Managing the Multiple Dimensions of Risk: Part I of a Two-Part Series

By Robert S. Kaplan, Baker Foundation Professor, and Anette Mikes, Assistant Professor, Harvard Business School

Following his 2009 BSR article on risk and the Kaplan-Norton strategy execution framework, Robert Kaplan has conducted, with Anette Mikes, an extensive program of research, case-writing, and teaching on risk management. The two expanded the scope of their study beyond the financial sector and the failures leading to the 2007–2008 global financial crisis. Here, they identify three categories of risk and elaborate on the ways companies can identify and mitigate them, with particular emphasis on strategy execution risks.

All profit and nonprofit enterprises face three different categories of risk. Each has a different degree of controllability—from complete to zero—and each requires a different approach for mitigation and management. (See Figure 1.) These categories build on the work of University of Chicago economist Frank Knight, who defined risk as “measurable uncertainty,” reserving the term “uncertainty” for unmeasurable future events. Former U.S. defense secretary Donald Rumsfeld updated these distinctions when he classified future uncertain events as “known knowns” (“things [that] we know we know”), “known unknowns” (“some things we [know that] we do not know”), and “unknown unknowns” (“the ones we don't know we don't know”).

We believe these are useful distinctions for risk management. Let's start with the risks, which we label as Category I, caused by employees’ unauthorized, illegal, unethical, or inappropriate actions. In general, management knows the actions it wants employees to avoid (they are “known knowns”) and has specific management tools to deter or prevent them from occurring. Ideally, companies want to drive the probability of Category I risks to zero.

Category II risks arise in strategy execution. Organizations voluntarily take on Category II risks so that they can generate high returns from their strategies. Managers can identify Category II risk events (they are “known unknowns”) and can influence both their likelihood and impact. While managers have some ability to reduce the likelihood and impact of Category II risks, they cannot eliminate the probability of their occurrence. Some residual risk, inherent to the strategy, always remains.

continued on the following page

2 F.H. Knight, Risk, Uncertainty, and Profit (Dover Publications, 1921).
Category III risks arise from events outside the company and its strategy and beyond the company’s direct influence or control. Managers cannot estimate their likelihood and, in many cases, are not even aware of such events (they are “unknown unknowns”) or that they could jeopardize the company’s strategy and survival. Managing Category III risks requires a process of “risk envisionment,” in which managers rely less on quantitative risk management and more on their experience, intuition, and imagination to create new mental models about future scenarios and strategic uncertainties. Once Category III risks have been envisioned, managers can brainstorm about how to enhance organizational resilience to withstand the most consequential of them.

In short, management wants to, and generally can, prevent any Category I risk event from occurring; it reduces the likelihood of Category II risks and mitigates their adverse consequences, should they occur, in a cost-effective way; and, finally, it anticipates the most dire consequences of Category III risks by modifying strategies and taking actions to reduce their consequences should they occur.

The power of this multidimensional risk taxonomy arises from the very different management processes, organizational units, and actions put in place to deal with each risk category. The internal audit, a powerful and effective process for managing Category I risks, may be useless for managing Category II and III risks. Conversely, solutions for managing Category II or Category III risks would be inappropriate (or overkill) for managing Category I risks. Organizations must tailor their risk management processes to the inherent nature and controllability of the different categories of risk they face.

### Category I: Risks Arising from Employees’ Undesirable or Unauthorized Actions

Category I risks arise from employees’ failure to perform routine, standardized, or predictable processes. These processes, well understood and documented, are generally not central to executing the firm’s differentiated strategy. But the failure to perform them as specified can expose the firm to substantial loss. Companies implement standardized operating procedures, hoping to drive the probability of many Category I risks essentially to zero. Nevertheless, breakdowns do occur as firms become less diligent in enforcement or induce laxity through forgetfulness and inattention. When such breakdowns occur, companies can experience highly adverse consequences, even threats to their very survival; a well-publicized example is the demise of the public accounting firm Arthur Andersen after it suffered breakdowns in its routine delivery of audit services.

Companies cannot anticipate all the possible circumstances that an employee might encounter, nor can they provide detailed instructions of what should or should not be done in every situation involving a potential conflict of interest. Their first line of defense for preventing Category I risk events is to provide positive guidelines so that all employees understand the company’s goals and values. A well-crafted and -communicated mission statement articulates the organization’s fundamental purpose. The mission should provide a guiding light, a “true north,” for all employees to follow. When a company such as Johnson & Johnson states, in the first sentence of its renowned credo, “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,” it provides clear guidance to all its employees about whose interests should be primary in any situation.

Companies should also clearly articulate the values that guide employee behavior toward stakeholders: the company’s customers, suppliers, fellow employees, communities, and shareholders. Clear value statements help employees avoid decisions and actions that would violate company standards and put the company’s reputation and assets at risk.

---

But companies also need to be explicit about what actions are expressly prohibited. Boundary systems specifically define the limits of acceptable behavior and actions and should clearly spell out, in negative terms, actions that are unacceptable, such as bribery, kickbacks, discrimination, and harassment. Nine of the tenets in two of society’s most important documents—the Ten Commandments and the first ten amendments to the U.S. Constitution (the Bill of Rights)—are written in negative terms to limit the freedom of action by individuals and the central government. Like these two documents, codes of business conduct proscribe behaviors relating to conflicts of interest, antitrust, treatment of trade secrets and confidential information, and unauthorized payments or gifts to government officials and customers’ purchasing agents.

But mission and value statements and boundary systems are, by themselves, insufficient to deter all undesirable behavior. Employees, under the day-to-day pressures of organizational life, must learn to live by them. Managers must translate the “tone at the top” into “tunes in the middle” (and on the front lines). In addition to active communication and training on the organization’s fundamental beliefs, companies must institute strong internal controls, such as the segregation of duties and an active whistle-blowing program, to reduce the incidence of employee misbehavior and the temptations for fraud and abuse. By continually checking employees’ compliance with internal controls and standard operating processes, a strong, capable, and independent internal audit department deters employees from violating the company’s operating procedures and policies, and detects violations when they do occur.

Category II: Risks Associated with Strategy Execution

A company’s strategy describes how it intends to differentiate its offerings from those of competitors by delivering superior value to a targeted group of customers. A strategy requires the company to voluntarily assume some risk. A bank assumes default risk when it extends credit to customers; an electric utility must manage the risks of demand surges and weather-induced outages; a high-technology company risks financial loss when it funds the research and development of a new product platform; a major global retailer faces supplier, reputation, and competitive risk when it decides to enter a country where it has never before operated.

When Category II strategy risks are managed, the goal is not to inhibit innovation. Rather, risk management should strive to identify all potential risks to the strategy, attempt to mitigate and manage the most likely and consequential ones, and then continually monitor the risk exposure the organization has voluntarily accepted. Occasionally, risk management might reveal that the residual risk exposure remains too high, even after the principal risks are mitigated cost-effectively. In that case, the risk management process could influence the company to modify its strategy to a lower risk/return profile.

John Fraser, chief risk officer of Hydro One, the Canadian electric transmission and distribution company, helped his organization implement an effective Category II risk management program. In phase 1 of the program, employees participate in a series of workshops to collectively identify and quantify the principal risks to the company’s strategic objectives. Hydro One’s no-blame culture encourages people to speak up and report deviances, issues, and potential threats that worry them. An anonymous voting technology allows employees to rate on a scale of 1 to 5 the impact of each risk, the strength of existing controls, and the likelihood of occurrence. These judgments are summarized by placing each risk event within a 5x5 risk map. Multiplying the likelihood and impact scores of each risk yields a ranking of the highest-priority risks. The risk map, albeit a simple and subjective tool, effectively facilitates communication and discussion about the focus and direction for Hydro One’s risk-mitigating actions.

In phase 2, Fraser conducts a series of semiannual one-on-one interviews with senior managers to review the corporate risk profile for the CEO’s review. In phase 3, which takes place during the annual planning process, senior executives allocate resources to investment project proposals that have been selected based on their ability to mitigate the company’s principal risks. By tying risk assessments to the investment management process, the process gives business managers an incentive to disclose, and not hide, risks so that they can obtain resources for risk reduction. The mantra is, “If you have no risk, you get no money.” All three phases channel risk information vertically and horizontally throughout the company, enabling executives and employees to have a shared understanding of the company’s risk profile and the high priority it places on continually reducing the residual risks from high-impact events.

The Jet Propulsion Laboratory’s (JPL’s) approach to risk management, described in a Harvard Business School case and BSR article, provides an excellent example of managing risks in highly innovative projects—sending unmanned scientific missions to Mars. Senior systems engineer Gentry Lee described
his challenge in introducing a new risk culture at JPL:

JPL engineers graduate from top schools at the top of their class. They are used to being right in their design and engineering decisions. I have to get them comfortable thinking about all the things that can go wrong. … Innovation, looking forward, is absolutely essential, but innovation needs to be balanced with reflecting backwards, learning from experience about what can go wrong.  

Lee introduced three risk management processes into every project:

1. **Identifying and assessing risks at the beginning and throughout every project.** Risks are summarized on two-dimensional risk maps (similar to those used at Hydro One).

2. **Conducting periodic and rigorous three-day risk review meetings** with an independent risk review board that actively challenges project engineers’ risk assessments.

3. **Establishing explicit risk-based cost and time reserves** (analogous to Hydro One’s “no risk, no resources” policy) to allow problems to be solved during the course of every multiyear project without exceeding the project’s budget or jeopardizing its scheduled launch date.

JPL’s rigorous project risk management processes generate extra costs. But consider the alternative, as exemplified by Boeing and its new 787 Dreamliner. The project incorporates two major innovations. First, much of the design and manufacturing was outsourced so that suppliers would share in the project’s economic risk. Second, more than 50% of the 787 is constructed from light-plastic composites instead of principally from aluminum, whose properties under stress are much better understood.

Inevitably, the well-known Murphy’s Law of engineering has prevailed during the Dreamliner project. Several key suppliers failed to perform as specified, and the composite fabrication process experienced difficulties. To date, Boeing has announced seven separate delays for first shipments and cost overruns in excess of $20 billion.

The well-studied BP Deepwater Horizon disaster illustrates a similar lack of risk anticipation. BP voluntarily took on a risky project to drill through one mile of water to reach oil deposits two miles below the ocean floor. As with sending unmanned missions to distant planets or introducing a radically new aircraft, the potential rewards from success can justify the risks involved. But without adequate risk identification, mitigation, and management, risky projects can lead to disastrous outcomes. For BP, the outcomes included the death of 11 workers, the spill of more than 4 million barrels of oil into the Gulf of Mexico, extensive damage to wildlife and plants, economic disruption for millions, and a price tag that will likely exceed $40 billion. The National Commission’s Report to the President attributed the disaster to a significant management failure that crippled “the ability of individuals involved to identify the risks they faced, and to properly evaluate, communicate, and address them.” The project had fallen behind schedule and gone over budget. An analyst observed, “With the clock ticking, bad decisions went unchecked, warning signs went unheeded, and small lapses compounded.” A high-level investigative panel concluded, “The disaster can be attributed to an organizational culture and incentives that encouraged cost cutting and cutting of corners—that reward workers for doing it faster and cheaper, but not better.”

Ironically, BP considered itself a leader in safety and risk management because of its strict guidelines—for example, forbidding employees from carrying a cup of coffee without a lid or texting while driving. While BP focused on measuring and controlling Category I (employee misbehavior) risks, it invested too little in identifying and mitigating the Category II risks associated with the refinery and deep-water drilling operations central to its strategy.

Risk management is certainly not free and can often be expensive. But forgoing it can be far more expensive. To paraphrase an old TV oil filter commercial, organizations can pay now for risk identification, measurement, and mitigation—or they can pay later. Now is generally cheaper. Boeing, BP, and the financial institutions that failed in 2007 and 2008 learned the high costs of paying later rather than paying now with contemporaneous and effective risk management processes.

**Identifying and Mitigating Category II Strategy Risks**

Strategy maps and their associated Balanced Scorecards, with measures, targets, and strategic initiatives, provide a natural foundation for thinking systematically about how to identify, mitigate, and manage the risks to a company’s strategy. To illustrate, consider a discount airline’s strategic objective to reduce ground turnaround time. Performing well on this process objective is strategic because it contributes directly to the airline’s customer objective for on-time departures and arrivals. It also advances the company’s financial objectives by enabling greater utilization of two of its most expensive resources: airplanes and flight crews. In translating strategy to operations, the
introduce delays into the various sub-
its consequences should it occur. In
or prompt corrective action to mitigate
likelihood of the risk event occurring
also signals the need to take immedi-
to fall short on a strategic objective. It
lead indicators. It heightens manage-
ment's and employees' awareness of
airline's strategic objective “Reduce
ground turnaround time,” ground crew
staff could identify excessive employee
turnover as a risk factor leading to
slow down the work processes but
such as snow or ice, which not only
slow down the work processes but
also require additional work. For each
risk event, employees could devise risk
indicators that signal when the event is
becoming more likely, allowing employ-
ees to react faster to its occurrence.
A key risk indicator (KRI) scorecard, con-
taining risk metrics for every strategic
objective, is the ultimate collection of
lead indicators. It heightens manage-
ment's and employees' awareness of
events that could cause the company to
fall short on a strategic objective. It
also signals the need to take immedi-
ate preventive action to reduce the
likelihood of the risk event occurring
or prompt corrective action to mitigate
its consequences should it occur. In
the case of BP's Deepwater Horizon ac-
cident, multiple indicators were flashing
warning signs to the drilling rig's crew
about potential problems: gas bubbles
appearing when they shouldn't have,
crude not sealing the wellhead as
expected, instruments going out of
service or signaling adverse readings
and unusual conditions. However, rather
than respond immediately to the risk indi-
cators, the crew—neither trained nor
empowered to take immediate action,
and under intense pressure to complete
the well—forbore ahead.
A Balanced Scorecard's metrics guide a
company forward in its journey toward
achieving strategic objectives. KRIs are
different; they help predict the
events that could impede or reverse the
company's progress in reaching its
strategic destination. The absence of risk
events does not advance the strategy,
that is the role of BSC metrics and dash-
board KPIs. But as the strategy is driven
forward, the sudden emergence of a risk
event can stop the company in its tracks.
So the company must simultaneously
improve its operational KPIs and BSC
strategic metrics while being ever alert
to the early warning from an uptick in a
KRI, which signals the increased likely-
hood of an imminent risk event. A good
KRI scorecard enables and empowers
employees to respond immediately to
reduce the likelihood of consequences of
the risk event.
Consider the example of Infosys, the
leading India-based information technol-
yogy (IT) services provider, whose strategy
is to partner with the largest organiza-
tions in the world and help them create
new value through innovative IT solu-
tions. A customer metric on Infosys's BSC
counts the number of clients with more
than, say, $50 million in annual revenues,
and a financial metric shows annual
percentage increases in revenues from
such clients. Infosys recognized that a
client default would be a key risk event
from this large-client-focused strategy.
(Previously, when its business was based
on a large number of small clients, a
default of any one would not jeopardize
the strategy.) Infosys therefore created
a risk indicator based on the credit
default swap rates of every large client.
Increases in the market's assessment
of a client's likelihood of default would
lead Infosys to take actions to reduce
the likelihood or impact of the client
defaulting on its account payable. Again,
avoiding defaults will not drive Infosys's
strategy forward; that is the role of BSC
metrics and dashboard KPIs. But having
several large clients default would put
the entire strategy at risk.
An enterprise can also invest in initia-
tives that reduce the likelihood and con-
sequences of a risk event. Risk review
meetings focused on the key risk events
associated with strategy map objectives
enable employees to suggest risk mitiga-
tion initiatives and projects. The funded
initiatives should address the risk events
that are in the yellow and red zones
of each objective's risk (or heat) map.
Green-zone risks (those with a low likeli-
hood and impact, if they occurred) can
be tolerated. Employees and managers
should search for cost-efficient initia-
tives to reduce the likelihood or mitigate
the consequences of risk events that fall
in the yellow and red zones.
For example, a top research university
located in North Carolina might identify
the risk from a major hurricane to its
local IT system and data centers. Simi-
larly, a comparable research university
located on the San Andreas Fault in Cali-
ifornia might identify the risk to its IT
and data centers from a severe earthquake.
The likelihood of a hurricane sweeping
in from the Atlantic Ocean on the same
day that a major earthquake occurs in
California might be considered suffi-
ciently small (a true "black swan" event)
that the two universities could agree
to back up each other's complete data
and information systems every night. As
with any risk mitigation initiative, each
university would pay a cost every day to
protect itself against an event that nei-
ther one might experience for 100 years.
But both prefer to pay a little more each
day than to bear all the costs of losing data and information from a rare, but not unfeasible, event that would put their research and education strategies at risk.

A company does not have to manage all its strategic risks by itself. Financial markets and insurance may provide better ways to mitigate the adverse consequences of risk events outside the company’s control. For example, the discount airline’s low-cost strategy could be jeopardized by significant increases in jet fuel prices. Since the price of jet fuel is beyond the airline’s control, the airline gains no comparative advantage in managing this risk internally. Futures markets enable the airline to offload some or all of its fuel-cost risks to those better able and willing to take it on for a price. In general, a company will find that it should manage internally only those risks for which it has superior information and better means of control than an external insurer or investor (or speculator).

A strategy map, Balanced Scorecard, and operational dashboards provide the tangible road map to guide the company in its strategy implementation journey. Risk management is different. It focuses on learning about and overcoming the hurdles that the strategy may encounter along the way. Its role is to reduce the obstacles and barriers that could prevent the organization from reaching its strategic destination.

**Category III: Risks from Uncertain, Uncontrollable External Events**

Category III risks arise from events outside the company—those beyond its ability to influence or control, and not obviously related to its strategy. The events triggering a Category III risk could originate from physical forces, such as climate change, or geologic forces, such as the earthquake and tsunami that shut down Japanese suppliers’ production for weeks or the volcanic eruption that shut down European airspace. Category III risks can arise from geopolitical events such as insurrections and wars, or from pandemics, droughts, or supply restrictions of key raw materials or energy. Some risks arise from unexpected governmental actions to restrict immigration, impose new regulations, limit imports, subsidize exports, or raise taxes. Still others result from unforeseen economic developments such as recessions, inflation, or major currency price movements. These risks may have little direct connection to a company’s strategy, but since every company operates in the real world, any major change in the world could adversely affect its ability to achieve its strategic objectives.

Companies may fail entirely if they neglect to assess and mitigate the losses from Category III “unknown unknowns.” They need to consider what unlikely event or combination of unlikely events could lead to their demise. Some companies force an active discussion of unlikely events and their consequences. Goldman Sachs and JP Morgan Chase hold regular “tail risk” meetings in which a senior manager leads a discussion of an unlikely event, such as a tripling of energy prices, a devaluation of the U.S. dollar, a civil insurrection in China, a devastating earthquake or hurricane in a sensitive region, or war in the Middle East.

Since the likelihood of Category III “uncertain” events is unknown, and perhaps unknowable, traditional risk maps are of little use. Companies need other risk management tools to identify and address the most consequential Category III risks.

Scenario planning, war gaming, and tail-risk stress-testing meetings enable business leaders to learn about the sensitivity of their strategy to events that occur outside their control. From evolutionary biology, we learn that species that have become too specialized and successful in the existing environment may not have the requisite variety to survive major changes to that environment. The discussions around Category III uncertainties help the leadership team determine whether the company’s strategy has sufficient requisite variety to survive the disruptions that might occur from unusual, potentially catastrophic events in its economic, regulatory, competitive, and physical environments.

Editor’s Note: In Part II (appearing in the September–October 2011 BSR), the authors will explore the concept of an Office of Risk Management (modeled after the Office of Strategy Management), along with a case study of an innovative risk management function at JP Morgan Chase Private Bank. They will also look at the “softer” components of risk management, including a survey of different risk management cultures and a comparison of two different but equally effective risk officers’ personalities and roles.