McKinsey Working Papers on Risk, Number 18




A Board Perspective on Enterprise Risk Management

André Brodeur
Kevin Buehler
Michael Patsalos-Fox
Martin Pergler

February 2010

Contents

McKinsey Working Papers on Risk presents McKinsey's best current thinking on risk and risk management. The papers represent a broad range of views, both sector-specific and cross-cutting, and are intended to encourage discussion internally and externally. Working papers may be republished through other internal or external channels. Please address correspondence to the managing editor, Rob McNish (rob_mcnish@mckinsey.com)

A Board Perspective on Enterprise Risk Management

The recent economic crisis has clearly demonstrated that many companies were inadequately prepared to deal with major risks. Although the lack of preparation was most visible among financial institutions, companies from all sectors were hit by unexpected events such as drops in product demand, declines in commodity prices, wild swings in currency exchange rates, and a broad liquidity crunch.

Some of the shortfall in preparation, but only some, can be explained by the inevitable challenges of responding to a "black swan" event. While financial firms are struggling to understand how their risk systems failed, at nonfinancial companies there is a growing sense that their oversight of risks is superficial and their risk management activities are not well integrated in the company's management system. They suspect that their business activities may hide continued vulnerabilities that will manifest themselves in the next risk storm.

At the height of the crisis, many companies had to cancel plans, making rapid and painful tradeoffs to ensure their immediate survival. Now, as the tide seems to be turning, these companies are resuming their long-term strategies. With the benefit of lessons learned, hopefully they will be better prepared for the next shock, whenever it comes and whatever the cause.

In this paper we share our some of those lessons and our observations on best practices in enterprise risk management (ERM) from a board perspective. And we highlight 12 specific actions related to ERM that all boards should consider taking to lift their company to the highest standards of risk management.

Risk and the board

Boards play a crucial role in risk oversight. Directors at corporations are encouraged to embrace entrepreneurial risks and pursue risk-bearing strategic opportunities.[1] In most common-law jurisdictions (including most of the English-speaking world), directors do so under the protection of the business judgment rule, which is the legal foundation of risk undertaking. With the rule, however, comes an obligation for due diligence which implies the responsibility to understand thoroughly the company's risks. Because of this, it is widely recognized that corporate directors are responsible for reviewing and approving the company's ERM program.

Our view is that boards must go a step further, and ensure that their company's ERM capabilities are at the level of best practices and are well adapted to the company's business culture and the nature of the risks it faces. We argue that best practices are needed in all five dimensions of ERM[2] (Exhibit 1):

- Risk transparency and insight
- Risk appetite and strategy
- Risk-related business processes and decisions
- Risk organization and governance
- Risk culture

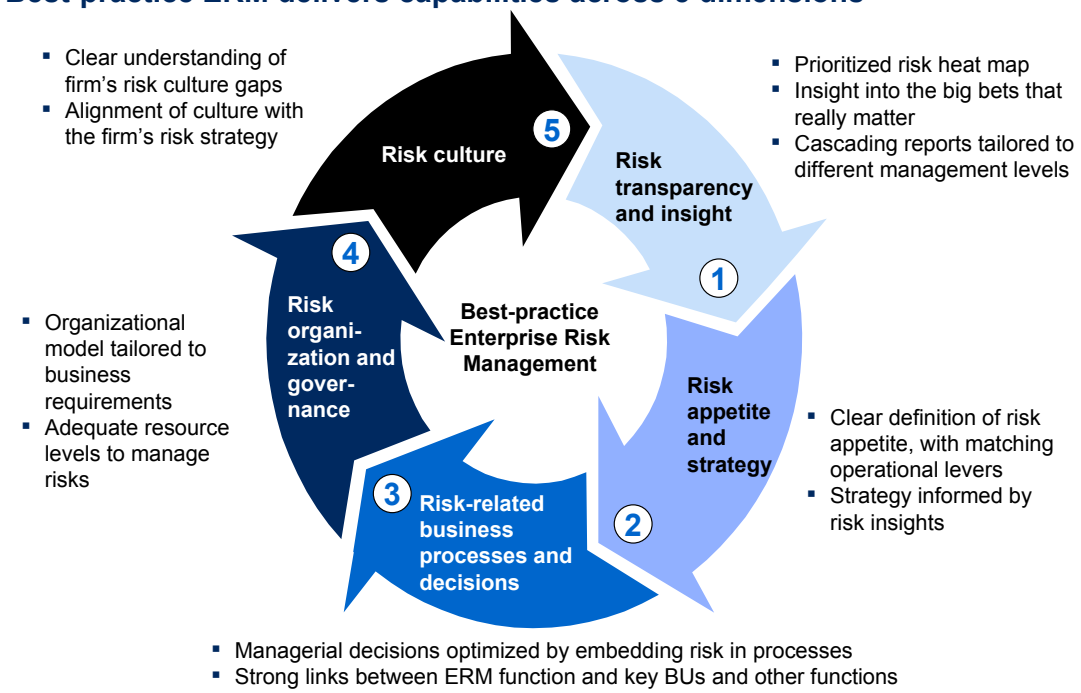
1 Matteo Tonello, "Corporate Governance Handbook: Legal Standards and Board Practices (Third Edition)," The Conference Board, 2009, page 14.

2 For more on the five dimensions of enterprise risk management, see Kevin Buehler, Andrew Freeman, and Ron Hulme, "Owning the right risks," *Harvard Business Review*, September 2008.

We will examine each of the five dimensions in turn and highlight the recommended actions in each.

Exhibit 1

Best-practice ERM delivers capabilities across 5 dimensions



Source: McKinsey

Risk transparency and insight

Many companies have—and had, well before the crisis—risk identification processes to identify, consolidate, and prioritize the risks facing the company. At least once a year, they generate a risk report, listing 20 or more important risks with at least a qualitative assessment of the probability and impact of each.

Why did these risk processes not raise the alarm during the crisis? We see three reasons. These risk assessments often miss large company-wide risks; they do not uncover the fundamental drivers of the large risks identified; and they fail to consider how multiple risks can operate in tandem. As a result, such processes fail to generate insight that management or boards can act on.

A strong risk identification process casts a broad net that captures all key risks and then drills down within the major risks to understand root causes. It should have three elements: a "heat map," an exercise to identify the company's "big bets," and a risk reporting system that delivers consistent and insightful information.

Prioritized risk heat map

Most companies have some sort of heat map that lists and classifies risks by potential impact and likelihood. While this is a good start, many heat maps would be improved and their focus on the most important risks strengthened by adopting the three following practices:

Ensure adequate risk impact estimation. When it comes to identifying key risks, many companies choose to look merely at high-level sensitivities on the balance sheet or income statement. This is insufficient. For instance, say a company wants to understand its exposure to the dollar/euro exchange rate. Getting to the answer requires more than looking at the currency in which it records its sales, or the currency of the instruments on its balance sheet. The analysis needs to include such counterintuitive considerations as the currencies that determine raw material prices and suppliers' costs, and the terms of supply contracts regarding risk pass-through. The analysis also needs to identify the drivers of pricing dynamics in different markets—for instance, the possibility that a change in exchange rates will allow a foreign company to become the price setter, thereby giving them a competitive advantage. Some of these effects can be negligible under short-term, business-as-usual conditions, but can become the dominant risk drivers in times, like the present, of rapid economic change.[3]

Ensure coherence and calibration across businesses. Many risk heat maps are built from the bottom up, with each business unit naming and classifying risks in its own way. Someone in the corporate center then aggregates these business unit maps into one company-wide map, in which risks that are obviously of the same type are aggregated. But business units may use different names for the same risk or for very similar ones. When these risks are not added together, the company's big risk might be missed. Another common issue is the calibration of different types of risk. How for example should a company quantify the impact of damage to its reputation, and how should that risk be calibrated against the impact of currency hedge losses? The task of developing a consistent and transparent view—across different business units and seemingly different risks—is an important one that requires significant effort and insight into the business.

Look beyond likelihood and impact. While the likelihood (or frequency, or probability) of potential risks and their estimated impact is important, it is not the whole story. Also important are preparedness (how ready is the company to respond to the risk if it occurs?) and lead time (how far ahead can the company see the risk event coming?). Many simple risk heat maps continually highlight the high-likelihood, high-impact risks that everyone recognizes, but fail to support management and board discussion about the company's preparedness to respond and its proper appreciation of early-warning signals.

Insight into the big bets

As just mentioned, the risks identified as "high priority" by many companies are often self-evident, along the lines of "if market demand evaporates or a major supply disruption occurs, unfortunate results will follow." A far more useful exercise for boards and top management is to identify the three to five "big bets" the company depends on. These may not be obvious. For example, the performance of a maker of regional aircraft is of course dependent on global macroeconomic growth. A stronger insight, though, is to note its dependence on the health of those few airlines that are pursuing a point-to-point business model, and its implicit bet on high fuel prices that would accelerate demand for more fuel-efficient jets to replace older, fuel-guzzling but still safe clunkers. This bet on high fuel prices is compounded by the fact that the source of much of the world's demand for business jets, the Middle East and Russia, have economies that are strongly correlated to prices for crude oil and refined products, including jet fuel.

What are your big bets? Does the board understand them and is it comfortable with them?

3 For more on this topic, see Eric Lamarre and Martin Pergler, "Risk: Seeing around the corners," mckinseyquarterly.com, October 2009

Risk reports

Risk transparency at the board level is ultimately only possible where a risk reporting process produces insightful and well-synthesized board-level risk reports.

One common challenge is that management does not actually understand the expectations of the board with respect to risk reports. In part this is because most executives do not have the benefit of experience as a board director. Also, many executives do not realize that the board needs a full understanding of the company's risks in order to fulfill its fiduciary duty.

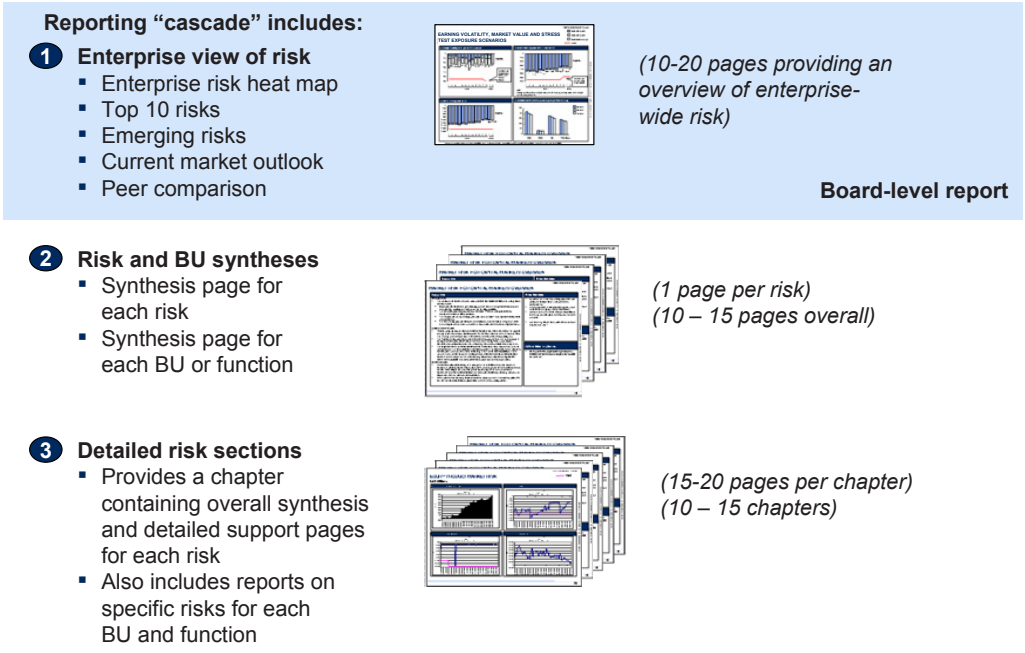
The design of risk reports for the board begins with a clear understanding of the information they should contain and the board actions that the information might prompt. What risks does the board need to understand? How often does it need to review them? What should be reviewed by the various committees (e.g., finance, audit, risk, human resources, compensation)? And for what purpose is management asking the board to consider these risks?

The board's risk report should prioritize key risks and include management's assessment of those risks—i.e., it should provide a transparent description of the tradeoffs involved, management's decision, and the business rationale. Finally, the board report should be part of an integrated system, in which business unit reports are aggregated into a company-level risk report, and management information flow and reporting are consistent with board reporting (Exhibit 2).

Exhibit 2

An integrated system of risk reports

CASE EXAMPLE



Source: McKinsey

Risk appetite and strategy

One would expect that companies, which are inherently risk takers, would clearly articulate how much risk they are comfortable taking, what kind of risk they are willing to take, and how they expect to profit from those risks. However, most boards and management teams have only a vague idea of their actual appetite for risk and their overall risk strategy. This leaves value on the table in the best of times and in times of economic discontinuity may lead to dismal surprises.

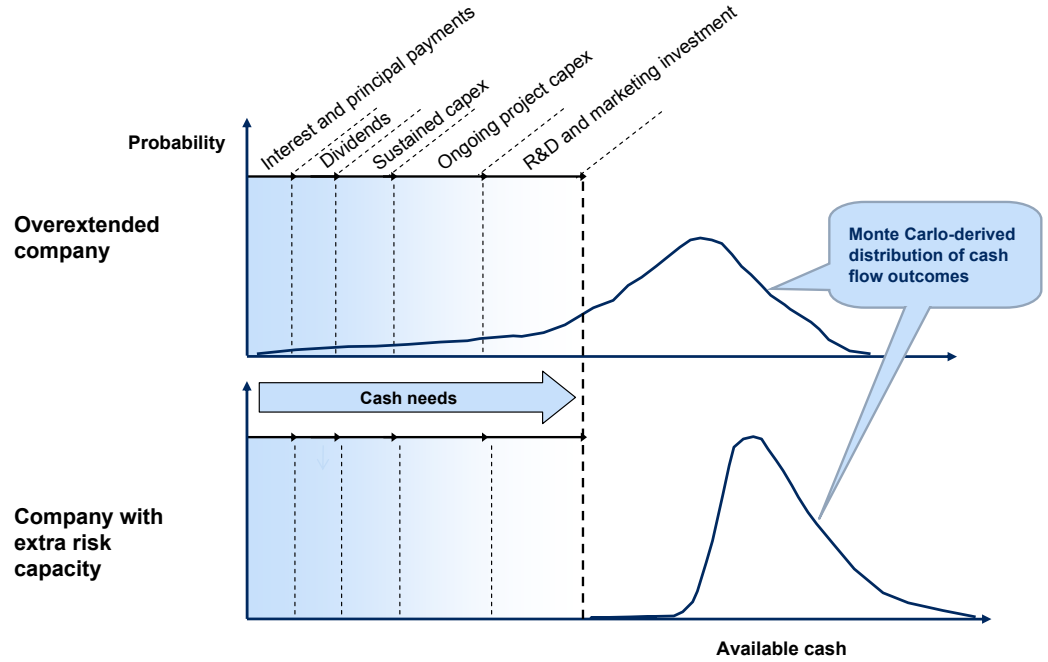
Risk appetite

Determining a company's risk appetite starts by first assessing its risk capacity. By risk capacity we mean the company's ability to withstand risk when it materializes into actuality, while avoiding unwanted effects such as canceled projects, postponed maintenance, damage to the company's reputation, rating downgrades, and of course default and insolvency. Once such constraints are quantified, the board is able to determine how much of that capacity the company should expend (i.e., how much risk it should assume), and how much of a cushion should be kept.

The best approach to assessing risk capacity depends on the nature of the business and its risk profile. For instance, in the case of companies whose key exposures are commodity prices, currencies, and other "data-rich" risk factors, risk capacity can be assessed with a Monte Carlo model that produces a cash flow-at-risk analysis. Exhibit 3 presents such an analysis.

Exhibit 3

Assessing risk capacity using Monte Carlo simulations



Source: McKinsey

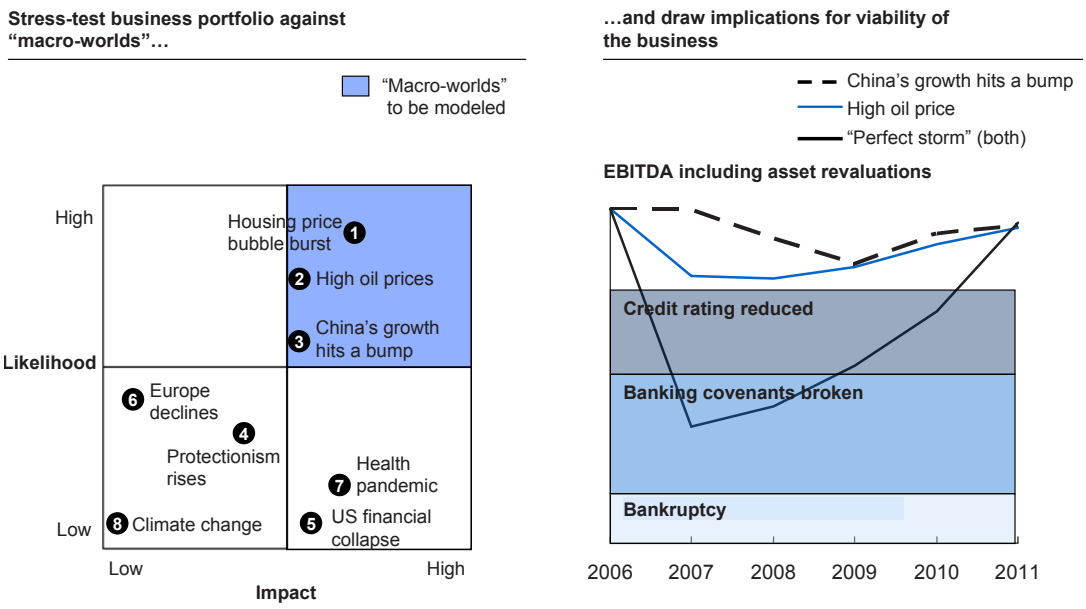
Any point on the curve represents the company's cash flow from a single iteration of the model as it assigns values to the range of scenarios and assumptions with which it has been programmed. The curve is developed from thousands of these iterations. This distribution of potential cash flows is then compared to prioritized cash needs, represented as blocks ranging from most essential (left) to least essential (right). In the top example, there is a significant likelihood that cash needs will not be met; this company's risk capacity is quite low. Unless capital can be sourced elsewhere, this company should reduce its risk appetite. In the bottom example, the company could likely take on more risk and generate more returns without affecting its ability to cover its cash needs; its appetite for risk could be set higher than what it is today.

For other companies, a Monte Carlo approach may not be useful. Instead they can calculate cash flows using a small number of discrete scenarios that describe all the effects that might result from a given event—what one might call a "macro-world." Exhibit 4 shows a number of these macro-worlds for a multinational real estate firm, whose principal risks were associated with major macroeconomic shifts that could erode property prices in Asia and the Middle East, the company's main markets. The company must carefully think through all the second- and third-order effects that might come to pass in a given scenario. To take another example, in a scenario in which commodity prices rise sharply, companies should generally incorporate a rising Australian dollar, given the currency's strong correlation with commodity prices. (For more on scenario planning of this kind, see "Business scenario planning—getting it right" on page 7.)

Exhibit 4

Assessing risk capacity using discrete scenarios

REAL ESTATE EXAMPLE



Source: McKinsey

Once the most threatening scenarios have been identified, they are used to produce a simulation of future EBITDA, as shown at right. The board has to decide whether it is comfortable with breaking bank covenants under a "perfect storm" scenario. If not, risk appetite should be lowered.

Risk ownership and strategy

Risk-taking is an integral part of business activities. The risk appetite defines how much risk the company will take on overall. It then needs to decide which risks it makes sense to embrace. These will primarily be those risks the company "owns," i.e. those risks which it is equipped to manage and exploit competitively. The company also needs to decide which risks to mitigate (e.g., to minimize via managerial actions), to transfer out (e.g., to insure) and to reject (e.g., which businesses to exit on the basis of risk exposure).

For instance, a metal producer faced the choice of either remaining fully exposed to the metal price or hedging it. It believed it had superior insight into the supply and demand dynamics of its market and chose to place only occasional and partial hedges, depending on its views of the direction of future prices. Another metal producer, acknowledging it had no real information advantage, preferred to fully hedge the metal price and offer its shareholders the risk profile of an industrial company rather than that of a commodity producer. In another instance, a paper producer realized that its competitive position depended almost entirely on currency exchange rates. It chose to hedge all of its currency exposure at a time when the rate was deemed "good," in order to focus management on the critical challenge of improving the company's cost position. Similarly, a leading airline decided that it was not the natural owner of risks of price changes in jet fuel, and hedged these away. This proved to be critical when oil prices took off in 2006.

Business scenario planning – getting it right

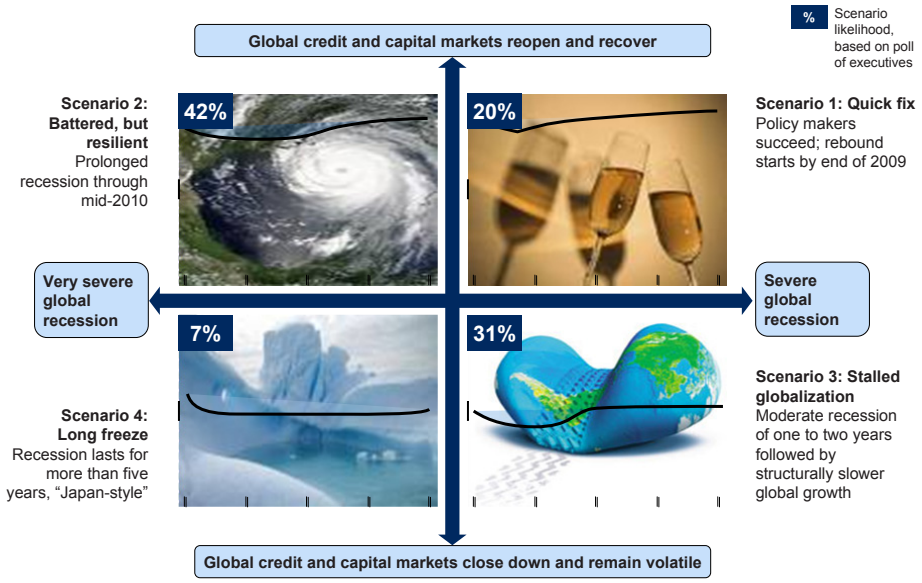
Many companies say they do scenario planning. What this typically means, unfortunately, is that each business leader develops the same unimaginative scenarios: a base case, an upside scenario, and a downside scenario. The assumptions behind these cases are often unclear and inconsistent, both in specifics (e.g. exactly which forward rates were used for currency risk) and in spirit: one manager's downside is a one-chance-in-a-million situation, while for another it is what she secretly already knows or suspects is most likely to happen. Because of these inconsistencies between businesses, it becomes impossible to draw conclusions for the enterprise.

By contrast, good scenario planning starts with consistent assumptions on core economic drivers. It may be impossible to decide exactly how likely these assumptions are, but they should at least describe a plausible situation. Examples of such scenarios are McKinsey's four post-crisis macroeconomic scenarios. Exhibit A presents an overview of these, and Exhibit B contains more detailed descriptions. These scenarios reflect differences in two crucial variables that will have much to say about how the world economy recovers.

Good business scenarios then take these core assumptions and derive implications for business-specific drivers such as product demand, factor costs, financial variables, and the like. These additional assumptions are documented and discussed. Only in scenarios planned in this way are results aggregated across business units meaningful.

Exhibit A

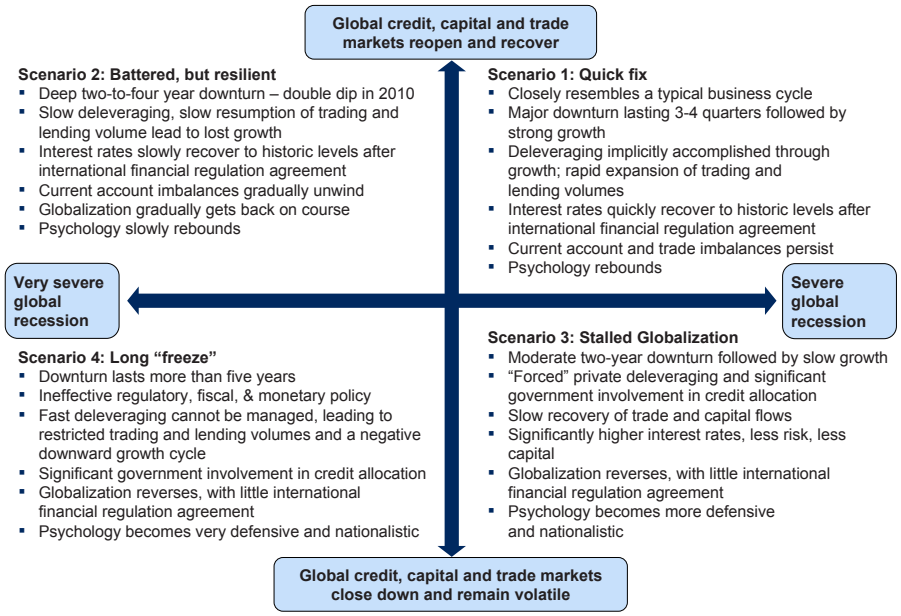
Overview of the four McKinsey macroeconomic scenarios



Sources: McKinsey Global Institute; McKinsey's Center for Managing Uncertainty; McKinsey Quarterly Executive Survey (November 2009)

Exhibit B

Description of the four scenarios



Sources: McKinsey Global Institute; McKinsey's Center for Managing Uncertainty

Discussions about risk appetite and natural ownership culminate in the definition of an explicit risk strategy (or risk policy)—an agreed-upon statement of the risks the company will seek to take on, and those it will pass on to others. The board should be instrumental in defining and validating such a statement. Such a statement should be embedded in the company's strategic plan, and it can be shared with shareholders and other stakeholders. Exhibit 5 shows a number of examples of such statements from companies leading the charge in this area.

Exhibit 5

Company risk appetite and strategy statements - examples

	Risk appetite and strategy statements
Leading engine manufacturer	▪ "[our risk systems are] … designed to manage, rather than eliminate, the risk of failure to achieve business objectives" ▪ Risk levels will be set to target a credit rating of 'A'
Leading high-technology manufacturer and service provider	▪ "We have evaluated our exposure to changes in FX, interest rates and commodity prices … using a value-at-risk analysis" ▪ "As part of our growth strategy, we invest in businesses in certain countries that carry high levels of currency, political and/or economic risk, such as Argentina, Brazil, China, India, Russia, and South Africa" ▪ "Investment in any one of these countries has been limited to 4 percent of consolidated shareowners' equity"
Global metals producer	▪ "[We] …manage risk through… diversity of the portfolio" ▪ "[We] … only hedge when residual risk in the portfolio may compromise corporate objectives" ▪ "Portfolio risk [is] managed within approved limits"
Low-cost airline	▪ Determined it was natural owner of operational risks but not fuel-price risks ▪ Hedged fuel prices and focused on maximizing value from operational excellence
Top energy utility	▪ Defined appetite to regain exposure to wholesale power prices; restructured company and unwound hedges to enable this ▪ Updated risk appetite for this and other core risks with higher limits to increase potential returns

Sources: Company annual reports and websites

Risk-related processes and decisions

Good risk management needs to go well beyond the narrow confines of the core risk process. Indeed, risk and return tradeoffs are integral to a wide range of business processes. In this paper we highlight three core processes where risk considerations need to be integrated and where the board plays a key role: strategic planning, capital allocation, and financing.

Strategic planning

Too often, risk management and strategic planning operate in parallel but with little connection. Typically, strategic planning makes assumptions about the businesses, and risk management then explores the uncertainties of these assumptions during implementation. But if strategists do not think carefully and comprehensively about the risks that might be encountered in their plans, then much risk will be missed, more than any after-the-fact management approach can mitigate. The strategic planning process must be grounded in risk transparency and insight, and strategic choices must be made consistent with risk appetite.

For a strategic planning process to dovetail well with risk management it should raise questions such as: What assumptions about the "big bets" of the business are we including, perhaps unconsciously, in the strategic plan? Who has assessed the risks to the plan as it is being prepared? Has the plan been stress-tested with integrated economic scenarios as it was being prepared? Can those risks that the company does not want to own be transferred or mitigated on acceptable terms? Is the ambition for the risk/return tradeoff appropriate?

Capital allocation

The capital allocation process is the mechanism by which management (and the board) gives its blessing to parts of the company to take on certain risks in the search for return. All investment decisions typically include important tradeoffs between risk, return, and flexibility. Are they being properly identified and considered? Are the investment choices the company makes consistent with its risk strategy? What is the impact of these investments on risk capacity? Is the company capable of responding to key downside risks—and can it respond flexibly to upside opportunities?

Risk resilience can be an important catalyst for crucial decisions, no matter what process is used for capital allocation. For instance, the risk of becoming uncompetitive versus lower-cost competitors should currency exchange rates or other macroeconomic fundamentals change may bolster the business case for a major shift in the manufacturing "footprint" or the supply chain. To be sure, such a change can invoke new risks, such as faulty execution—will the anticipated cost benefits be captured, and will quality be maintained? But the benefits of greater resilience may well outweigh these concerns. A global or more diversified footprint may give a company more choices (for instance, about where to manufacture what product) that can be optimized on the fly to profit from volatility in economic conditions.

Financing

The decision to take on long-term debt or otherwise change the capital structure (as well, of course, as any M&A activity) has important implications for risk capacity. The cash needs of Exhibit 3 and the thresholds shown at right in Exhibit 4 are dependent on the financial structure of the company. Other financial or treasury operations may also change the picture. For instance, hedging currency or commodity price exposures may, by locking in favorable economics and reducing cash flow volatility, support a capital structure that would otherwise be hard to sustain. However, hedging decisions may also impose new demands on cash flow, such as the need to post collateral for the hedges. Is the board considering these risk ramifications—and is the information provided to the board by management sufficient for the board to understand them?

Risk organization and governance

As mentioned, risk oversight is one of the core responsibilities of boards. The best boards have all their members take responsibility for risk oversight. As should be evident from the foregoing, they interact directly with management on risk matters. And they ensure that the company has an ERM organizational model that is optimized for the kinds of risk a company encounters and the work entailed in reporting on, evaluating, and deciding to accept or mitigate risks.

Board responsibility for risk oversight

Within the board, where does responsibility for risk oversight lay? At many companies, directors will say it rests with the board's audit committee. This is likely a mistake, and might result from a deep-seated underestimation of the value and importance of risk oversight to the company's performance and health. It could also result from

a too-casual working definition of risk, leading directors to confuse the audit committee's compliance-related approach to risk with a true ERM approach. [4]

By contrast, the best-performing boards involve all their directors in the evaluation of risks and they do so at least semiannually during a full-board, dedicated discussion of risk. To be sure, at some companies and in some circumstances a separate risk committee can be useful, to ensure that risk is given proper attention. But at the end of the day, risk oversight remains the full board's responsibility.

To prosecute that responsibility well, the board must have the right composition. For instance, having a mix of backgrounds ensures a variety of perspectives on risk issues. Equally important is a board culture that promotes dialogue and constructive challenge.

Board-management interaction

To gain a thorough understanding of the company's risks, the board needs to interact with the managers who know the risks best. Increasingly, directors are interacting directly with senior executives (line management and risk officers) to get insights into risk, as opposed to relying merely on the reports of the CEO or CFO.

Risk-minded directors tend to favor a risk dialogue centered on specific business issues, rather than a discussion of high-level generalities about risk. They also dislike rigid and bureaucratic risk processes. They identify the handful of executives who have the best perspectives on the company's key risks, and then ensure that the board interacts with them directly.

Organization of the ERM function

An ERM organizational model can take a number of forms, depending on the nature of the business, its risks, and the mandate the ERM function is given.

For instance, an asset management firm needing to optimize risk and return on portfolio investments created a risk function with a chief risk officer reporting directly to the CEO. Within the risk group it employed 50 people assigned to different risks (e.g., market, credit, liquidity, counterparty, operational) and asset classes (e.g., equities, bonds, private equity, real estate). This team is required to perform four functions: analyze financial data, produce risk-return reports, lead an enterprise-wide risk-return dialogue at all levels from portfolio managers to the board, and exert risk control, including adherence to risk limits.

The ERM organizational model for a basic materials company would likely be entirely different. One such company, needing to optimize its exposure to commodity prices, project risks, and operational risks, chose to implement ERM as a "pillar" of its management system and created a small risk function within the finance function. This group has five activities: (i) drive an enterprise-wide process to aggregate risk exposures, produce risk reports, and establish mitigation plans; (ii) measure net exposures to commodities and currencies (i.e., net long and short positions in the supply chain and in trading books) and recommend hedging strategies to the head trader; (iii) exert risk control to ensure risk guidelines and policies approved by the board are applied; (iv) inject risk thinking into the three critical management processes (strategic planning, capital allocation, and financing); and (v) lead an enterprise-wide risk dialogue by initiating risk discussions in a variety of forums. To ensure that the risk group gets "traction" with the company's core business, it appointed "risk champions" in each of the businesses and functions, with a "dotted-line" reporting relationship into the central risk team.

4 See André Brodeur and Gunnar Pritsch, "Making risk management a value-adding function in the boardroom," *McKinsey Working Papers on Risk*, No. 2, 2008.

A common difficulty in setting up an ERM function is that the business units and functions usually manage risk already. They are in fact in the best position to do so, because they know the business best. It is therefore important to conceive an ERM model that will capitalize on existing knowledge and practices, while adding a layer of value by developing an integrated view of risks, harmonizing and calibrating practices across the company, and providing "checks and balances" by creating a risk dialogue in multiple forums across the organization.

In any case, no matter what model is chosen, the basic principles listed in Exhibit 6 should apply.

Exhibit 6

Principles for designing a best-practice risk management organization

1. Strong and visible commitment from all members of the top team
2. Central oversight of risk management across the enterprise (including subsidiaries and corporate functions)
3. Separation of duties between policy setting, monitoring, and control on the one hand; and risk origination and risk management execution on the other
4. Clearly defined accountability
5. Risk appetite and strategy clearly defined by top management (and the board)
6. Full ownership of risk and risk management at business-unit level
7. Business units formally involved and view risk function as a thought partner
8. Robust risk management processes reinforce organizational design (e.g., incentive systems incorporate risk-return considerations)

Source: McKinsey

Risk culture

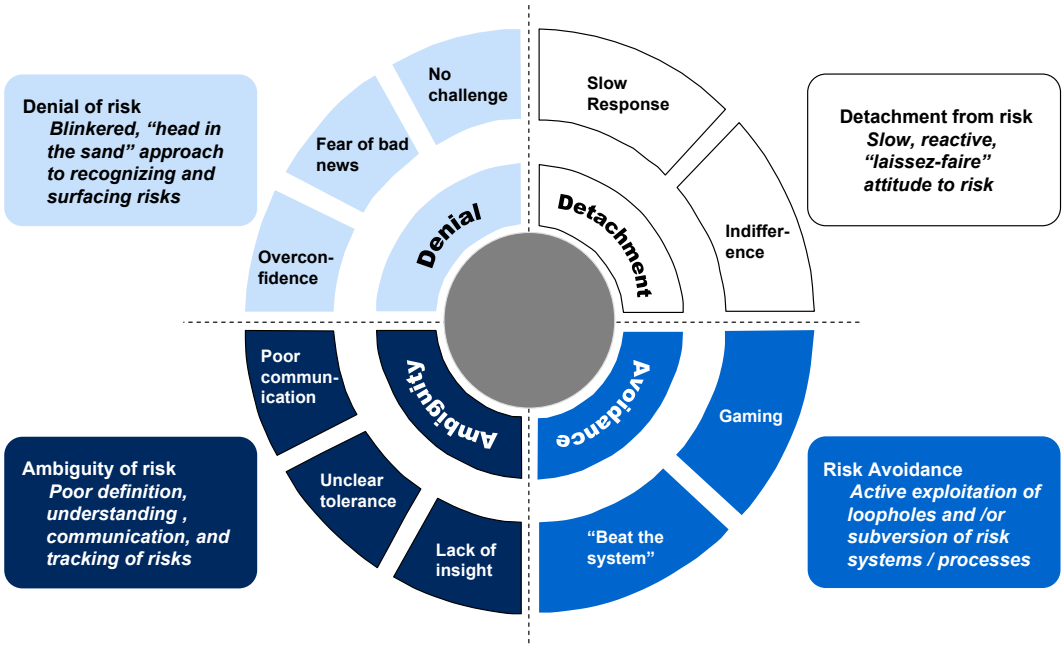
Almost all agree that failures in risk culture were a main cause of the credit crisis of 2008. In fact, it is altogether too easy for human beings to fall into several behavioral traps that lead to poor decision-making in situations where risk and reward have to be weighted (Exhibit 7)[5] . Such behaviors can become a threat to an organization when they become the norm—that is, when they become engrained in the company's risk culture.

We define "risk culture" as the norms of behavior for individuals and groups within a company that determine the collective willingness to accept or take risk, and the ability to identify, understand, discuss, and act on the organization's risks. Such norms can be difficult to determine, of course. The best way to establish the true condition of a company's risk culture is to conduct a cultural survey with a sample of the organization, complemented by a series of structured interviews.

5 For more on risk culture, see Eric Lamarre, Cindy Levy, and James Twining, "Taking Control of Organizational Risk Culture," *McKinsey Working Papers on Risk*, No. 16, January 2010

Exhibit 7

Flaws in risk culture



Source: McKinsey

Once a diagnostic of this sort is completed, management may decide to work on changing the company's risk culture. Most of the tools of cultural influence fall into four categories, all of which should usually be used to effect sustainable change in an organization:

1. Fostering understanding and conviction. *"I know what kind of risk management is expected of me—it is meaningful and I agree with it."* Actions may include post-mortems such as incident reviews and lessons learned sessions, to understand what went wrong in both risk errors and near misses; discussions to explore potential emerging risks; and a well communicated aspiration to reach risk culture excellence.

2. Role modeling. *"I see superiors, peers, and subordinates behaving in the new way with respect to risk."* Actions may include public statements to set market standards for professional behavior and senior executives visibly including risk considerations in decision making.

3. Developing talent and skills. *"I have the skills and competencies to behave in the new way with respect to risk."* Actions may include conducting tailored training and education workshops on risk for senior management.

4. Reinforcing with formal mechanisms. *"The structures, processes, and systems reinforce the change in risk-related behavior I am being asked to make."* Actions may include reinforcing escalation processes and formally including risk dimensions in performance evaluation and compensation.

Compensation is another important driver of culture, and one over which the board has direct influence. In general, the structure of compensation structure and its components do not take into account the risks that were taken to generate a given performance. In many cases, the metrics are short-term, for instance only one year's divisional EBIT. The wrong metric can promote unhealthy approaches that promote one unit of a company at the expense

of the whole. A chief purchasing officer whose compensation is based solely on year-over-year average cost decreases can hardly be expected to make good risk decisions for the company in his contract negotiations.

We believe executive compensation should embed the notion that a dollar of profit generated by low-risk business activities is, in a very real sense, "worth" more to shareholders than a dollar of profit generated by high-risk activities. In light of the crisis, directors should ask themselves whether their company has analyzed its management compensation structure and checked that it is aligned with both the desired risk culture and the risk strategy, especially with respect to key risks.

Twelve board actions to strengthen ERM

In summary, boards have a responsibility to ensure optimal risk oversight of their companies. As we have outlined above, this involves ensuring appropriate capabilities (and management discipline) are in place in all of the five core dimensions of enterprise risk management: risk transparency and insight, risk appetite and strategy, risk-related processes and decisions, risk organization and governance, and risk culture.

Ensuring best practices along all of these dimensions is a journey that management and boards need to take together. Where to start? We highlight twelve specific actions, across these five dimensions, that all boards should consider taking when aiming for best practice.

1. Require from management the establishment of a top-down ERM program that addresses key risks across the company and elevates risk discussions to the strategic level
2. Require a risk heat map that identifies and collates exposures across the company, reveals linkages between exposures, and identifies fundamental risk drivers
3. Require an in-depth, prioritized analysis of the top three to five risks that can really make or break the business—the company's "big bets" and key exposures
4. Require integrated, multi-factor scenario analysis that includes assumptions about a wide range of economic and business-specific drivers
5. Establish a board-level risk review process and require from management insightful risk reports
6. Establish a clear understanding of risk capacity based on metrics that management can measure and track
7. Produce a strategy statement that clarifies risk appetite, risk ownership, and the strategy to be used for the company's key risks
8. Require management to formally integrate risk thinking into core management processes, e.g., strategic planning, capital allocation, and financing
9. Clarify risk governance and risk-related committee structures at board level, and review board composition to ensure effective risk oversight
10. Define a clear interaction model between the board and management to ensure an effective risk dialogue
11. Require that management conduct a diagnostic of the organization's risk culture and formulate an approach to address gaps
12. Review top management's compensation structure to ensure performance is also measured in light of risks taken

Taking these twelve actions would go a long way toward helping directors fulfill their fiduciary duties and their companies thrive.

* * *

Among the many lessons of the crisis, it is clear that there is no magic prescription for crisis-proofing a business. Companies have to figure that out for themselves—a task in which the board plays a key role, by asking probing questions and engaging in productive discussions. The topics above are the ones where, in our experience, these questions provide the most value to build a flexible, resilient, and risk-aware business.

André Brodeur *is a partner in the Montréal office, where* ***Martin Pergler*** *is a senior expert.* ***Kevin Buehler*** *and* ***Michael Patsalos-Fox*** *are directors in the New York office.*

McKinsey Working Papers on Risk

1. **The Risk Revolution**
   Kevin Buehler, Andrew Freeman, and Ron Hulme
2. **Making Risk Management a Value-Added Function in the Boardroom**
   Gunnar Pritsch and André Brodeur
3. **Incorporating Risk and Flexibility in Manufacturing Footprint Decisions**
   Martin Pergler, Eric Lamarre, and Gregory Vainberg
4. **Liquidity: Managing an Undervalued Resource in Banking after the Crisis of 2007-08**
   Alberto Alvarez, Claudio Fabiani, Andrew Freeman, Matthias Hauser, Thomas Poppensieker, and Anthony Santomero
5. **Turning Risk Management into a True Competitive Advantage: Lessons from the Recent Crisis**
   Gunnar Pritsch, Andrew Freeman, and Uwe Stegemann
6. **Probabilistic Modeling as an Exploratory Decision-Making Tool**
   Martin Pergler and Andrew Freeman
7. **Option Games: Filling the Hole in the Valuation Toolkit for Strategic Investment**
   Nelson Ferreira, Jayanti Kar, and Lenos Trigeorgis
8. **Shaping Strategy in a Highly Uncertain Macro-Economic Environment**
   Natalie Davis, Stephan Görner, and Ezra Greenberg
9. **Upgrading Your Risk Assessment for Uncertain Times**
   Martin Pergler and Eric Lamarre
10. **Responding to the Variable Annuity Crisis**
    Dinesh Chopra, Onur Erzan, Guillaume de Gantes, Leo Grepin, and Chad Slawner
11. **Best Practices for Estimating Credit Economic Capital**
    Tobias Baer, Venkata Krishna Kishore, and Akbar N. Sheriff
12. **Bad Banks: Finding the Right Exit from the Financial Crisis**
    Luca Martini, Uwe Stegemann, Eckart Windhagen, Matthias Heuser, Sebastian Schneider, Thomas Poppensieker, Martin Fest, and Gabriel Brennan
13. **Developing a Post-Crisis Funding Strategy for Banks**
    Arno Gerken, Matthias Heuser, and Thomas Kuhnt
14. **The National Credit Bureau: A Key Enabler of Financial Infrastructure and Lending in Developing Economies**
    Tobias Baer, Massimo Carassinu, Andrea Del Miglio, Claudio Fabiani, and Edoardo Ginevra
15. **Capital Ratios and Financial Distress: Lessons from the Crisis**
    Kevin Buehler, Christopher Mazingo, and Hamid Samandari
16. **Taking Control of Organizational Risk Culture**
    Eric Lamarre, Cindy Levy, and James Twining
17. **After Black Swans and Red Ink: How Institutional Investors Can Rethink Risk Management**
    Leo Grepin, Jonathan Tétrault, and Greg Vainberg
18. **A Board Perspective on Enterprise Risk Management**
    André Brodeur, Kevin Buehler, Michael Patsalos-Fox, and Martin Pergler

McKinsey Working Papers on Risk
February 2010
Designed by North American Design Center

www.mckinsey.com