McKinsey&Company

McKinsey Working Papers on Risk, Number 40

Enterprise risk management

What's different in the corporate world and why

Martin Pergler

December 2012

Contents

Enterprise risk management: What's different in the corporate world and why

Introduction 1

Reframing a basic misconception 1

The nature of risks in corporates versus financial institutions 3

Implications for risk-management practices 4

Overall consequences 8

Areas of greatest—and least—opportunity for sharing 10

Conclusion 11

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).

Enterprise risk management: What's different in the corporate world and why

Introduction

Given the current environment of continuing economic uncertainty, plus a steady stream of unfortunate major operational-risk events striking companies around the globe, few would dispute that some attention to risk management at the enterprise level is important. Nor would many dispute that typical current practices too often fail to deliver. For companies outside the financial sector, however, it is challenging to find inspiration.

Historically, a significant part of risk-management practice at corporates has evolved from health and safety risk management in heavy industrial and natural-resources companies. It focuses on detailed cataloguing, tracking, and mitigation of a long list of what might go wrong—expanded beyond health and safety. This list is typically called the "risk register." Yet companies that use this as their core framework for enterprise-level risk management routinely miss or woefully misestimate the risks that end up really mattering to the achievement of their overall objectives or even fundamental health.

On the other hand, given its role as an intermediator and disaggregator of risk, the financial sector has led the charge in developing risk-management practices related to financial and market risks. Of course, waves of recent systemic failure in the financial sector promote a healthy sense of skepticism about the idea of using the practices developed in that industry as a blueprint for others. In addition, current innovation in the financial sector is largely focused on responding to changes in governmental regulation and other firefighting measures. Nevertheless, as far as these "liquid" risks are concerned, the financial sector continues to provide a rich seam of frameworks and methodologies from which all sectors can potentially mine.

But where to go for broader inspiration? The overall risk-management framework, the nature of management (and board) dialogue about risk, or the integration of "risk thinking" into navigating overall business uncertainty? The reality is that while the need for thoughtful enterprise risk management (ERM) is clear, corporate decision makers, from line managers to board members, are jaded. The risk-management process is usually perceived as unclearly scoped, bureaucratic, ineffective, and even obstructionist. Participation in an enterprise-level process is viewed with about as much enthusiasm as going to the dentist—with the additional suspicion that the risk-management tooth-puller may in fact be a quack.

Perhaps that partly explains why many corporates are looking to the financial sector for the broader inspiration they seek—after all, the approaches and techniques are familiar and available and there is plenty of talent for hire. "We hired a risk manager from a US bank, but he's still getting to know our business," reports the CFO of an Asian conglomerate. "Our overall risk transformation is being driven by two new board members, one from a European financial institution, with deeper technical knowledge than the rest of us," recounts another board member of a US consumer-goods company.

The enthusiasm in those statements is at best lukewarm. Comments from deeper in the organization are often scathing: "Now that there is an ex-banker on the board, we're somehow supposed to create regular financial-risk reports allocating risk capital to risk types and business units. It makes no sense for us," complains the treasurer of an industrial-manufacturing company.

Our belief is that thoughtful importing by corporates of talent and good practices from the financial sector can indeed be highly beneficial. But all those involved need to be continually conscious of the differences in expectations, challenges, and even the language used to frame the role of the risk-management function, in order for the cross-industry transfer of ERM approaches to work.

Reframing a basic misconception

Financial institutions, whose entire business model relies on the aggregation and disaggregation of risk, have been the cradle of modern risk management as a set of disciplines and processes developed since the late 1980s.

However, that does not mean there is a linear evolutionary path whereby financial institutions define the leading edge and others' risk-management practices obediently follow over some uncertain timeframe. Looking at all business sectors, it is useful to reframe the journey and to differentiate among four stages of maturity (Exhibit 1).

Exhibit 1 There are four stages of maturity in risk management.

	0 Initial transparency stage	1 Systematic risk reduction	2 Risk-return management	3 Risk as competitive advantage
Drivers	▪ Compliance with basic standards/regulations ▪ Reduction of regular surprises	▪ Avoiding unexpected large loss events ▪ Stability to enable growth plan ▪ Professionalized management	▪ ROE[1] improvement requirements ▪ Competitive pressure ▪ Navigating trade-offs	▪ Top management focus on risk-adjusted performance ▪ Finding niche in mature marketplace
Key tools	▪ **Opportunistic approaches**	▪ **Risk heat map** based on consensus assessments	▪ **At-risk measures** (eg, VAR,[2] CFAR[3]) ▪ Systematic **scenario analysis of profit and loss**	As left, plus: ▪ Strong **risk culture** ▪ **Unbundling risks** through contracting and markets

1 Return on equity.
2 Value at risk.
3 Cash flow at risk.

While some financial institutions (for instance, many smaller regional banks) find themselves in stage 1, and a handful of investment banks would consider themselves at stage 3, the average financial institution sits squarely in stage 2 of this spectrum. (Of course, regardless of stage, the topic of changing financial-sector regulation and its implications is very much top of mind.) Other industry sectors have different centers of gravity. The retail sector and telecoms, for example, on average are on the cusp of passing from stage 0 to stage 1. Companies in sectors with strong natural-resources exposure (whether as resource extractors or processors) or important technical or R&D risks (for example, pharma) are more often on the cusp of stage 1 to stage 2, or wholly in stage 2. Typical companies moving into stage 3 are energy companies using increasingly mature liquid commodity markets, or conglomerates or asset managers/investors juggling a diverse portfolio of assets, in each case seeking a source of advantage in a crowded, competitive arena.

Even within sectors there is a strong lack of homogeneity. For example, in one major market, a leading telco is developing quite sophisticated stress-testing macroscenario for its profit and loss and strategic plan, and models the value at risk (VAR) from its currency exposures (stage 2). By contrast, one of its peers, with a roughly comparable market position and performance, has formalized risk-management approaches that consist of the bare minimum required to meet regulatory requirements (stage 0). Similarly, there are mining companies with advanced cash-flow-at-risk models and optimized project financing and commodity hedging for new mines (stage 3) competing with others that merely conduct an annual review of mitigation plans for their top-30 operational risks (stage 1).

There is, so far, an absence of robust statistical evidence that "more mature risk management," however defined, would necessarily translate into better performance. However, in our opinion, these differences in maturity are neither accidental, nor irrelevant. Rather, they reflect underlying differences in drivers of value creation, including assets and exposures, and management culture. Companies find niches not only in terms of market opportunity and value-chain position, but also in strategic capabilities; risk management can be one of these.

Just as over the past 40 years there has been a powerful shift toward more careful strategic management of the firm, we believe that there will continue to be a powerful overall shift to the right on this risk-management maturity spectrum. But it will be a gradual process, with drift happening at different speeds. Depending on one's circumstance, moving to

the right in risk management at the right time will be a strategic investment for differentiation versus peers, or a catch-up move if one has fallen behind. In particular, individual corporates need to find their own path based on their specific opportunities for value-creating competitive differentiation, and not just seek to "learn from the one's betters."

In view of this landscape, with a variety of levels of maturity and philosophy, there is sometimes also the misconception that there are no transferrable good practices—that the differences among and between companies are so great that every company needs to improvise in its own way. We shall see below that while customization is important, there are emerging good practices that can be applied, *mutatis mutandis*.

The nature of risks in corporates versus financial institutions

The typical first surprise experienced by the financial-institution risk practitioner arriving at a corporate is the absence of a standardized risk taxonomy. In a bank, at a high level, there is a clear and ubiquitous separation into market, credit, operational, and liquidity risks. There are, of course, complications, such as how changes in the macroeconomic and regulatory environments translate into these four categories, and how they are correlated. But it is clear that a top-level standard taxonomy works well for institutions with very similar high-level business models.

Corporates that have thought systematically about their risks have usually developed a nonstandardized taxonomy of their own. The obvious reason for the difference is that the taking of financial-market positions and extending of credit is nearly always a less central part of their business model. Other risks—such as technical, supply chain, physical safety and environmental, natural-resources availability and cost, but grouped in whatever way reflects the management system of the company—are more characteristic.

A very high-level division among operational, strategic, and financial risks is usually helpful. However, a specific risk may be allocated to different categories based on how exactly it affects a particular company. For instance, developmental delays in new technologies may be operational risks for a company that needs to reconfigure its supply chain for a new project as a result, but may be crucial strategic risks (upside or downside) for someone in that supply chain. Commodity prices are a financial risk for a commodity processor that may suffer a temporary mismatch between its inventory costs and contracted selling price, but are a strategic risk for a real-estate developer with holdings in Australia, Canada, and the Middle East, whose economies are highly dependent on natural resources overall. As a result, nonstandard risk taxonomies actually work better, since they reflect the real differences in the mechanism through which these risks affect different companies, and therefore how the companies need to monitor and respond to these risks.

Less obviously, there are crucial differences in the nature of risk exposures. Fundamentally, the typical bank is leveraged, but has the ability to "dial up or down" its level of exposure to market or credit risks, and indeed to sample different flavors of each of these risks, by dialing up or down its appetite for transactions specifically exposed to these risks. This is why many banks have naturally settled at stage 2 of the risk-maturity framework: it provides exactly the right level of quantification to allow the navigation of such decisions.

In contrast, important risks faced by corporates are "chunky." You either enter a certain business arena at scale, or you don't. To be sure, there are certain opportunities for scaling your exposure, and sharing or mitigating risks, but fundamentally the typical corporate frames its core risk-management questions by asking "which are my main risks?" and "what risks am I willing to take on?" rather than deciding to "measure my exposure to a standard set of risks and I'll choose where to set the dial on each one."

The differences become more striking as one explores the nonlinearity of exposures. Financial institutions' nonlinear exposures arise from slicing financial risks into tranches, by quality or time to maturity, for example, so that individual asset holders' or counterparties' exposures are magnified (or constrained) within (or outside) a certain range. In contrast, while many corporates' risks are either discrete or linear, part of the reason some companies have moved to the right on the maturity spectrum is precisely because of the nonlinearity of certain crucial strategic risks that they face. And much of this nonlinearity is driven by the nature of the company's response to the risk.

Two examples help illustrate this important point. A heavy equipment manufacturer was considering building manufacturing facilities in Mexico and Thailand. It was therefore facing exposures to the evolution of labor costs in these countries, to transportation costs from these countries, as well as, of course, regional demand in different areas in the world. Up to a point, these risk exposures were linear—a small perturbation in any one of these drivers would propagate to a corresponding perturbation of financial performance, depending on the portion of total costs and/or revenues impacted. However, the company realized that past certain limits, its "country-risk" exposure was actually very different based on how quickly the company could realize—and react to—evolution in these risk factors by shifting production from one country and/or one product to another. The existence of that tipping point—the nonlinearity—is precisely the opportunity to profit from these risks.[1]

As a further example, oil companies involved in so-called "unconventional" development and production have a nonlinear exposure to oil prices. When prices are high, each dollar up or down propagates through to their bottom line. But if oil prices shift and stay sufficiently low, especially before their projects are sufficiently completed (sunk costs), their unconventional projects will very likely be out of the money. Their economic value will be determined at best by a real-options type of analysis to monetize the eventuality that at some point they will be in the money—a very different (and more complex) exposure. Furthermore, oil companies have realized that their break-even oil price for major projects actually depends heavily on whether they are procyclical developers (and face high costs in a tight specialized labor market) or contrarian countercyclical ones. For instance, construction costs in Alberta in 2008 were 1.6 times that of the US Gulf Coast—and then dropped 30 percent by 2010 as oil prices dropped and investment dried up.

Finally, due in part to "chunkiness," a corporate's list of its most important risks will more often contain so-called "data-poor" risks, where there is a dearth of historical or other readily available data on which to feed quantitative analytical approaches. This is a mixed blessing. Credit and market risks faced by financial institutions have a wealth of data available (even though recent experiences have shown the pitfalls on relying too much on these data). The simple absence of this amount of data for most operational, strategic, regulatory, and large-scale macroeconomic risks has led to them being considered less systematically by financial institutions in comparison. In contrast, for many corporates, data-poor risks have so clearly been integral to the risk profile that those companies have scaled back the overall level of quantification of their risk approaches, as compared to companies whose risk exposures are dominated by data-rich risks such as commodity prices. "We used to calculate VAR from financial risks in treasury; but we stopped once we realized it was swamped by our strategic and operational risks that we just couldn't calculate at all," reports one vice president of risk management.

Implications for risk-management practices

It would be tempting to conclude from the above that the differences in risk management, not only between financial institutions and corporates but also between individual corporates, are so great that there is really no alternative for the newly minted corporate-risk manager but to forget everything he or she knows and just start from scratch. Nevertheless, we believe there are important themes of good practice for corporate ERM that can be derived from financial approaches.[2]

Risk insight and transparency. Financial institutions emphasize quantifying (and maintaining up-to-date awareness of) their exposure to the core risks (credit, market, liquidity, and operational). The key output is an understanding of the degree of risk being taken—and therefore the amount of scarce risk capital needed—in different areas of the institution. The typical corporate invests much more time in identifying, assessing, and prioritizing a wide range of risks, unraveling relationships across the company and understanding the likely impact of the company's own potential responses to the risk. The level of quantification is highly variable. Where partial offsets (natural hedges), correlations, and/or trade-offs between these risks are crucial, sophisticated models similar to those embraced by

1 Eric Lamarre, Martin Pergler, and Gregory Vainberg, "Reducing risk in your manufacturing footprint," mckinsey-quarterly.com, April 2009.

2 The framework used here is the McKinsey framework for integrated risk management, revised from Kevin Buehler, Andrew Freeman, and Ron Hulme, "Owning the right risks," *Harvard Business Review*, September 2008 (hbr.org).

financial institutions are highly relevant. But where risks have poor data and exposure depends on untested and unpredictable endogenous responses by the company's own management to the risk stimulus, such models are excessive and can actually be misleading as a basis for decision making.

In particular, the financial-risk practitioner can help a corporate become more systematic at aggregating the common risk exposures across different business units, much in the style of the banks. On the other hand, the corporate-risk practitioner will need to work much harder than his or her financial peer in helping the company's top management develop a shared sense of the top dozen or so "mega-risks" that really drive corporate health and performance—and how to address them. This is the more complicated and situation-specific analog of the standard banking-risk taxonomy.

Risk appetite and strategy. The typical bank is highly leveraged, with risk capital a very scarce resource for which there is vigorous internal competition. In view of the standard risk taxonomy, setting risk appetite is an exercise in allocating this risk capital effectively, and defining the right risk limits to ensure overall risk taking is within appropriate bounds. Discussions about which risks to take are important at specific decision points, but tend to be focused on whether the institution understands the risks sufficiently, and whether the quantification of the risk capital needed is reasonably accurate, for example, by asking, "Do we dare commit to these products given what might happen in event of a correlation breakdown?"

The situation in corporates differs in two ways. First, corporates can have very fruitful discussions about exactly which risks they are preferentially positioned to own or want to learn to manage better, for example, by deciding "We have expertise in managing complex R&D portfolios that we can deploy here," "Our mix of short-term versus long-term contracts versus competitor X gives us more flexibility to respond," or "This is a good limited-downside opportunity to learn to manage a subsidiary in a developing country that we can then build on for more ambitious international growth." And the limitations of risk quantification (together with generally being less leveraged and less regulated) mean risk limits are typically replaced by more qualitative risk policies. For instance, as a matter of policy, some corporates insist that any open foreign-exchange positions are immediately hedged once created or that any project they bid to provide must have a clause limiting liability. Or they even insist they will not sell their product to certain customers or through certain channels due to potential liability or reputational risk issues. These are all examples where such companies do not calculate a limiting amount of risk capital that is allowable against such a risk, since they don't trust its quantification. In addition, the activity or investment in question is sufficiently non-core that it is not worth the trouble to try, even if there is the odd bit of value leakage (for example, the unnecessary cost of hedging and missing a business opportunity that could have been pursued at sufficient expected profit to cover the risk).

Second, the question of overall risk appetite is much broader in corporates. Given the macroeconomic and regulatory environment, the reality for many financial institutions is that the level of flexibility in overall risk appetite is fairly low. A typical corporate, however, manages for a whole range of financial metrics, such as earnings and cash over multiple time periods. Different stakeholders—including crucially important ratings agencies—have different expectations. All of these translate into constraints on risk appetite that many corporates are only beginning to explore systematically. In addition, corporate-financial levers such as raising debt or adjusting equity capital, and strategic levers such as joint ventures on a major project or hedging strategies, all affect, and are affected by, risk appetite. The implication is that the effective risk-appetite allocator at a financial institution is a technical (and regulatory) specialist, while the risk-appetite expert at a corporate needs to become a strategic financial thinker who brokers dialogue between the board and top management.

Risk-related decisions and processes. There are, though, crucial differences between corporates and financial institutions. The business model of a bank is to act as an intermediary (disaggregator and consolidator) of risk. Accordingly, on a fundamental level, risk is part of all bank decisions (for example, to whom to offer credit via lending or trading decisions). As a consequence, the role of risk "management" in business decisions and processes has mutated into asking, "What else is necessary beyond what business managers are already doing?" Typical

elements are processes related to proper risk assessment (including back office and infrastructure), compliance and escalation, and—in view of the changing landscape—regulatory and stakeholder management.

In contrast to their financial-sector counterparts, frontline managers in corporates are, in general, less comfortable and confident as risk takers, and their risk-taking actions more directly influence others. For instance, the purchasing manager's trade-offs on one versus several suppliers—lower cost versus greater supply-chain resilience—will give sales differing amounts of headroom within which to strike a deal. An environmental disaster in one asset may slow down governmental approvals for completely unrelated assets, or damage the brand. So a key focus of risk management in corporates is bringing a risk lens to inform precisely those decisions where the risk profile of the whole company actually is being changed. Exactly which decisions these are depends on the individual company, but it typically includes three categories:

- Significant operating decisions where the consequences affect others than the decision maker, such as supply-chain management ("Do we sole source at an expected saving but with less resilience?"), pricing, ("How much contingency do we need to factor into pricing our response to this RFP?"), product development and exploitation ("Public backlash against genetic modification could exceed share losses in this category")

- Business planning and overall strategic decisions, for instance, overall choice of strategy ("Do we expand overseas?"), capital investment ("We have $300 million of growth capital to invest and $700 million of ideas, with some of those ideas more risky than others.), as well as supporting financing decisions, ("Can we afford to lever up, and what if we hedged our fuel spend?")

- Opportunistic strategic decisions ("Do we do this M&A deal?," "Do we pull out from this market that is doing less well than expected?")

These are, of course, not purely risk decisions, but the key contribution of risk management is to frame the risk trade-offs and provide the insight to support informed management and board dialogue.

Risk organization and governance. There are some obvious differences in risk organization and governance between corporates and financial institutions. In particular, many fewer corporates have a C-suite level chief risk officer (CRO) and a dedicated risk committee on their boards. This is discussed further below, but it is a consequence of more fundamental differences in overall risk organization and governance. As we look at companies in all sectors, we see four different types of role for a central risk group (Exhibit 2).

These four models are not stages in a maturity spectrum; there is no "right" or "better" answer. Apart from tradition and organizational inertia, the most important drivers for the appropriate choice are as follows:

- the complexity of the company's risks. In particular, are crucial risks generated in the same organizational unit that bears the consequences and can effectively mitigate them?

- the degree of confidence in the treatment of risk by existing management processes and culture

In this realm, financial institutions generally fall squarely in one of the two buckets on the right. While basic risk taking remains an integral part of each manager's responsibility, events have repeatedly shown the myriad ways that careless or overly aggressive risk taking in one desk or department can reverberate across an organization. Processes are quite well developed, but it is a prisoner's dilemma–like situation, in which it is often in the personal interest of a talented individual to surf the boundaries of the risk policies or limits that are in place. This relates directly to the internal competition for risk capital, since taking on an extra bit of actual risk should create additional return, and if the risk is misevaluated by the systems and processes in place as being lower than it actually is, the indirect result is that the individual is "credited" with a higher risk-adjusted return.

Exhibit 2 There are four different roles for the central risk group.

Support line risk ownership[1]	Aggregate risk insight	Provide checks and balances	Actively manage risks
▪ **Line management** owns risks ▪ Minimal central risk function provides **expert advice on demand** ▪ Risk optimization effected by a **strong business and risk culture**	▪ Line **management owns risks** ▪ Small central risk team **aggregates** risk insight, **integrates** across enterprise ▪ Risk optimization performed by overall management, with informational support from central risk team	▪ Line management owns risks ▪ Central risk team led by CRO[2] with a **seat at the table**, acting as counterweight for important strategic decisions ▪ CRO acts as **thought partner** to business heads	▪ Risk function **owns and actively monitors** and manages certain key risks centrally (eg, FX hedging, trading/credit limits) ▪ Business heads get **approval** on other risk strategies from CRO

1 If there is any kind of central risk group at the organization; this model can be run with just line management.
2 Chief risk officer.

In contrast, corporates are all over the map, sometimes even in one sector. Donald Humphreys, senior vice president and treasurer of Exxon Mobil said in 2009 that the company does not believe in maintaining a separate risk organization, rather that risk management is naturally a direct responsibility of line management. This articulates an important principle: that operational risks in particular are best managed in situ in order to avoid diluting responsibility. This does not mean Exxon Mobil does not conduct risk management; on the contrary, its processes are quite sophisticated and it has systems in place to track risks and ensure preparedness/response. However, it has chosen to limit the central organizational oversight dedicated to risk.

On the other hand, several other major petroleum companies are moving from an "aggregate-risk-insight" model more to the right, having experienced increasing complexity in managing their strategic oil price and geopolitical exposures, as well as having seen the disasters that ensue if operational risks are poorly managed and a dysfunctional overall approach to risk takes hold.

Indeed, the distinction is one of balance. A common framework for risk management, especially in the financial sector, is that of "three lines of defense," the first being line management/front office, the second the risk-management function (and/or other control functions), and the third compliance and audit. This framework is typically brought out to emphasize that the risk-management function does not operate in isolation, and that robust risk management requires all three defensive lines to be in place. In this context, the differences among our four organizational models require choosing which lines of defense to prioritize. As one moves from left to right, the second line of defense (a central-risk-management function) takes on a more prominent role, while on the left-hand side, one is placing more reliance on culture and processes followed by the first line—and likely expanding the role of the third line of defense as a way of confirming that these processes are followed, compared to when a strong second line is present.

Indeed, the importance of risk culture—mind-sets and behaviors of all employees regarding risk-taking—is increasingly being recognized throughout all industry sectors. Earlier work on classifying and diagnosing cultural hotspots for risk via a survey-driven diagnostic[3] allowed an empirical observation of the relatively low level of systematic difference between sectors. There are significant differences between companies, of course, and often between business units in the same company, but characteristic issues relating to poor transparency on risk tolerance ("What are we allowed to do?"), lack of openness and fear to challenge ("Everyone knew it was a bad idea, but no one felt they could object"), and speed of response or gaming the system (such as finding ways to arbitrage transfer pricing that allows one unit to keep the benefit from risk taking but passes on the downside elsewhere inside the company) are ubiquitous.

3 *McKinsey Working Paper on Risk, Number 16*, "Taking control of organizational risk culture," (mckinsey.com).

Overall consequences

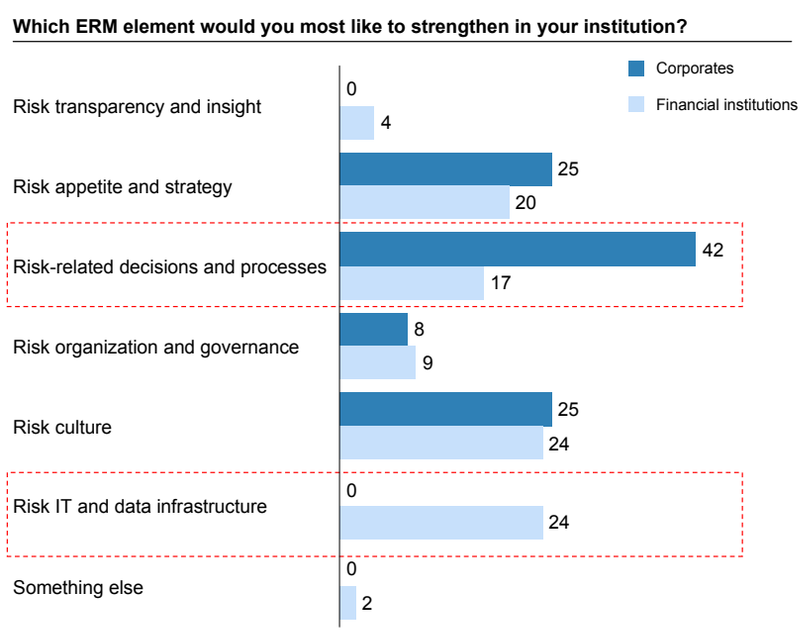
Within the context of the various risk exposures and risk practices described above, some of the more superficial differences between banking and corporate risk management are quite natural.

Importance of different elements of risk management. What do risk leaders in a company worry about most? As Exhibit 3 (below) shows, the different areas of risk management that are perceived to require the most reinforcement vary between financial institutions and corporates. The two sides agree that insight and transparency are (relatively) under control, while risk appetite and culture need more attention. The big difference is that while corporates see huge opportunity in improved risk-related decisions and processes—a reflection of how a plethora of management decisions can manipulate chunky risks with complex endogenous influences—financial institutions apply that level of focus to risk IT and other infrastructural fundamentals. This is, of course, a crucial concern when risk exposure comes from the aggregation of individual risk-intermediation decisions that businesses make, putatively within established quantitative risk limits.

The CRO function. The banking CRO is a specific, fairly well-defined function: an independent member of the bank's top management team, peer to the others, and with direct visibility to the board, often including an independent reporting line. This is very natural given the typical stage-2 maturity, and the desire for a checks-and-balances or even a more rigorous central-risk-management approach. The CRO is the steward of the bank's risk capital.

In contrast, most corporates do not have a CRO, or the title is given to someone who is at the N-2 or N-3 level and reports up through the CFO (or, in some cases, through another top-management team member, such as the chief strategy officer or even chief counsel). For a company in stage 0 or stage 1 in the maturity framework, a full CRO would be excessive. Even in stage 2, given the role of the CFO as the "conscience of the organization" in terms of prudent decision making based on the company's financial realities, a risk-management function reporting through the CFO often makes a lot of sense. It is, after all, the CFO who is already the steward of the company's de facto risk capital—its

Exhibit 3 Financial institutions and corporates have different concerns about enterprise risk management (ERM).



Source: Small-sample polls at Risk Capital 2011 and McKinsey-organized roundtables (not statistically significant)

equity. The exception comes either when the CFO's own decisions are an significant source of risk or the locus of risk-return trade-offs, which, in turn, require an effective checks-and-balances approach, or when the specific qualifications or background of the individual taking on the position makes him or her an asset to the C-suite as an empowered and independent advisor.

The most typical approach among corporates is to have the risk-management function reporting through the finance organization, but there are exceptions. For instance, US Steel appointed its first independent CRO in 2011. Lend Lease appointed its then head of legal as its CRO in 2005. And a number of technology- or R&D–heavy companies combine the risk function with strategy or corporate audit, recognizing that "basic" risk management happens in the line (first line of defense) and that the parts that are not covered reflect growth or portfolio decisions (the strategy angle) and compliance (third line of defense), not risk aggregation.

Board risk committee. Dedicated risk committees in financial institutions have evolved for several reasons, including the following:

- Specialized vocabulary and expertise needed to oversee risk taking
- Regulatory requirements
- Need for independent oversight

In many corporates, risk is discussed in the audit committee, reflecting the nature of risk management in stages 0 and 1 of the maturity cycle. Since risk management in these stages entails largely a combination of compliance, plus informal strategic decision making that takes place through the full board, this is an effective solution. However, as nonfinancial companies start thinking about risk-return trade-offs, their boards often find the usual audit committee mind-set restrictive and insufficient. They therefore take one of three approaches:

- Upgrade the mind-set and capabilities of the audit committee (by growing its mandate to become a full risk committee, regardless of name)
- Establish a separate risk committee that approaches risk more strategically
- Keep the audit committee responsible for risk-management oversight, but deliberately upgrade the board strategy committee dialogue from just strategy to risk-return trade-offs in the context of strategy setting.[4]

The risk profession and community. Risk management has grown tremendously as a profession in the past decade. However, the bulk of the related literature focuses on financial risk management, and the bulk of the attendees at industry events are from the financial sector. Part of this is a question of volume; given the difference in maturity, there are simply more interested practitioners. And given the standardization of risk types and methodologies, it is much easier to develop a common corpus of issues and knowledge around which to build a community.

However, a consequence of this is a different mind-set for risk professionals in corporates. As indicated above, the biggest concerns on risk in financial institutions encompass three areas—appetite, culture, and IT—where the transfer or codevelopment of emerging good practices across the industry is hugely important, as is the whole corpus of knowledge about how to deal with evolving regulation. In contrast, the biggest concerns for corporates relate to including risk in crucial business decisions and processes. The shared concerns of risk appetite and risk culture are particularly industry- and situation-specific, and so a "professional specialist" approach is more likely to lack critical scale. It is therefore hardly surprising that in many more instances, corporate-risk practitioners

4 André Brodeur and Martin Pergler, "Risk oversight practices: Insights from corporate directors," Director Notes, The Conference Board, September 2010 (conference-board.org).

are respected company insiders from adjacent fields who take on the mantle of risk management (sometimes on a temporary rotational basis as part of a general career progression) and develop tailored expertise and approaches, rather than external "industry professionals" looking to deploy the next generation of improved standardized approaches.

Areas of greatest—and least—opportunity for sharing

Which financial-sector tools and ideas will offer the most support to a newly arrived risk manager setting up shop in a corporation?

Rigorous risk dialogue. While the specifics of the risks being discussed and the level of information available about them can vary, the typical corporate can gain much by implementing a regular, fact-based, and timely dialogue on risk throughout the organization. A daily comprehensive risk report, with up-to-date assessments of risk levels by risk type and business unit, as in leading banks, is probably both impossible and impractical. However, expanding the paradigm beyond a risk register and/or risk heat map that is reviewed once a quarter (or once a year!) is crucial!

Careful quantification of risk and concept of risk-adjusted return. While VAR has become a bad word in many circles, thoughtful quantification of risks, recognizing that at different (approximate) probability levels they may have radically different levels of impact, can be highly beneficial. And while a black-box calculation of risk-adjusted return on capital or some other metric that, as if by magic, purports to derive "correct" returns for risk is rarely the right answer, a recognition that returns need to be compared and evaluated with a consideration for the level and nature of risks taken to achieve them is another key ingredient.

Aggregated risk across the enterprise, including stress testing, in particular. The response to the financial crisis (in part driven by external stakeholders) has sharpened the focus of financial institutions on assessing the aggregate impact of risks across the organizations. The same should be the case for corporates, if for no other reasons than to make more agile and informed decisions in the face of macro-uncertainty. The philosophy of stress testing, in particular, exploring the combined impact of a consistent multifactor set of risk assumptions on all the relevant key performance metrics of a company, and likely consequences (for example, credit-rating resilience), is a rich area of opportunity.

On the other hand, what are some of the key preconceptions from the financial sector that are most likely to trip up our corporate-risk manager and confound otherwise enthusiastic colleagues?

A "standardized" risk taxonomy. As discussed, the classification and aggregation of risks across a corporate is a valuable and never-ending exercise. But there is no "standard" risk taxonomy—even by industry sector—to structure the analysis akin to the standard financial-risk factors (market, credit, operational, liquidity, etc.). Untangling the Gordian knot of risk in a typical corporate has no easy solution.

Rigidity in approach to risk organization and governance. As discussed above, there is an established model for the role of the risk-management function—and of risk oversight—in a financial institution. The situation in a corporate depends much more on the nature of the risks and of the overall management system—and stakeholder expectations may well be poorly defined or inappropriate given the nature of the business. Finding the right solution and the right trajectory to get there can be one of the most complex tasks facing a corporate risk manager.

Insufficient focus on teaching, coaching, and listening to the business. While this may be an oversimplification, the typical credit manager or investment portfolio manager in a financial institution generally feels that he or she is knowledgeable enough to manage his or her own risks, even though they recognize the importance of coordination, aggregation, and oversight by the central risk function. In contrast, while many corporate line managers equally feel knowledgeable about risks they "own," there is, in general, a greater need for coaching on how to deal with

risk and uncertainty, teaching basic risk concepts and frameworks, and listening to the business and translating any insights for others.

Finally, suppose the same risk manager later returns to the financial sector (or—like some readers—never leaves it in the first place). There are some areas where the best organically developed practices in risk management in corporates would make good role models for financial institutions:

Top management focus on big bets or so-called mega-risks. As discussed, some of the biggest corporates have increasingly made efforts to identify and discuss their top risks, aggregated across the business, and, importantly, articulated in a way that recognizes how the risks are likely to arise. Financial institutions have been too hamstrung by their risk taxonomy to cut through it for truly franchise-affecting risks—such as the deep-seated crisis in Europe, the slowdown in Chinese economic growth, or even fraud that affects the institution's reputation or confidence in a profound way. Many a financial institution would do well to interrupt the discussion of market and credit risk and preface and frame its discussion of stress testing with a period of identification of and reflection on the handful of big bets the bank is truly taking.

Broad discussion on risk appetite and strategic choice of risks to take. This seems like an odd factor to include, since these days financial institutions are quite preoccupied with risk-appetite discussions. But by and large, these are discussions about how to articulate risk appetite to stakeholders, and how to set the overall risk tolerance—areas where many corporates are weak. Going the other way, financial institutions rarely emphasize the debate over which risks they are in an optimal position to deploy their risk capacity against in order to extract value, and the risks in which they want to "invest" for growth. They could well learn from corporates in this area. Financial institutions generally do a good job of making individual decisions, for example, with credit underwriting, or using a risk-return lens with market positions. However, they tend to be weaker with the fundamental decisions about "where do we play?"

Conclusion

There are both important similarities and differences between risk management in financial institutions and in corporates. This is the nature of the particular risks each face and the way these risks are reflected in a company's value creation and management culture. In particular, there are interesting conceptual and good-practice-transfer opportunities to consider—provided one steps beyond overly simplistic approaches that position one sector as an overall risk-management leader, does not reject it out of hand due to the challenges of recent years, or limits consideration purely to the mechanics of assessing or reporting specific shared risk types. The way forward for both financial and nonfinancial companies is best articulated as a situation-specific integration of approaches, rather than a wholesale adoption or rejection of a rigid set of choices. Even within sectors, companies can justifiably adopt quite different approaches at the enterprise level, provided there is adequate dialogue with all stakeholders. At this stage, there are the beginnings of back-and-forth executive movement between sectors, and there will be more in the future. It follows that debate and clarity around what works and what is likely to fail will only become more essential for effective enterprise risk management across the board.

Martin Pergler is a senior risk expert in McKinsey's Montreal office.

The author wishes to acknowledge the contributions of Andrew Freeman, Arno Gerken, Rob McNish, and Tony Santomero to the development of this paper.

Contact for distribution: Francine Martin
Phone: +1 (514) 939-6940
E-mail: francine_martin@mckinsey.com

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 macroeconomic 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
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, Holger Harreis, Stefano E. Manzonetto, Marco Piccitto, and Michal Skalsky

McKinsey Working Papers on Risk

22. **Top-down ERM: A pragmatic approach to manage risk from the C-suite**
André Brodeur and Martin Pergler

23. **Getting risk ownership right**
Arno Gerken, Nils Hoffmann, Andreas Kremer, Uwe Stegemann, and Gabriele Vigo

24. **The use of economic capital in performance management for banks: A perspective**
Tobias Baer, Amit Mehta, and Hamid Samandari

25. **Assessing and addressing the implications of new financial regulations for the US banking industry**
Del Anderson, Kevin Buehler, Rob Ceske, Benjamin Ellis, Hamid Samandari, and Greg Wilson

26. **Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation**
Philipp Härle, Erik Lüders, Theo Pepanides, Sonja Pfetsch, Thomas Poppensieker, and Uwe Stegemann

27. **Mastering ICAAP: Achieving excellence in the new world of scarce capital**
Sonja Pfetsch, Thomas Poppensieker, Sebastian Schneider, and Diana Serova

28. **Strengthening risk management in the US public sector**
Stephan Braig, Biniam Gebre, and Andrew Sellgren

29. **Day of reckoning? New regulation and its impact on capital markets businesses**
Markus Böhme, Daniele Chiarella, Philipp Härle, Max Neukirchen, Thomas Poppensieker, and Anke Raufuss

30. **New credit-risk models for the unbanked**
Tobias Baer, Tony Goland, and Robert Schiff

31. **Good riddance: Excellence in managing wind-down portfolios**
Sameer Aggarwal, Keiichi Aritomo, Gabriel Brenna, Joyce Clark, Frank Guse, and Philipp Härle

32. **Managing market risk: Today and tomorrow**
Amit Mehta, Max Neukirchen, Sonja Pfetsch, and Thomas Poppensieker

33. **Compliance and Control 2.0: Unlocking potential through compliance and quality-control activities**
Stephane Alberth, Bernhard Babel, Daniel Becker, Georg Kaltenbrunner, Thomas Poppensieker, Sebastian Schneider, and Uwe Stegemann

34. **Driving value from postcrisis operational risk management : A new model for financial institutions**
Benjamin Ellis, Ida Kristensen, Alexis Krivkovich, and Himanshu P. Singh

35. **So many stress tests, so little insight: How to connect the 'engine room' to the boardroom**
Miklos Dietz, Cindy Levy, Ernestos Panayiotou, Theodore Pepanides, Aleksander Petrov, Konrad Richter, and Uwe Stegemann

36. **Day of reckoning for European retail banking**
Dina Chumakova, Miklos Dietz, Tamas Giorgadse, Daniela Gius, Philipp Härle, and Erik Lüders

37. **First-mover matters: Building credit monitoring for competitive advantage**
Bernhard Babel, Georg Kaltenbrunner, Silja Kinnebrock, Luca Pancaldi, Konrad Richter, and Sebastian Schneider

38. **Capital management: Banking's new imperative**
Bernhard Babel, Daniela Gius, Alexander Gräwert, Erik Lüders, Alfonso Natale, Björn Nilsson, and Sebastian Schneider

39. **Commodity trading at a strategic crossroad**
Jan Ascher, Paul Laszlo and Guillaume Quiviger

40. **Enterprise risk management: What's different in the corporate world and why**
Martin Pergler

McKinsey Working Papers on Risk
December 2012
Designed by Global Editorial Services design team

www.mckinsey.com