McKinsey Working Papers on Risk, Number 22

Top-down ERM: A Pragmatic Approach to Managing Risk from the C-Suite

André Brodeur and Martin Pergler

August 2010

Contents

McKinsey Working Papers on Risk present 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)

Top-down ERM: A Pragmatic Approach to Managing Risk from the C-Suite

A global financial crisis, environmental disasters, product failures, commodity price spikes, and unexpected regulatory changes: the last decade has taught us that large risks materialize more frequently and with bigger impact than we like to think. As a result, a growing number of companies are taking a hard look at how they manage risk. Many management teams have lost confidence in their ability to identify and mitigate the risks that matter. Others can't keep up with rapidly evolving risks, or find it difficult to re-calibrate their level of risk-taking after a crisis. Some see opportunity in navigating current volatility more nimbly than their competitors. Not least, all companies are feeling an unprecedented level of external scrutiny.

Unfortunately, when boards and senior management turn to their organizations for risk insights, they are often unimpressed by what they see. Many non-financial companies are still in the early days of implementing an enterprise risk management (ERM) program, leaving their top management and boards with scarce or poorly structured information on the key risks facing the company. Others that have implemented a comprehensive ERM program have ended up with bureaucratic risk management processes that add little value.

In this paper we suggest an approach for non-financial companies to put in place an ERM system that quickly enables risk thinking in the C-suite, while not over-burdening the organization. It provides a starting blueprint for companies who want to raise their game in this area, as well as a sanity check for those whose existing risk approaches are not living up to their aspirations.

TOP-DOWN AND BOTTOM-UP ERM

A comprehensive ERM approach needs to have two facets (Exhibit 1):

1. A **"bottom-up"** system, whose objectives are to ensure a comprehensive identification and prioritization of all important risks, define and implement risk policies and processes that control daily decision making throughout the company, and ensure a robust risk culture company-wide. For instance, bottom-up ERM can help a company to spot a weak operational procedure, surface the issue at the right managerial level, and make the right risk-return trade-off to fix the problem.

2. A **"top-down"** system, whose objectives are to distill insights and provide clarity on the top 5 to 10 most important risks or *big bets* shaping company performance, support risk-informed decisions at the executive committee level, ensure a risk dialogue among the management team, and enable proper risk oversight by the board. Top-down ERM provides the crucial leadership and guidance that the organization needs to balance risk and reward optimally and steer the company in the right direction.

Exhibit 1

Top-down and bottom-up ERM

Most companies that have attempted to build ERM have focused disproportionally on the bottom-up system. While many have got the basics right, most struggle with a few common problems: difficulties in identifying and responding to emerging risks early enough, challenges translating risk policies into actions, and trouble creating a healthy risk culture throughout the business. In addition, many of these companies have ended up with a proliferation of processes that collect information on risk (e.g., complex risk registers; ERM workshops; environment, health, and safety scorecards; project risk assessments) that together give risk management a bureaucratic reputation, often with justification. Middle management in particular views the processes as a burden rather than as a help to good managerial practices. Despite all these challenges, however, a thoughtful bottom up system generally constitutes a good starting point to build an effective overall ERM program and should not be "rewired" according to the latest best-practice fad. (See the sidebar on typical elements of a robust bottom-up system on page 5.)

Where the vast majority of ERM approaches fail is in the top-down system. The following are the usual symptoms:

- Discussions on risk are shallow and lack insight, and in particular lack clarity on the handful of risks that define the franchise. In the words of one executive, "50% of what we talk about is obvious, and the other 50% is irrelevant."

- Major decisions (e.g., M&A, market entry, capital projects) are made with insufficient discussion of the risks involved, or with limited risk insights to support that discussion—and often turn out to be sub-optimal from a risk-reward standpoint. "We spent all of one hour debating whether to go ahead with the deal without any real data to answer the questions we raised."

- Insufficient follow-up by management on agreed actions to mitigate risk, and ineffective risk oversight by the board due to poor reporting and little interface with management on risk topics. "We see the same risks on the list each time, just with different names beside them [as the person responsible to mitigate them.]"

- Not enough challenge and dissent on risk matters, at both board and top management levels, resulting in risk blindness due to groupthink. "We don't have the right forum to ask each other 'Have you thought about this possibility?' without coming across as being negative."

- Top management sending the wrong signals to the organization, through a performance management approach that does not balance risk and reward in a way consistent with the company's actual risk appetite. "We have great policies on not taking unauthorized risks - but the way to get promoted is to ignore them and make bets that pay off."

In our opinion, it is the shortcomings in top-down ERM that usually drive management's overall malaise about risk management. While flaws on the bottom-up side can create vulnerabilities, gaps in the top-down system almost always drastically limit overall risk management effectiveness. These gaps can make management lose the forest for the trees and allow repeatedly poor decision-making about risk-return tradeoffs by managers. While it is important to manage risks in all corners of the organization, it is critical to drive risk management from the top.

THE BASIC BUILDING BLOCKS OF TOP-DOWN ERM

A top-down ERM system, reduced to its simplest form and geared for impact, should have the following five building blocks:

A risk dialogue forum for top management

Companies need a specific forum where risk is explicitly discussed at the C-suite level. In this forum, the executive team reviews the overall risk profile of the company, discusses the risks surrounding major decisions, and addresses "hot topics" surfaced by the organization's bottom-up ERM process. The forum offers an opportunity for top management to voice risk concerns or ask for risk guidance. It also offers an opportunity for the executive team to reflect on the signals it is sending to the rest of the organization—"how are we influencing our managers to strike the right risk-reward balance in their day-to-day decisions?" In a nutshell, the risk dialogue forum acts as the conscience of the organization regarding risk.

Creating the risk dialogue forum can be as simple as setting aside an hour each month on the executive committee's regular meeting to talk about risk. Alternatively, a separate "risk and strategy" committee can be created, meeting independently at periodic intervals. Regardless of the approach taken, it is crucial to make time for risk dialogue to be front and center, and avoid the risk topic being crowded out of discussions as crises recede and other topics clamor for immediate attention.

A risk charter for the board

At the board level, it is important to clarify responsibility for risk oversight. While at most companies the audit committee is responsible for overseeing the risk management *process* (including both top-down and bottom-up elements), we strongly believe that the *full board* needs to be responsible for overseeing the company's risk-taking. A risk charter will clarify responsibilities for the full board and its committees, as well as clarify expectations of individual directors, who may otherwise interpret the topic of "risk management" in very different ways. In our experience, the most successful risk transformations have always been led from the top. Apart from

fulfilling the board's fiduciary responsibilities to oversee risk taking by the organization, clarifying the board's role and expectations is hugely valuable to management, empowering them to pursue an ERM approach that will be "wired in" to top-level decision making.

A synthesized, actionable risk dashboard

An effective way to jumpstart risk thinking in the C-suite (and at board level) is to create a risk "dashboard" that truly fits the needs of top management (Exhibit 2). In our experience, an effective risk dashboard is an extension of the reports and documentation that top management already uses. It invariably goes beyond the classic "risk heat map" that displays risk on a matrix of probability vs. impact, and also beyond the typical 10-page report containing numbers and graphs on some selected "risk indicators." For instance, the executive committee of one industrial company structured its standing agenda around a review of updated cash flow projections. The risk dashboard it developed was an overlay to these projections, drawing attention to the specific risks associated with specific numbers in these projections. The overlay was color-coded to reflect severity of impact, likelihood, and degree of preparedness. At another company, with a very different management style, the management team instead preferred a dashboard that was a narrative explaining past performance, the relationship to the company's current "big bets", and implications for the future. Annotated cash flow projections would not have been effective, since that was not how the executive committee as a whole managed the business.

Exhibit 2

A top management risk dashboard

SIMPLIFIED EXAMPLE

USD Millions

EBITDA by country	2010	2011	2012	2013	2014
Brazil	1,000	1,107	1,080	1,120	1,230
Europe	500	520	648	837	900
South Africa	250	243	210	175	205
U.S.	250	350	720	1,155	1,810
Mexico	200	189	210	105	103
Thailand	75	81	96	70	82
Costa Rica	25	27	36	39	53
Total EBITDA	**2,300**	**2,517**	**3,000**	**3,500**	**4,383**
Working Capital	(180)	(25)	(95)	(80)	(70)
Taxes	(300)	(430)	(400)	(500)	(650)
Cash generation from operations	**1,820**	**2,062**	**2,505**	**2,920**	**3,663**
Maintenance CAPEX	(300)	(400)	(550)	(600)	(650)
Strategic CAPEX	(200)	(200)	(250)	(250)	(400)
Fixed asset sales	100	80	30	10	-
Net investment in fixed assets	**(400)**	**(520)**	**(770)**	**(840)**	**(1,050)**
Op. Deferred Charges	(15)	(15)	(20)	(15)	(25)
Other Cash Expenses	(80)	(50)	(50)	(50)	(55)
Other uses of free cash flow	(50)	(10)	(10)	(20)	(10)
Total other uses	**(145)**	**(75)**	**(80)**	**(85)**	**(90)**
Total free cash flow from operations	**1,275**	**1,467**	**1,655**	**1,995**	**2,523**
Net financial expense	(1,198)	(1,328)	(1,476)	(1,433)	(1,221)
Total cash generated	**77**	**139**	**179**	**562**	**1,301**
Financial cash uses					
Equity, Convertible	1,000				
Debt conversion effects	400	150	260	150	60
Other	85				
Debt downpayment	**(477)**	**(289)**	**(439)**	**(712)**	**(1,361)**
Cash reserves used/(built up)	**174**		-	-	-
Total Financial cash uses	**(77)**	**(139)**	**(179)**	**(562)**	**(1,301)**
Consolidated total debt					
Initial balance	15,500	15,023	14,734	14,294	13,583
Debt downpayment	(477)	(289)	(439)	(712)	(1,361)
Ending balance	**15,023**	**14,734**	**14,294**	**13,583**	**12,221**
Debt:EBITDA	7	**5.9**	**4.8**	**3.9**	**2.8**

Top risks

1. **Weak recovery and slow growth in U.S. revenues**
2. **Change in environmental regulation in U.S.**
3. **Retroactive tax negotiation with Country X**
4. **Drop in cash flows dedicated to debt reduction**
5. **Weak economic growth in Brazil**
6. **Slow economic recovery in Europe**
7. **JV failure in Country Y**

Whatever the format, the risk dashboard should convey insights on risks that truly shape the company's future performance. This is not the place to assure management that all material risks are being taken care of; the goal is to highlight the 5-10 risks that should be "top of mind" and the object of active debate among senior managers

as they run the business. The dashboard needs to lead to action, and should facilitate follow-up (including who is responsible for each risk).

A risk appetite and strategy statement

Companies make strategic and operational decisions all the time that define where and how the company chooses to create value. These decisions carry risk. Some of these risks are clear (entering a new market overseas carries country risk in that market, for instance, as well as execution risks), but others are more complex. For instance, any company buying a newsprint plant in the U.S. is effectively taking on a long position in the Canadian dollar, in addition the more obvious exposure to newsprint demand. (This is because several Canadian newsprint producers are at the margin on the cost curve, and so their Canadian-dollar denominated costs affect North American-wide prices.)

Companies also have different abilities to manage or otherwise respond to these risks. One company may have rich experience managing execution risks in unfamiliar countries already, while for another that is a reason to pass on the opportunity. One company may be comfortable taking on additional Canadian dollar exposure, while another may need to offset that risk in some costly way. What is clear is that companies need to be thoughtful about how they make these choices. The best way to achieve this is to develop a set of overall guidelines to contain the risk taking that accompanies major strategic decisions. A risk appetite and strategy statement should do the following:

Building blocks of bottom-up ERM

The important building blocks of bottom-up ERM include:

- A regular and comprehensive process for risk identification, assessment, prioritization, and reporting– one that is nimble enough to identify emerging risks as they occur and elevate them in a timely fashion
- Appropriately detailed policies and guidelines on key risks, elaborated in sufficient detail to guide the whole organization from the C-suite down in taking on, mitigating, and responding to those risks in the scope of their responsibility. For instance, a policy may specify that business units must hedge currency exposures with treasury.
- Embedding appropriate risk analyses into normal management processes, and providing the tools to conduct these. For instance, an approval process for new operating procedures should contain a "hook" that requires an operational risk review before the procedures are adopted.
- Clear risk roles, decision rights, and escalation mechanisms. This includes clarity on the roles and reporting mechanisms for any central risk function and risk management teams embedded in business units.
- An overall risk culture improvement program, including regular self-assessments and targeted interventions to address key issues

It is of course crucial to appropriately link these bottom-up elements to the top-down ERM system.

- Dictate a limit for overall risk taking by the company. This is usually best expressed as a set of financial metrics, for instance a target coverage ratio, credit rating, or leverage ratio
- State the risks that the company wants to take actively and manage. Ideally these are the risks for which the company has a competitive advantage; for instance, a company may decide to take on emerging market risk in countries where it has a strong presence, price risk for commodities it produces, and market demand risk for its products
- State the risks that the company wants to minimize, which are those from which it cannot extract value systematically. For instance, many companies refuse to take on currency risk, reputation risk, or certain technical/quality risks

Of course, such a statement has to be consistent with the company's strategy. Its development usually requires in-depth discussions and typically results in heightened understanding of the company's strategy and vision. It also requires developing insight on the relative strengths and weaknesses of the company as compared to both competitors and its value chain partners—something that provides value well beyond the risk appetite and strategy discussion.

Risk analyses embedded in key business processes

At the end of the day, the purpose of ERM is to help management make better decisions about balancing risk and reward. A good top-down approach is to identify the 3 to 5 core business processes or decisions that shape the risk and reward profile of the company, and to equip these processes and decisions with the right risk support.

For instance, an industrial company growing rapidly through acquisitions needed to ensure that the M&A decision process had robust risk components. The VP of Strategy designed, with the help of the risk team, a standard set of risk analyses to support decisions. Specific tools included qualitative questions, analytical methodologies, risk assessment templates, and agenda items for executive committee discussions.

Another company, whose performance depended on the successful launch and execution of capital-intensive projects, put in place a robust evaluation process for its capital projects. A key feature of the new process was a risk-adjusted valuation metric that reflected the investment's risks. The company used this as well as its traditional NPV metrics. This company also established a robust project risk management approach to ensure project delivery with minimal delays and cost overruns.

A third company with an aggressive international growth strategy needed to manage a rapidly evolving portfolio of risks as it expanded first sales and then production in a sequence of new markets. The company defined a stage-gate process to assess country risk and local demand risk, leading ultimately to a debate at board level and more thoughtful go/no-go decisions for market entry.

RISK LEADERSHIP TO DELIVER ERM

To deliver integrated top-down and bottom-up ERM capabilities, companies need to define an ERM leadership model appropriate to their situation. We have observed two broadly successful models in non-financial companies: the "ERM program" and the "risk function." (See "The 'stealth' ERM program" for a view on why not having even an ERM program is rarely a viable model.)

- **ERM program model:** In this model, ERM implementation (both top-down and bottom-up) is overseen by a "risk champion," often reporting to the CFO. The risk champion has the responsibility for developing the ERM process and methodologies, and for facilitating risk discussions by the executive committee and the board. The risk champion may be helped by a few analysts, depending on the complexity of analyses to be undertaken, and by BU risk champions located in the businesses. However, nearly all of the risk-related workload is embedded into standard line and functional responsibilities. The risk champion acts largely as a risk information aggregator and internal consultant.

- **Risk function model:** In this model, a full-blown risk function is set up, under the leadership of a chief risk officer (CRO) who sits on the executive committee[1]. The role of the CRO is to implement and drive ERM, but also to be a dedicated "thought partner" to the BU heads on matters related to risk, and to act as the risk-reward counterweight—an empowered advisor, if you will—in top management decision forums.

1 The role is not always called "CRO," and may formally report directly to the CEO or to another C-level officer, such as the CFO. What is essential is that the role is that of an independent thought-partner who is a peer to others on the executive committee.

The CRO has a team of analysts; the team's size depends on the complexity of risk measurement and report production. For instance, a large diversified multinational conglomerate may have a team of 10 to 20 people to conduct risk analyses, facilitate risk workshops, maintain early-warning indicators, develop macroeconomic insight, develop risk reports, and follow up on mitigation actions. In this model, the risk function is a core pillar of the company's management system, on par with all other functions represented on the executive committee.

The choice of model depends on the company's culture and the complexity of its risk profile. The ERM program model requires a belief that key risks are transparent enough to be operationally handled by managers closest to them, and that corporate processes and risk culture are robust enough to avoid problems. The risk function model reflects a belief in the value of a system of checks and balances on risk-related decisions, or at least an expert second set of eyes to help managers navigate the maze of complex or rapidly changing risks. Regardless of the model chosen, key to success is senior-level championing by the board and executive committee.

While a comprehensive and sustainable bottom-up ERM system may well take 12 to 24 months to embed throughout the organization, a skeletal top-down ERM system can be put in place in as little as 3 months. This typically includes a first-generation dashboard, the embedding of risk analyses and discussion in one or two key business processes, and launching a risk dialogue forum. The risk appetite statement and board charter, which require full board involvement, of course take more time.

The 'stealth' ERM program

A handful of companies manage risk quite effectively, yet appear to have no formal ERM program. There is no overall "risk champion" or central risk aggregation team. Risk is just considered a core part of managers' responsibilities. In reality, however, these companies actually have an extensive ERM program, anchored by exceptionally strong individual risk-related managerial processes and a robust risk culture that permeates the enterprise. It is in essence a stealth ERM program that is able to run itself without an explicit organizational lead. Apart from strong culture and processes, such decentralization also requires that key risks do not overlap organizational boundaries, and involves significant and continual top management attention.

This combination of circumstances is exceptional. Most companies seeking to enhance their risk management capabilities find value in thoughtful and non-bureaucratic risk aggregation and oversight using one of the two models described—with someone at the center explicitly in charge.

* * *

Establishing a top-down ERM program that complements a comprehensive bottom-up ERM system is an important step to ensure sound management of enterprise-wide risks. In our experience, adding the missing "top piece" to the existing ERM architecture is often what it takes to turn what is perceived as a bureaucratic or ineffective exercise into an effective enhancement of decision-making across the organization

André Brodeur *is a partner in McKinsey's Risk Practice, where* ***Martin Pergler*** *is a senior expert.*

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 Gregory Vainberg
18. **A Board Perspective on Enterprise Risk Management**
    André Brodeur, Kevin Buehler, Michael Patsalos-Fox, and Martin Pergler
19. **Variable Annuities in Europe after the Crisis: Blockbuster or Niche Product?**
    Lukas Junker and Sirus Ramezani
20. **Getting to Grips With Counterparty Risk**
    Nils Beier, Holger Harreis, Thomas Poppensieker, Dirk Sojka, and Mario Thaten
21. **Credit Underwriting After the Crisis**
    Daniel Becker, Nils Beier, Holger Harreis, Stefano Emanuele Manzonetto, Marco Piccitto, and Uwe Stegemann
22. **Top-down ERM: A Pragmatic Approach to Manage Risk from the C-Suite**
    André Brodeur and Martin Pergler

McKinsey Working Papers on Risk
August 2010
Designed by US Design Center

www.mckinsey.com