and discover solutions to resolve unanticipated challenges when larger country-level institutions and governance systems are challenged or fail."

d. "Response means the ability to mobilize quickly in the face of crises. This component of resilience assesses whether a nation has good methods for gathering relevant information from all parts of society and communicating the relevant data and information to others, as well as the ability for decision-makers to recognize emerging issues quickly."

e. "Recovery means the ability to regain a degree of normality after a crisis or event, including the ability of a system to be flexible and adaptable and to evolve to deal with the new or changed circumstances after the manifestation of a risk. This component of resilience assesses the nation's capacities and strategies for feeding information into public policies and business strategies, and the ability for decision-makers to take action to adapt to changing circumstances." (pp. 38–39)

The World Economic Forum chose to assess national resilience to global risks as a system of five "core subsystems" (economic, environmental, governance, infrastructure, and social) and thus advocated assessing the resilience of each of the five subsystems by each of the five components of resilience.

Separately, survey respondents suggested that national resilience has seven characteristics or attributes: politicians' ability to govern; healthy business-government relations; efficient implementation of reforms; public trust of politicians; low wastefulness of government spending; measures to control corruption; and government services for improved business performance.

Response

The World Economic Forum places recovery as a part of resilience, but U.S. emergency management always has separated response as a "phase" of emergency management before recovery.

> [Response is the] activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities

> designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increasing security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (U.S. DHS, 2009, p. 111)

Continuity

The management of emergency, consequence, or continuity essentially means the same thing as resilience.

The British Civil Contingencies Secretariat defines *continuity* as "the grounding of emergency response and recovery in the existing functions of organisations and familiar ways of working" and defines "business continuity management" as "a management process that helps manage risks to the smooth running of an organization or delivery of a service, ensuring that it can operate to the extent required in the event of a disruption" (U.K. Cabinet Office, 2013). Public Safety Canada (2012) defines *business continuity management* as "an integrated management process involving the development and implementation of activities that provides for the continuity and/or recovery of critical service delivery and business operations in the event of a disruption" (pp. 7–8).

Recovery

Continuity might overlap *recovery*—although recovery might imply outside aid, such as by the UN, which would mean that the risk had been transferred. The UNHCR defined recovery as a focus on how best to restore the capacity of the government and communities to rebuild and recover from crisis and to prevent relapses into conflict. "The UN ISDR (2009) defined recovery as "the restoration, and improvement where appropriate, of facilities, livelihoods and living conditions of disaster-affected communities, including efforts to reduce disaster risk factors" (p. 9).

The U.S. DHS (2009) defined recovery as

> the development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents. (p. 111)

The Canadian government defined recovery as "actions taken to repair or restore conditions to an acceptable level after a disaster" and noted that recovery includes "the return of evacuees, trauma counseling, reconstruction, economic impact studies, and financial assistance." It also referred to response —"actions taken during or immediately after a disaster to manage its consequences and minimize suffering and loss" —noted examples— "emergency public communication, search and rescue, emergency medical assistance, evacuation, etc." (Public Safety Canada, 2012, pp. 78, 81).

For the British Civil Contingencies Secretariat, recovery is the "process of rebuilding, restoring, and rehabilitating the community following an emergency." Linked to recovery, is *remediation*: "restoration

of a built or natural environment that has been destroyed, damaged, or rendered hazardous as the result of an emergency or disasters" (U.K. Cabinet Office, 2013).

Turn

We could effectively terminate the risk by turning the source or cause in our favor. For instance, rather than kill the leader of the criminal gang, we could ally with it against another threat or offer a cooperative return to lawful activities.

The strategy of turning the risk offers more than either terminating or taking the opportunity because it turns a negative into a positive risk.

We would never want to turn a positive risk into a negative risk, but we could do so unintentionally, for instance, by upsetting an ally until the ally turns against us. Moreover, a strategy of turning a negative into a positive risk could fail and could introduce new risks from the same source. At worst, an alliance could expose us to a temporary ally that ends up a threat. For instance, from 2007, the U.S.-led coalition in Iraq chose to pay rents and to arm various militia or insurgent groups in return for their commitment to stop attacks on coalition targets; some of these groups helped to combat others who remained outside of the coalition, but some eventually turned their new arms on the coalition. The continuing lawlessness and multiple duplicities in Iraq were permissive of such chaos. At worst, an alliance could expose us to a threat that is only pretending to be an ally.

A strategy of turning threats into allies can be tricky too because of reactions from third parties. For instance, many victims of the criminals would feel justifiably aggrieved if you offered cooperation with the criminals without justice for the victims. Some other criminals could feel that their further crimes would be rewarded by cooperation or feel aggrieved that you chose not to cooperate with them.

Take

Taking a risk is a deliberate choice to pursue a positive risk, even if negative risks are taken too. The strategy of taking risk is known elsewhere as a strategy of pursuing, enhancing, or exploiting positive risks. (The British Treasury, and thence most of British government, has called the strategy "taking the opportunity," but I have found that users conflate its intended meaning with any strategic response to risk, as in "taking the opportunity" to do anything but nothing.)

Taking risk could include accepting some potential negative returns, so long as we are simultaneously pursuing positive risk. For instance, any speculative risk includes the chance of gaining less than we expected or even a loss. Taking a risk does not need to mean avoidance of potentially negative returns, just to mean pursuit of potential positive returns.

Taking the risk would seem obvious if we estimate a large chance of positive outcomes and no chance of negative outcomes. Nevertheless, many people take speculative risks despite a much higher chance of loss than of gains. In fact, against a competent bookmaker, most bets have negative expected returns, but plenty of people make such bets in pursuit of an unlikely big win.

Even if the chance of positive outcomes is higher than of negative outcomes, we should still not take the risk if the cost of taking the risk outweighs the potential positive returns or at least the expected return (see Chapter 3). Taking the risk may necessitate investments or expenditures of resources. For instance, many business ventures involve hefty investment in the hope of future profits or returns on investment. Sometimes investors must take highly subjective decisions about whether the potential positive returns outweigh the potential loss of the exposed investment.

Finally, taking the risk may involve unobserved risks. For instance, we could agree to make a hefty investment after having estimated that positive returns are highly likely, yet that investment might leave us without reserves against unrelated negative risks, such as potential collapse in our health or income while awaiting the returns on our investment.

Transfer

Transferring the risk means that we transfer some of the risk to another actor. We could pay an insurer for a commitment to cover any negative returns, hope to sue the liable party through the tort system, rely on charity to cover our losses, rely on some guarantor to compensate us, share the risk with business partners, or share risks with contractors.

The most likely alternative to transferring the risk is to retain the risk—relying on our internal resources to cover negative returns. Retaining the risk is a form of tolerating the risk, whereas transferring the risk implies that we cannot tolerate the risk. Retaining the risk makes better sense if we were to believe that the other actor could not or would not cover our negative returns.

The sub-sections below discuss the six main vectors for transferred risk: insurers; tort systems; charities; guarantors; partners; and contractors.

Pedagogy Box 10.9 UN Definition of Risk Transfer

The UN ISDR (2009) defines *risk transfer* as "the process of formally or informally shifting the financial consequences of particular risks from one party to another whereby a household, community, enterprise, or state authority will obtain resources from the other party after a disaster occurs, in exchange for ongoing or compensatory social or financial benefits provided to that other party" (p. 11).

Insurers

Insurers accept a premium (usually a financial price per period of coverage) in return for accepting some responsibility for a risk (usually a promise to pay monies toward the financial costs that you would suffer due to agreed events).

Insurers cover some risks at standard rates—these standard risks are easier for the insurer to assess, such as potential harm from road traffic accidents, home fires, and work-related injuries. Traditionally, most potential insurees were forced to retain risks associated with war, terrorism, natural disasters, and other risks that insurers liked to write up as "acts of god," either because insurers refused to insure against such risks, given their greater uncertainty, or because few consumers could afford the premiums (or because consumers were less trusting of the insurer who would insure against such risks). In recent decades, particularly since the terrorist attacks of 9/11 (September 11, 2001), governments have guaranteed insurers against higher losses associated with these risks, promised to cover the losses directly, or legislatively forced insurers not to exclude such risks. These official actions have encouraged insurers and insurees and discouraged retention of risk. Consequently, take-up of political risk and terrorism insurance has jumped 25%–50% since 9/11.

However, at the same time, legal disputes between insurer and insuree over huge losses have discouraged potential insurees in certain domains. Insurers sometimes disagree with the insured party

about whether the insured is covered against a certain negative return. For instance, the insurers of the twin towers in Manhattan that collapsed on September 11, 2001, tried to claim that the source was domestic terrorism (because the terrorists, although foreign by citizenship and sponsorship, were passengers and hijackers of planes that had taken off from American airports), which was not covered, rather than international terrorism, which was covered.

Sometimes insurers find that incoming claims run ahead of their reserves or their reinsurers' reserves, so in theory the insuree could be left retaining all the risk even after paying for insurance, although governments can choose to guarantee insurers.

Tort System

The tort system is the legal system that allows parties to bring claims of wrongdoing, harm, or injustice against another party.

The tort system is an uncertain instrument and a negative risk given that a court could disagree with the claimant's case against a liable party, leaving the claimant with legal costs or an order to pay the other party's legal costs. The tort system is useless to us if the court is biased against us, the liable party has insufficient reserves or assets to cover our losses, or the liable party is able to evade a court's judgment.

The effectiveness of the tort system varies by time and space. For instance, the United States has a strong tort system and highly accountable public services, where service providers and suppliers complain that their liabilities make business difficult, whereas Britain has a weak tort system and poorly accountable public services, where consumers complain that service providers and suppliers are too willing to make promises for which they are practically not liable (except in terms of lost customers).

Charities

Charities accept risks that otherwise would not be covered by those exposed, perhaps because they are too poor in material terms or too poorly represented. Charities often appear in response to crisis. For instance, some persons chose to manage donations of money in response to Storm Sandy in the northeastern United States in October 2012, and others chose to volunteer their labor. Most international aid is essentially charitable, although some quid pro quo, such as preferential trade, might be implied.

Charities are the least certain of the actors to which we could transfer our risks, since they themselves usually rely on voluntary donations and their reserves tend to be unpredictable and particular in form. Unlike insurers with whom we contract, charities are under no obligations, so they can choose not to cover our losses.

Guarantors

Guarantors promise to cover our negative returns. Guarantors could be as simple as a relative who promises to help out if our business fails or as authoritative as a government that promises to pay "benefits"/"entitlements" if we lose our jobs or become too ill to work. Some guarantors effectively preempt the tort system by promising to pay us compensation if some representative causes us injury or injustice. For instance, in order to encourage business, many governments guarantee residents against losses due to riots, terrorism, or other organized violence.

However, guarantors sometimes choose not to honor their commitments. Ultimately few governments are beholden to any independent judicial enforcement of their promises, so any official guarantee

is effectively a political risk. For instance, governments often guarantee to compensate businesses against mass lawlessness or political violence in order to encourage business within their jurisdiction, but after widespread riots in Britain in August 2011, the British government was criticized for its incremental interpretation of who was eligible for compensation and how quickly their businesses should be restored, leading eventually to official clarification of its future interpretation.

Partners

We could persuade another party to coinvest or codeploy —effectively sharing the chance of lost investment or mission failure. However, a coinvestor could sue us for false promises or incompetence or some other reason to blame us disproportionately for the losses—effectively using the tort system to transfer the risk back to us. Similarly, political partners can blame each other for shared failures.

Contractors

Contractors who agree to provide us with some service or product effectively share the risk of their nonperformance, such as a failure to deliver a service on time or as specified. Contractual obligations may mean nothing in the event of nonperformance if the contractor does not accept those obligations, refuses to compensate us for nonperformance, is not found liable by the tort system, or does not have the reserves to cover our losses.

Thin the Risk

Thinning the risk is a strategy known usually as diversification. It is a unique strategy that does not terminate, turn, take, transfer, or treat any particular risk but nevertheless reduces our total risk by spreading or thinning our loss exposure across more diverse types of risks, sites, partners, providers, etc. You could take on more types of risk while reducing your total negative risk, although at the same time you may reduce your potential positive returns.

Readers may be most familiar with diversification in financial risk management. The simplest example of nondiversification is a situation where one investor has speculated all his or her resources on one venture. Whatever the likelihood of failure, the investor has exposed all his or her resources to a failure in that venture. Alternatively, the investor could invest all the same resources in two ventures. Even if the likelihood of failure is the same for both ventures, the total risk has fallen, without reducing either the likelihood of an individual failure or total exposure. This is mathematically true because total loss is possible only if both ventures fail rather than one venture fails. If the likelihood of failure is 50%, the likelihood of total loss from investing in one venture is 50%, but the likelihood of total loss from investing in two ventures is 25% (50% multiplied by 50%; the two events are independent or consecutive, so their probabilities are multiplied when we want to know the probability of both events occurring). Our total risk has thinned because our exposure to any one negative event has thinned, not because the likelihood of any event or our total exposure has changed.

Although diversification is applied routinely to financial risks, it can be applied to any risk. For instance, imagine that we are operating in an area where terrorists are plotting to destroy our operations. Instead of operating in a single city with a 20% chance of total loss ($\$x$), we could spread our operations equally over two cities ($\$0.5x$ per city), each with an independent (consecutive) 20% chance of loss within that city. The probability of total loss ($\$x$) would shift from 20% to 4% (20% multiplied by 20%).

However, thinning or diversifying the risks could involve new costs. For instance, operating in two cities might be more expensive than operating in one city (if only because we have foregone the efficiencies of scale or centralization).

Moreover, thinning or diversifying the risks often reduces the chance of the best outcome at the same time as it reduces the chance of the worst outcome. For instance, if we operate in one city, as specified above, the chance of not losing any of $\$x$ is 80%, but across two cities, the chance is 64% (80% multiplied by 80%). The way to justify reductions in the likelihoods of both the best and worst outcomes is to realize that the range of returns has narrowed (thus, we face narrower uncertainty over the range of possible outcomes) and the chance of the worst outcome has fallen (this combination of effects fulfills *risk efficiency*—see Chapter 3).

Combining and Balancing Strategies

Ideally, we want the single most efficient strategy. For instance, we would not want to purchase very expensive controls on the negative returns of a potential event if we could freely persuade a hazardous actor not to cause the event.

In practice, we often combine strategies in response to a collection of risks, even in response to one risk, in order to combine the best of different strategies. For instance, we might seek both to terminate a risk while we seek to control its potential negative returns in case termination does not work. The Humanitarian Practice Network (2010) notes that "[i]n practice, a good security strategy needs a flexible combination of approaches" (p. 56).

We should combine strategies that hedge against one another failing. We should also combine strategies when risks lie on four polarized dimensions, as described in the subsections below: negative versus positive risks; pure versus speculative risks; unknown versus known causes and sources; and uncontrollable and controllable causes and sources.

Negative and Positive Risks

The most basic strategic response to risk is to maximize positive risks and minimize negative risks. For this reason, PRINCE2 starts its strategic recommendations with a question about whether the risks are positive or negative (although the authority misleadingly uses the terms *threat* and *opportunity*). British Prime Minister Tony Blair once advocated to government a similar strategy, where risk management is "getting the right balance between innovation and change on the one hand and avoidance of shocks and crises on the other" (Strategy Unit, November 2002, foreword). The IRGC (2008, p. 4) agrees that the "challenge of better risk governance" is "to enable societies to benefit from change while minimizing the negative consequences of the associated risks."

Pure and Speculative Risks

Relatedly, we should minimize pure risks and speculate in the most positive risks. Indeed, some authors have defined risk management as an "activity seeking to eliminate, reduce and generally control pure risks . . . and to enhance the benefits and avoid detriment from speculative risks" (Waring & Glendon, 1998, p. 3).

These strategic approaches to pure and speculative risks can be known by specific terms, such as the following:

- *Strategic risk management*, which "addresses interactions between pure and speculative risks" (Waring & Glendon 1998, p. 14). For instance, your exposure to natural disaster (natural risk)

could deter investors (financial risk), or a potential financial crisis (financial risk) suggests potential collapse in outside resourcing of your security.

- *Enterprise risk management*, which "addresses interactions between pure and speculative risks" (Waring & Glendon 1998, p. 14) or is "making use of methods and processes to capitalize on opportunities or avoid hazards to meet institutional goals" (Kennedy & Van Brunschot, 2009, p. 28).
- *Integrated risk management* is "a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective and to support strategic decision making that contributes to the achievement of an organization's overall objectives" (Public Safety Canada, 2012, p. 56), or a "multi-agency approach to emergency management entailing six key activities—anticipation, assessment, prevention, preparation, response, and recovery" (U.K. Cabinet Office, 2013).
- *Uncertainty management*: "[M]anaging perceived threats and opportunities and their risk implications but also managing the various sources of uncertainty which give rise to and shape risk, threat and opportunity" (Chapman & Ward, 2002, p. 54), or "the process of integrating risk management and value management approaches" (Smith, 2003, p. 2).
- *Risk efficiency*: "Successful risk management is not just about reducing threats to project performance. A key motive is the identification of opportunities to change base plans and develop contingency plans in the context of a search for risk efficiency, taking an aggressive approach to the level of risk that is appropriate, with a view to long-term corporate performance maximization" (Chapman & Ward, 2002, p. 54).

Unknown and Known Causes and Sources

The IRGC (2008, p. 6, 16–17) recommends categorization of risks by our "knowledge about the cause-effect relationships" (our "knowledge challenge"), where each category would suggest a different response. The IRGC recommends placing a risk in one of four categories: simple, complex, uncertain, or ambiguous.

1. *Simple risks*, such as home fires, where the causes are obvious, "can be managed using a 'routine-based' strategy, such as introducing a law or regulation."
2. *Complex risks* arise from "difficulties in identifying and quantifying causal links between a multitude of potential causal agents and specific observed effects. Examples of highly complex risks include the risks of failures of large interconnected infrastructures and the risks of critical loads to sensitive ecosystems." They "can be addressed on the basis of accessing and acting on the best available scientific expertise, aiming for a 'risk-informed' and 'robustness-focused' strategy. Robustness refers to the degree of reliability of the risk reduction measures to withstand threatening events or processes that have not been fully understood or anticipated."
3. *Uncertain risks* arise from "a lack of clarity or quality of the scientific or technical data. Highly uncertain risks include many natural disasters, acts of terrorism and sabotage, and the long-term effects of introducing genetically-modified species into the natural environment." They "are better managed using 'precaution-based' and 'resilience-focused' strategies, with the intention being to apply a precautionary approach to ensure the reversibility of critical decisions and to increase a systems' coping capacity to the point where it can withstand surprises."

4. *Ambiguous risks* result "from divergent or contested perspectives on the justification, severity, or wider meanings associated with a given threat. Risks subject to high levels of ambiguity include food supplements, hormone treatment of cattle, passive smoking, some aspects of nanotechnology, and synthetic genomics." The "appropriate approach comprises a 'discourse-based' strategy which seeks to create tolerance and mutual understanding of conflicting views and values with a view to eventually reconciling them."

Uncontrollable and Controllable Causes and Sources

Similarly, in search of categories of risk that would be easier to act upon, Robert Kaplan and Anette Mikes (2012) suggested, and the World Economic Forum endorsed (2013, p. 36), the management of risks by the extent to which their sources and causes were controllable. They effectively combined judgments of positive versus negative, pure versus speculative, and internal versus external risks to suggest three categories:

1. *Preventable risks*: "These are internal risks, arising from within the organization, that are controllable and ought to be eliminated or avoided. Examples are the risks from employees' and managers' unauthorized, illegal, unethical, incorrect, or inappropriate actions and the risks from breakdowns in routine operational processes." The correct response is to set rules demanding behaviors that prevent these risks.
2. *Strategy risks*: "Strategy risks are quite different from preventable risks because they are not inherently undesirable. A strategy with high expected returns generally requires the company to take on significant risks, and managing those risks is a key driver in capturing the potential gains." To me, strategy risks sound like speculative risks, so the correct response is to treat the risks in order to minimize the negative and maximize the positive. (Kaplan and Mikes advise us "to reduce the probability that the assumed risks actually materialize and to improve the company's ability to manage or contain the risk events should they occur." Their general point was that rules-based prevention would be too exclusive for strategy risks.)
3. *External risks*: "Some risks arise from events outside the company and are beyond its influence or control. Sources of these risks include natural and political disasters and major macroeconomic shifts." The World Economic Forum (2013, pp. 9, 36) endorsed external risks as "global risks" and characterized "most" of the global risks in its reports as "difficult to predict" with "little knowledge on how to handle such risks." To me, external risks sound like pure risks, to which the correct responses are avoidance or insurance (or some other form of transference). Kaplan and Mikes advise us to "focus on identification (they tend to be obvious in hindsight) and mitigation of their impact." The World Economic Forum advises us to focus on resilience.

SUMMARY

This chapter has

- defined control,
- given advice on establishing tolerable risks,