SMART COMPANIES MATCH THEIR APPROACH TO THE NATURE OF THE THREATS THEY FACE.

BY ROBERT S. KAPLAN AND ANETTE MIKES

MANAGI RISKS: A NEW FRAMEW

Robert S. Kaplan is a Baker Foundation Professor at Harvard Business School and the cocreator of the Balanced Scorecard management system.

Anette Mikes is an assistant professor at Harvard Business School.

NG

/ORK

WHEN TONY HAYWARD BECAME CEO OF BP, IN 2007, he vowed to make safety his top priority. Among the new rules he instituted were the requirements that all employees use lids on coffee cups while walking and refrain from texting while driving. Three years later, on Hayward's watch, the *Deepwater Horizon* oil rig exploded in the Gulf of Mexico, causing one of the worst man-made disasters in history. A U.S. investigation commission attributed the disaster to management failures that crippled "the ability of individuals involved to identify the risks they faced and to properly evaluate, communicate, and address them."

Hayward's story reflects a common problem. Despite all the rhetoric and money invested in it, risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. Many such rules, of course, are sensible and do reduce some risks that could severely damage a company. But rules-based risk management will not diminish either the likelihood or the impact of a disaster such as Deepwater Horizon, just as it did not prevent the failure of many financial institutions during the 2007–2008 credit crisis.

In this article, we present a new categorization of risk that allows executives to tell which risks can be managed through a rules-based model and which require alternative approaches. We examine the individual and organizational challenges inherent in generating open, constructive discussions about managing the risks related to strategic choices and argue that companies need to anchor these discussions in their strategy formulation and implementation processes. We conclude by looking at how organizations can identify and prepare for nonpreventable risks that arise externally to their strategy and operations.

Managing Risk: Rules or Dialogue?

The first step in creating an effective risk-management system is to understand the qualitative distinctions among the types of risks that organizations face. Our field research shows that risks fall into one of three categories. Risk events from any category can be fatal to a company's strategy and even to its survival.

Category I: 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. To be sure, companies should have a zone of tolerance for defects or errors that would not cause severe damage to the enterprise and for which achieving complete avoidance would be too costly. But in general, companies should seek to eliminate these risks since they get no strategic benefits from taking them on. A rogue trader or an employee bribing a local official may produce some short-term profits for the firm, but over time such actions will diminish the company's value.

Idea in Brief

For all the rhetoric about its importance and the money invested in it, risk management is too often treated as a compliance issue.

A rules-based risk-management system may work well to align values and control employee behavior, but it is unsuitable for managing risks inherent in a company's strategic choices or the risks posed by major disruptions or changes in the external environment. Those types of risk require systems aimed at generating discussion and debate.

For strategy risks, companies must tailor approaches to the scope of the risks involved and their rate of change. Though the risk-management functions may vary from company to company, all such efforts must be anchored in corporate strategic-planning processes.

To manage major external risks outside the company's control, companies can call on tools such as war-gaming and scenario analysis. The choice of approach depends on the immediacy of the potential risk's impact and whether it arises from geopolitical, environmental, economic, or competitive changes.

This risk category is best managed through active prevention: monitoring operational processes and guiding people's behaviors and decisions toward desired norms. Since considerable literature already exists on the rules-based compliance approach, we refer interested readers to the sidebar "Identifying and Managing Preventable Risks" in lieu of a full discussion of best practices here.

Category II: Strategy risks. A company voluntarily accepts some risk in order to generate superior returns from its strategy. A bank assumes credit risk, for example, when it lends money; many companies take on risks through their research and development activities.

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. BP accepted the high risks of drilling several miles below the surface of the Gulf of Mexico because of the high value of the oil and gas it hoped to extract.

Strategy risks cannot be managed through a rules-based control model. Instead, you need a risk-management system designed 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. Such a system would not stop companies from undertaking risky ventures; to the contrary, it would enable companies to take on higher-risk, higher-reward ventures than could competitors with less effective risk management.

Category III: 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. External risks require yet another approach. Because companies cannot prevent such events from occurring, their management must focus on identification (they tend to be obvious in hindsight) and mitigation of their impact.

Companies should tailor their risk-management processes to these different categories. While a compliance-based approach is effective for managing preventable risks, it is wholly inadequate for strategy risks or external risks, which require a fundamentally different approach based on open and explicit risk discussions. That, however, is easier said than done; extensive behavioral and organizational research has shown that individuals have strong cognitive biases that discourage them from thinking about and discussing risk until it's too late.

Why Risk Is Hard to Talk About

Multiple studies have found that people overestimate their ability to influence events that, in fact, are heavily determined by chance. We tend to be *overconfident* about the accuracy of our forecasts and risk assessments and far too narrow in our assessment of the range of outcomes that may occur.

We also *anchor our estimates* to readily available evidence despite the known danger of making linear extrapolations from recent history to a highly uncertain and variable future. We often compound

PHOTOGRAPHY: SHUTTERSTOCK

Identifying and Managing Preventable Risks

Companies cannot anticipate every circumstance or conflict of interest that an employee might encounter.

Thus, the first line of defense against preventable risk events is to provide guidelines clarifying the company's goals and values.

THE MISSION A well-crafted mission statement articulates the organization's fundamental purpose, serving as a "true north" for all employees to follow. The first sentence of Johnson & Johnson's renowned credo, for instance, states, "We believe our first responsibility is to the doctors, nurses and patients, to mothers and fathers, and all others who use our products and services," making clear to all employees whose interests should take precedence in any situation. Mission statements should be communicated to and understood by all employees.

THE VALUES Companies should articulate the values that guide employee behavior toward principal stakeholders, including customers, suppliers, fellow employees, communities, and shareholders. Clear value statements help employees avoid violating the company's standards and putting its reputation and assets at risk.

THE BOUNDARIES A strong corporate culture clarifies what is not allowed. An explicit definition of boundaries

this problem with a *confirmation bias,* which drives us to favor information that supports our positions (typically successes) and suppress information that contradicts them (typically failures). When events depart from our expectations, we tend to *escalate commitment,* irrationally directing even more resources to our failed course of action—throwing good money after bad.

Organizational biases also inhibit our ability to discuss risk and failure. In particular, teams facing uncertain conditions often engage in *groupthink*: Once a course of action has gathered support within a group, those not yet on board tend to suppress their objections—however valid—and fall in line. Groupthink is especially likely if the team is led by an overbearing or overconfident manager who wants to minimize conflict, delay, and challenges to his or her authority.

Collectively, these individual and organizational biases explain why so many companies overlook or misread ambiguous threats. Rather than mitigating risk, firms actually incubate risk through the *normalization of deviance,* as they learn to tolerate apparently minor failures and defects and treat early warning signals as false alarms rather than alerts to imminent danger.

Effective risk-management processes must counteract those biases. "Risk mitigation is painful, not a natural act for humans to perform," says Gentry Lee, the chief systems engineer at Jet Propulsion Laboratory (JPL), a division of the U.S. National Aeronautics and Space Administration. The rocket scientists on JPL project teams are top graduates from elite universities, many of whom have never experienced failure at school or work. Lee's biggest challenge in establishing a new risk culture at JPL was to get project teams to feel comfortable thinking and talking about what could go wrong with their excellent designs.

Rules about what to do and what not to do won't help here. In fact, they usually have the opposite effect, encouraging a checklist mentality that inhibits challenge and discussion. Managing strategy risks and external risks requires very different approaches. We start by examining how to identify and mitigate strategy risks.

Managing Strategy Risks

Over the past 10 years of study, we've come across three distinct approaches to managing strategy risks. Which model is appropriate for a given firm depends largely on the context in which an organization operates. Each approach requires quite different structures and roles for a risk-management function, but all three encourage employees to challenge existing assumptions and debate risk information. Our finding that "one size does not fit all" runs counter to the efforts of regulatory authorities and professional associations to standardize the function.

Independent experts. Some organizations—particularly those like JPL that push the envelope of technological innovation—face high intrinsic risk as they pursue long, complex, and expensive product-development projects. But since much of the risk arises from coping with known laws of nature, the risk changes slowly over time. For these organizations, risk management can be handled at the project level.

JPL, for example, has established a risk review board made up of independent technical experts whose role is to challenge project engineers' design, risk-assessment, and risk-mitigation decisions. The experts ensure that evaluations of risk take place periodically throughout the product-development cycle. Because the risks are relatively unchanging, the review board needs to meet only once or twice a year, with the project leader and the head of the review board meeting quarterly.

SEE ALSO Robert Simons's article on managing preventable risks, "How Risky Is Your Company?" (HBR May 1999), and his book *Levers of Control* (Harvard Business School Press, 1995).

is an effective way to control actions. Consider that nine of the Ten Commandments and nine of the first 10 amendments to the U.S. Constitution (commonly known as the Bill of Rights) are written in negative terms. Companies need corporate codes of business conduct that prescribe behaviors relating to conflicts of interest, antitrust issues, trade secrets and confidential information, bribery, discrimination, and harassment.

Of course, clearly articulated statements of mission, values, and boundaries don't in themselves ensure good behavior. To counter the day-to-day pressures of organizational life, top managers must serve as role models and demonstrate that they mean what they say. Companies must institute strong internal control systems, such as the segregation of duties and an active whistle-blowing program, to reduce not only misbehavior but also temptation. A capable and independent internal audit department tasked with continually checking employees' compliance with internal controls and standard operating processes also will deter employees from violating company procedures and policies and can detect violations when they do occur.

The risk review board meetings are intense, creating what Gentry Lee calls "a culture of intellectual confrontation." As board member Chris Lewicki says, "We tear each other apart, throwing stones and giving very critical commentary about everything that's going on." In the process, project engineers see their work from another perspective. "It lifts their noses away from the grindstone," Lewicki adds.

The meetings, both constructive and confrontational, are not intended to inhibit the project team from pursuing highly ambitious missions and designs. But they force engineers to think in advance about how they will describe and defend their design decisions and whether they have sufficiently considered likely failures and defects. The board members, acting as devil's advocates, counterbalance the engineers' natural overconfidence, helping to avoid escalation of commitment to projects with unacceptable levels of risk.

At JPL, the risk review board not only promotes vigorous debate about project risks but also has authority over budgets. The board establishes cost and time reserves to be set aside for each project component according to its degree of innovativeness. A simple extension from a prior mission would require a 10% to 20% financial reserve, for instance, whereas an entirely new component that had yet to work on Earth—much less on an unexplored planet—could require a 50% to 75% contingency. The reserves ensure that when problems inevitably arise, the project team has access to the money and time needed to resolve them without jeopardizing the launch date. JPL takes the estimates seriously; projects have been deferred or canceled if funds were insufficient to cover recommended reserves.

Facilitators. Many organizations, such as traditional energy and water utilities, operate in stable technological and market environments, with relatively predictable customer demand. In these situations risks stem largely from seemingly unrelated operational choices across a complex organization that accumulate gradually and can remain hidden for a long time.

Risk management is painful—not a natural act for humans to perform.

Since no single staff group has the knowledge to perform operational-level risk management across diverse functions, firms may deploy a relatively small central risk-management group that collects information from operating managers. This increases managers' awareness of the risks that have been taken on across the organization and provides decision makers with a full picture of the company's risk profile.

We observed this model in action at Hydro One, the Canadian electricity company. Chief risk officer John Fraser, with the explicit backing of the CEO, runs dozens of workshops each year at which employees from all levels and functions identify and rank the principal risks they see to the company's strategic objectives. Employees use an anonymous voting technology to rate each risk, on a scale of 1 to 5, in terms of its impact, the likelihood of occurrence, and the strength of existing controls. The rankings are discussed in the workshops, and employees are empowered to voice and debate their risk perceptions. The group ultimately develops a consensus view that gets recorded on a visual risk map, recommends action plans, and designates an "owner" for each major risk.

Hydro One strengthens accountability by linking capital allocation and budgeting decisions to

The danger from embedding risk managers within the line organization is that they "go native"—becoming deal makers rather than deal questioners.

identified risks. The corporate-level capital-planning process allocates hundreds of millions of dollars, principally to projects that reduce risk effectively and efficiently. The risk group draws upon technical experts to challenge line engineers' investment plans and risk assessments and to provide independent expert oversight to the resource allocation process. At the annual capital allocation meeting, line managers have to defend their proposals in front of their peers and top executives. Managers want their projects to attract funding in the risk-based capital planning process, so they learn to overcome their bias to hide or minimize the risks in their areas of accountability.

Embedded experts. The financial services industry poses a unique challenge because of the volatile dynamics of asset markets and the potential impact of decisions made by decentralized traders and investment managers. An investment bank's risk profile can change dramatically with a single deal or major market movement. For such companies, risk management requires embedded experts within the organization to continuously monitor and influence the business's risk profile, working side by side with the line managers whose activities are generating new ideas, innovation, and risks—and, if all goes well, profits.

JP Morgan Private Bank adopted this model in 2007, at the onset of the global financial crisis. Risk managers, embedded within the line organization, report to both line executives and a centralized, independent risk-management function. The face-to-face contact with line managers enables the market-savvy risk managers to continually ask "what if" questions, challenging the assumptions of portfolio managers and forcing them to look at different scenarios. Risk managers assess how proposed trades affect the risk of the entire investment portfolio, not only under normal circumstances but also under times of extreme stress, when the correlations of returns across different asset classes escalate. "Portfolio managers come to me with three trades, and the [risk] model may say that all three are adding to the same type of risk," explains Gregoriy Zhikarev, a risk manager at JP Morgan. "Nine times out of 10 a manager will say, 'No, that's not what I want to do.' Then we can sit down and redesign the trades."

The chief danger from embedding risk managers within the line organization is that they "go native," aligning themselves with the inner circle of the business unit's leadership team—becoming deal makers rather than deal questioners. Preventing this is the responsibility of the company's senior risk officer and—ultimately—the CEO, who sets the tone for a company's risk culture.

Avoiding the Function Trap

Even if managers have a system that promotes rich discussions about risk, a second cognitive-behavioral trap awaits them. Because many strategy risks (and some external risks) are quite predictable—even familiar—companies tend to label and compartmentalize them, especially along business function lines. Banks often manage what they label "credit risk," "market risk," and "operational risk" in separate groups. Other companies compartmentalize the management of "brand risk," "reputation risk," "supply chain risk," "human resources risk," "IT risk," and "financial risk."

Such organizational silos disperse both information and responsibility for effective risk management. They inhibit discussion of how different risks interact. Good risk discussions must be not only confrontational but also integrative. Businesses can be

derailed by a combination of small events that reinforce one another in unanticipated ways.

Managers can develop a companywide risk perspective by anchoring their discussions in strategic planning, the one integrative process that most well-run companies already have. For example, Infosys, the Indian IT services company, generates risk discussions from the Balanced Scorecard, its management tool for strategy measurement and communication. "As we asked ourselves about what risks we should be looking at," says M.D. Ranganath, the chief risk officer, "we gradually zeroed in on risks to business objectives specified in our corporate scorecard."

In building its Balanced Scorecard, Infosys had identified "growing client relationships" as a key objective and selected metrics for measuring progress, such as the number of global clients with annual billings in excess of $50 million and the annual percentage increases in revenues from large clients. In looking at the goal and the performance metrics together, management realized that its strategy had introduced a new risk factor: client default. When Infosys's business was based on numerous small clients, a single client default would not jeopardize the company's strategy. But a default by a $50 million client would present a major setback. Infosys began to monitor the credit default swap rate of every large client as a leading indicator of the likelihood of default. When a client's rate increased, Infosys would accelerate collection of receivables or request progress payments to reduce the likelihood or impact of default.

To take another example, consider Volkswagen do Brasil (subsequently abbreviated as VW), the Brazilian subsidiary of the German carmaker. VW's risk-management unit uses the company's strategy map as a starting point for its dialogues about risk. For each objective on the map, the group identifies the risk events that could cause VW to fall short of that objective. The team then generates a Risk Event Card for each risk on the map, listing the practical effects of the event on operations, the probability of occurrence, leading indicators, and potential actions for mitigation. It also identifies who has primary accountability for managing the risk. (See the exhibit "The Risk Event Card.") The risk team then presents a high-level summary of results to senior management. (See "The Risk Report Card.")

Beyond introducing a systematic process for identifying and mitigating strategy risks, companies also need a risk oversight structure. Infosys uses a

Understanding the Three Categories of Risk

The risks that companies face fall into three categories, each of which requires a different risk-management approach. Preventable risks, arising from within an organization, are monitored and controlled through rules, values, and standard compliance tools. In contrast, strategy risks and external risks require distinct processes that encourage managers to openly discuss risks and find cost-effective ways to reduce the likelihood of risk events or mitigate their consequences.

	CATEGORY 1 **Preventable Risks** Risks arising from within the company that generate no strategic benefits	CATEGORY 2 **Strategy Risks** Risks taken for superior strategic returns	CATEGORY 3 **External Risks** External, uncontrollable risks
RISK MITIGATION OBJECTIVE	Avoid or eliminate occurrence cost-effectively	Reduce likelihood and impact cost-effectively	Reduce impact cost-effectively should risk event occur
CONTROL MODEL	Integrated culture-and-compliance model: Develop mission statement; values and belief systems; rules and boundary systems; standard operating procedures; internal controls and internal audit	Interactive discussions about risks to strategic objectives drawing on tools such as: • Maps of likelihood and impact of identified risks • Key risk indicator (KRI) scorecards Resource allocation to mitigate critical risk events	"Envisioning" risks through: • Tail-risk assessments and stress testing • Scenario planning • War-gaming
ROLE OF RISK-MANAGEMENT STAFF FUNCTION	Coordinates, oversees, and revises specific risk controls with internal audit function	Runs risk workshops and risk review meetings Helps develop portfolio of risk initiatives and their funding Acts as devil's advocates	Runs stress-testing, scenario-planning and war-gaming exercises with management team Acts as devil's advocates
RELATIONSHIP OF THE RISK-MANAGEMENT FUNCTION TO BUSINESS UNITS	Acts as independent overseers	Acts as independent facilitators, independent experts, or embedded experts	Complements strategy team or serves as independent facilitators of "envisioning" exercises

dual structure: a central risk team that identifies general strategy risks and establishes central policy, and specialized functional teams that design and monitor policies and controls in consultation with local business teams. The decentralized teams have the authority and expertise to help the business lines respond to threats and changes in their risk profiles, escalating only the exceptions to the central risk team for review. For example, if a client relationship manager wants to give a longer credit period to a company whose credit risk parameters are high, the functional risk manager can send the case to the central team for review.

These examples show that the size and scope of the risk function are not dictated by the size of the organization. Hydro One, a large company, has a relatively small risk group to generate risk awareness and communication throughout the firm and to advise the executive team on risk-based resource allocations. By contrast, relatively small companies or units, such as JPL or JP Morgan Private Bank, need multiple project-level review boards or teams of embedded risk managers to apply domain expertise to assess the risk of business decisions. And Infosys, a large company with broad operational and strategic scope, requires a strong centralized risk-management function as well as dispersed risk managers who support local business decisions and facilitate the exchange of information with the centralized risk group.

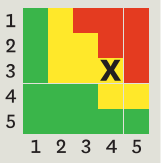
Managing the Uncontrollable

External risks, the third category of risk, cannot typically be reduced or avoided through the approaches used for managing preventable and strategy risks. External risks lie largely outside the company's control; companies should focus on identifying them, assessing their potential impact, and figuring out how best to mitigate their effects should they occur.

Some external risk events are sufficiently imminent that managers can manage them as they do their strategy risks. For example, during the economic slowdown after the global financial crisis, Infosys identified a new risk related to its objective of developing a global workforce: an upsurge in protectionism, which could lead to tight restrictions on work visas and permits for foreign nationals in several OECD countries where Infosys had large client

The Risk Event Card

VW do Brasil uses risk event cards to assess its strategy risks. First, managers document the risks associated with achieving each of the company's strategic objectives. For each identified risk, managers create a risk card that lists the practical effects of the event's occurring on operations. Below is a sample card looking at the effects of an interruption in deliveries, which could jeopardize VW's strategic objective of achieving a smoothly functioning supply chain.

STRATEGIC OBJECTIVE	RISK EVENT	OUTCOMES	RISK INDICATORS	LIKELIHOOD/ CONSEQUENCES	MANAGEMENT CONTROLS	ACCOUNTABLE MANAGER
Guarantee reliable and competitive supplier-to-manufacturer processes	Interruption of deliveries	Overtime Emergency freight Quality problems Production losses	Critical items report Late deliveries Incoming defects Incorrect component shipments		Hold daily supply chain meeting with logistics, purchasing, and QA Monitor suppliers' tooling to detect deterioration Risk mitigation initiative: Upgrade suppliers' tooling Risk mitigation initiative: Identify the key supply chain executive at each critical supplier	Mr. O. Manuel, director of manufacturing logistics

engagements. Although protectionist legislation is technically an external risk since it's beyond the company's control, Infosys treated it as a strategy risk and created a Risk Event Card for it, which included a new risk indicator: the number and percentage of its employees with dual citizenships or existing work permits outside India. If this number were to fall owing to staff turnover, Infosys's global strategy might be jeopardized. Infosys therefore put in place recruiting and retention policies that mitigate the consequences of this external risk event.

Most external risk events, however, require a different analytic approach either because their probability of occurrence is very low or because managers find it difficult to envision them during their normal strategy processes. We have identified several different sources of external risks:

• *Natural and economic disasters with immediate impact.* These risks are predictable in a general way, although their timing is usually not (a large earthquake will hit someday in California, but there is no telling exactly where or when). They may be anticipated only by relatively weak signals. Examples include natural disasters such as the 2010 Icelandic volcano eruption that closed European airspace for a week and economic disasters such as the bursting of a major asset price bubble. When these risks occur, their effects are typically drastic and immediate, as we saw in the disruption from the Japanese earthquake and tsunami in 2011.

• *Geopolitical and environmental changes with long-term impact.* These include political shifts such as major policy changes, coups, revolutions, and wars; long-term environmental changes such as global warming; and depletion of critical natural resources such as fresh water.

• *Competitive risks with medium-term impact.* These include the emergence of disruptive technologies (such as the internet, smartphones, and bar codes) and radical strategic moves by industry players (such as the entry of Amazon into book retailing and Apple into the mobile phone and consumer electronics industries).

Companies use different analytic approaches for each of the sources of external risk.

Tail-risk stress tests. Stress-testing helps companies assess major changes in one or two specific variables whose effects would be major and imme-

The Risk Report Card

VW do Brasil summarizes its strategy risks on a Risk Report Card organized by strategic objectives (excerpt below). Managers can see at a glance how many of the identified risks for each objective are critical and require attention or mitigation. For instance, VW identified 11 risks associated with achieving the goal "Satisfy the customer's expectations." Four of the risks were critical, but that was an improvement over the previous quarter's assessment. Managers can also monitor progress on risk management across the company.

STRATEGIC OBJECTIVE	ASSESSED RISKS	CRITICAL RISKS	TREND
Achieve market share growth	4	1	↔
Satisfy the customer's expectations	11	4	↑
Improve company image	13	1	↔
Develop dealer organization	4	2	↔
Guarantee customer-oriented innovations management	5	2	↓
Achieve launch management efficiency	1	0	↔
Increase direct processes efficiency	4	1	↔
Create and manage a robust production volume strategy	2	1	↓
Guarantee reliable and competitive supplier-to-manufacturer processes	9	3	↔
Develop an attractive and innovative product portfolio	4	2	↓

A firm's ability to weather storms depends on how seriously executives take risk management when the sun is shining and no clouds are on the horizon.

diate, although the exact timing is not forecastable. Financial services firms use stress tests to assess, for example, how an event such as the tripling of oil prices, a large swing in exchange or interest rates, or the default of a major institution or sovereign country would affect trading positions and investments.

The benefits from stress-testing, however, depend critically on the assumptions—which may themselves be biased—about how much the variable in question will change. The tail-risk stress tests of many banks in 2007–2008, for example, assumed a worst-case scenario in which U.S. housing prices leveled off and remained flat for several periods. Very few companies thought to test what would happen if prices began to decline—an excellent example of the tendency to anchor estimates in recent and readily available data. Most companies extrapolated from recent U.S. housing prices, which had gone several decades without a general decline, to develop overly optimistic market assessments.

Scenario planning. This tool is suited for long-range analysis, typically five to 10 years out. Originally developed at Shell Oil in the 1960s, scenario analysis is a systematic process for defining the plausible boundaries of future states of the world. Participants examine political, economic, technological, social, regulatory, and environmental forces and select some number of drivers—typically four—that would have the biggest impact on the company. Some companies explicitly draw on the expertise in their advisory boards to inform them about significant trends, outside the company's and industry's day-to-day focus, that should be considered in their scenarios.

For each of the selected drivers, participants estimate maximum and minimum anticipated values over five to 10 years. Combining the extreme values for each of four drivers leads to 16 scenarios. About half tend to be implausible and are discarded; participants then assess how their firm's strategy would perform in the remaining scenarios. If managers see that their strategy is contingent on a generally optimistic view, they can modify it to accommodate pessimistic scenarios or develop plans for how they would change their strategy should early indicators show an increasing likelihood of events turning against it.

War-gaming. War-gaming assesses a firm's vulnerability to disruptive technologies or changes in competitors' strategies. In a war-game, the company assigns three or four teams the task of devising plausible near-term strategies or actions that existing or potential competitors might adopt during the next one or two years—a shorter time horizon than that of scenario analysis. The teams then meet to examine how clever competitors could attack the company's strategy. The process helps to overcome the bias of leaders to ignore evidence that runs counter to their current beliefs, including the possibility of actions that competitors might take to disrupt their strategy.

Companies have no influence over the likelihood of risk events identified through methods such as tail-risk testing, scenario planning, and war-gaming. But managers can take specific actions to mitigate their impact. Since moral hazard does not arise for nonpreventable events, companies can use insurance or hedging to mitigate some risks, as an airline does when it protects itself against sharp increases in fuel prices by using financial derivatives. Another option is for firms to make investments now to avoid much higher costs later. For instance, a manufacturer with facilities in earthquake-prone areas can increase its construction costs to protect critical facilities against severe quakes. Also, companies exposed to different but comparable risks can cooperate to mitigate them. For example, the IT data centers of a university in North Carolina would be vulnerable to hurricane risk while those of a comparable university on the San Andreas Fault in California would be vulnerable to earthquakes. The likelihood that both disasters would happen on the same day is small enough that the two universities might choose to mitigate their risks by backing up each other's systems every night.

The Leadership Challenge

Managing risk is very different from managing strategy. Risk management focuses on the negative—threats and failures rather than opportunities and successes. It runs exactly counter to the "can do" culture most leadership teams try to foster when implementing strategy. And many leaders have a tendency to discount the future; they're reluctant to spend time and money now to avoid an uncertain future problem that might occur down the road, on someone else's watch. Moreover, mitigating risk typically involves dispersing resources and diversifying investments, just the opposite of the intense focus of a successful strategy. Managers may find it antithetical to their culture to champion processes that identify the risks to the strategies they helped to formulate.

For those reasons, most companies need a separate function to handle strategy- and external-risk management. The risk function's size will vary from company to company, but the group must report directly to the top team. Indeed, nurturing a close relationship with senior leadership will arguably be its most critical task; a company's ability to weather storms depends very much on how seriously executives take their risk-management function when the sun is shining and no clouds are on the horizon.

That was what separated the banks that failed in the financial crisis from those that survived. The failed companies had relegated risk management to a compliance function; their risk managers had limited access to senior management and their boards of directors. Further, executives routinely ignored risk managers' warnings about highly leveraged and concentrated positions. By contrast, Goldman Sachs and JPMorgan Chase, two firms that weathered the financial crisis well, had strong internal risk-management functions and leadership teams that understood and managed the companies' multiple risk exposures. Barry Zubrow, chief risk officer at JP Morgan Chase, told us, "I may have the title, but [CEO] Jamie Dimon is the chief risk officer of the company."

RISK MANAGEMENT is nonintuitive; it runs counter to many individual and organizational biases. Rules and compliance can mitigate some critical risks but not all of them. Active and cost-effective risk management requires managers to think systematically about the multiple categories of risks they face so that they can institute appropriate processes for each. These processes will neutralize their managerial bias of seeing the world as they would like it to be rather than as it actually is or could possibly become. ▼

HBR Reprint R1206B

CARTOON: ROY DELGADO