McKinsey&Company

McKinsey Working Papers on Risk, Number 53

Enterprise-risk-management practices: Where's the evidence?

A survey across two European industries

Sven Heiligtag
Andreas Schlosser
Uwe Stegemann

The authors would like to acknowledge the significant contribution to this paper made by Konrad Richter.

February 2014

Contents

Enterprise-risk-management practices: Where's the evidence?

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 practices: Where's the evidence?

A survey across two European industries

Executive summary

This paper reports the findings of a 2012 survey conducted by McKinsey & Company and the working group for corporate growth and internationalization of the Schmalenbach Society (the oldest German nonprofit organization for the exchange of ideas among business practitioners and academics).

The goal of the survey was to assess the current state of the art of corporate enterprise risk management (ERM) in Europe and to identify recent developments that promise to bring further change to ERM. More specifically, the survey sought to accomplish several aims:

- gain a qualitative understanding of ERM objectives and risk-management practices across industries
- provide a basis for comparison of companies, through the creation of a comprehensive scoring system, so they can improve their risk-management practices
- provide a perspective on best-practice risk-management approaches across companies and potential sources of value in the discipline

To allow for meaningful comparisons, but also to highlight similarities and differences in practices across industries, the survey was confined to two industries. It considered advanced industries (AI), which includes assembly- and high-tech-intensive industries, and the energy industry, which includes companies involved in the production and distribution of electric power, natural gas, and other fuels.

However, these two industries display relatively distinct approaches to ERM, in particular in the organization and role of the ERM function, and these might highlight decisions that risk managers in other industries need to make as well.

Survey respondents included three AI companies and nine energy companies. Our sample size is small as we elected to go deep rather than wide in this effort, conducting several rounds of interviews and qualitative discussions with respondents to flesh out how risk management is really done rather than relying only on quantitative data and providing statistical comparisons.

This report is structured as follows. We begin with a discussion of companies' differing objectives for ERM. We then explore in detail one of the biggest differences among the companies studied: the role of the central risk-management function. We conclude with a discussion of the relative performance of the two kinds of companies studied and the ways that they might step up their ERM, highlighting industry-specific and overarching opportunities for improvement.

What companies want from ERM

In discussions with companies, we have often noticed that the term "enterprise risk management" means different things in different industries. To contribute to a common terminology and to foster exchange among them, we asked survey participants to specify the goals of ERM for their company. (For more on the survey, see "Methodology," page 4.) We asked them to rank four potential objectives of ERM, two for internal stakeholders and two for external:

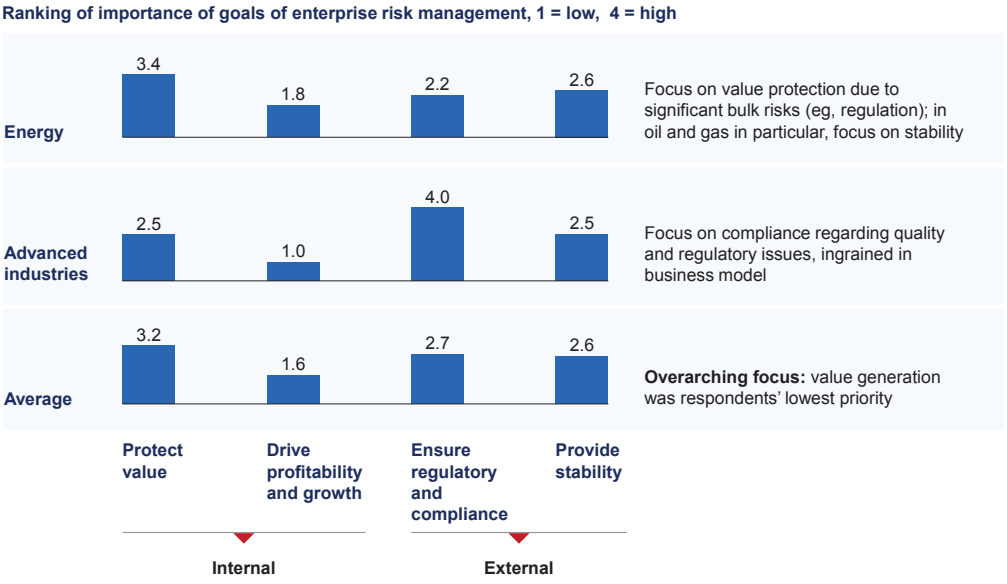
- protect value, for example, by ensuring a certain target rating, avoiding large losses or default, and avoiding volatility in the P&L
- drive profitability and growth by using risk-management techniques to generate value, as reflected in a rising P/E multiple, as well as increased profit and return on equity, and encouraging controlled risk taking in innovation or R&D and investments

- ensure regulatory compliance, protecting the enterprise from negative regulatory intervention and avoiding penalties such as product-liability or safety claims

- provide stability and continuity, ensuring the independence of the enterprise, avoiding unpleasant surprises for shareholders, providing a sustainable workplace for employees, minimizing negative externalities for society at large, and maintaining the confidence of business partners

As expected, the industries that were the focus of our survey showed significant deviations in their objectives for ERM (Exhibit 1).

Exhibit 1 Corporates mean different things when they talk about enterprise risk management.



The most important objective for surveyed companies in advanced industries was ensuring compliance. This result was supported by many discussions we've had with industry practitioners in which quality risk (that is, a failure to meet internal and external quality standards) and the resulting reputational problems were mentioned as the biggest risks that corporates in these industries face. The focus on quality risk can be explained by taking a closer look at the business model of advanced industries. Typically, these companies make significant up-front investments (in R&D, platform development, and so on) that are paid back only if a sufficient number of goods are sold. As such, these industries focus on sales and other revenues, and risks that might hamper sales are considered the most important ones. Quality risk is chief among these. After all, the damage to a company's reputation that results from, say, malfunctioning brakes or tires that catch fire is difficult to fix once such an incident has occurred.

Energy companies identified value protection as the most important goal of ERM. Again, this can be explained by taking a closer look at the industry's business model. One of its biggest risks is regulatory risk (for example, the abolition of nuclear energy in Germany or the passage of renewable-energy laws that encourage decentralized structures and thus limit the competitiveness of the big energy companies). Clearly, regulatory risk has mostly downside potential in current times. Another prominent risk is operational risk (for instance, problems leading to the shutdown of power plants, spills in oil exploration and production, and so on). Looking to ERM for value protection is natural for companies facing these risks.

Companies with an emphasis on oil and gas exploration often also mention the importance of stability. This industry has a particularly long-term view—exploration of oil and gas fields can take years and subsequent production can span several decades. If everything goes as planned, these oil fields are profitable. But the value of these projects is dependent on stable revenues, both due to the long-term nature of the projects and the risk adjustment of the interest rate used in the calculation of net present value as these projects are planned.

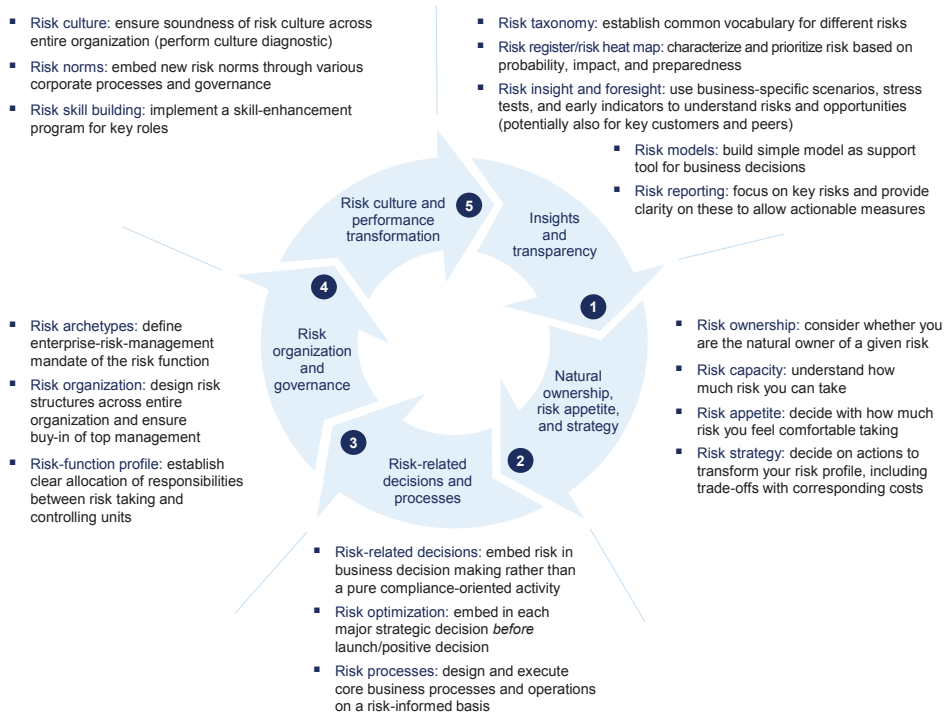
Overall, it is worth noting that across industries, generating value through ERM was the lowest priority for respondents. While this is understandable given today's turbulence, more emphasis should be put on value creation. In many discussions with practitioners, we have heard that risk management has risen on the senior-management agenda since the global financial crisis began and consequently that the power of the risk-management function has increased. However, most leaders are unsure whether this change is temporary or permanent. There seems to be a window of opportunity at present to prove the value-creation potential of risk management.

A common framework for ERM

To help risk practitioners develop a shared vocabulary for ERM, we used a framework to assess ERM practices (Exhibit 2). It includes five dimensions: insights and transparency; natural ownership, risk appetite, and strategy; risk-related decisions and processes; risk organization and governance; and risk culture and performance transformation. The framework is versatile—it applies to both ERM practices and the management of individual risk types such as commodity risk, credit risk, and operational risk.

The survey asked respondents roughly 100 questions across the five dimensions. In the next section, we review the survey findings in the dimension of risk organization and governance because it is here that one of the most important points of distinction among companies' risk practices can be found. Then we review the performance of the two sets of companies, AI and energy, on the full spectrum of ERM activities.

Exhibit 2 A framework helps in assessing enterprise risk management.



Methodology

The research consisted of several stages:

1. We conducted a high-level two-hour discussion with a senior manager involved with risk (such as the CFO, head of compliance, or head of control) to obtain a general understanding of the objectives and peculiarities of ERM and to provide participants with a preview of the questionnaire, its structure, and an understanding of how to fill it out.

2. Respondents filled out the questionnaire by entering qualitative descriptions of their practices into a spreadsheet, an exercise that took about ten hours. The main contact for filling out the questionnaire was typically the head of ERM, who coordinated more detailed questions with the responsible people in individual departments (typically, an additional five to ten people gave input).

3. The survey team reviewed the questionnaire and gave it a preliminary score, using predefined criteria to distinguish among four levels of sophistication: best practice, sound market standards, some shortcomings, and significant shortcomings. The team also highlighted the areas where the information provided was insufficient to assign a score. This round took about ten hours.

4. Follow-up telephone interviews were conducted to clarify remaining questions; interviews lasted about three hours.

5. The survey team finalized the feedback report for every company and highlighted specific recommendations for how each could improve ERM; this took around five hours.

6. The survey team and respondents held a final two-hour workshop to discuss the results and findings of the survey. All interviews were conducted by the same interviewer to maintain consistency.

The setup of the ERM function

Through the survey, we found two different archetypes for the organization of the ERM function, driven by the degree of centralization. A company's dominant archetype typically will not govern all of its ERM activities; some risks may be managed in different ways. Still, the archetypes provide a good way to think about fundamentally different approaches to ERM.

- **Decentralized.** In this approach, line management owns all risks and a slim central risk department provides light-touch support and coordination as needed. The central risk department sees itself mainly in a process-coordination role, but it typically lacks the resources and insights to challenge businesses on their risk-management and control practices. The central risk department is, however, accompanied by a broad network of "risk champions" throughout the other departments. In one case, a central risk-management department of fewer than 20 full-time employees was accompanied by a broad risk-champion network composed of several hundred people who spent between 10 and 20 percent of their time on risk topics, collectively representing about 50 to 60 additional full-time positions.

  Many of the corporates that follow a decentralized approach conduct regular surveys (for example, quarterly) and brief polls of the risk-champion network to ensure that business departments think through and identify the most important existing and emerging risks. A strong risk culture is a key ingredient of this approach, since the departments themselves are held responsible for risks that strike.

- **Centralized.** Here, the risk function closely controls and owns most of the risks (an arrangement that is often used for foreign exchange (FX) and commodity risk hedging) while remaining risks are overseen by line managers, with double-checking or even close supervision provided by the central risk function. Risk-related models typically reside in the central risk group and are rolled out and updated consistently throughout the company. The risk function challenges the assumptions made by businesses and enters into detailed discussions with them. As a result, the central risk department often also assigns responsibilities for individual risks and business departments to its dedicated employees.

Both decentralized and centralized designs for the risk function have their merits. Each is suited to managing different kinds of risk. A decentralized approach allows greater variety and flexibility in risk-management practices; business departments can tailor models and processes to their specific needs. Operational and technical risks, which rely for their management on expert knowledge that resides in the individual businesses, are usually best managed by a decentralized approach, with supporting tools and best practices supplied by the central department.

Another advantage of the decentralized approach is the close integration of the risk function with the business through the risk-champion network, which ensures a seamless flow of communication on risk-related topics. The central group is frequently updated on topics emerging throughout the company, and embedding risk champions in business departments ensures that risk is an integral part of the decisions made there.

The decentralized approach ensures a strong culture of risk ownership throughout the company, as there is no "third party" (the central risk department) that can be held responsible for risk problems.

A centralized risk function, on the other hand, ensures a consistent approach and is often used for comparable risks throughout the organization; similar risks are treated with the same tools and processes. For these reasons, market and credit risk, which are usually quite similar across the enterprise, will typically benefit from a centralized approach. Such an approach increases the efficiency and effectiveness of risk management because it allows for the sharing and refinement of good practices throughout the organization.

To select the right approach, corporates first need to identify the risks inherent in their business model and then decide on the trade-offs between centralization and decentralization of their setup for each risk type. They might consider questions such as the following: Who is responsible for managing and controlling each risk type? Which management approach best fits the company's context and the nature of the risks? In the future, who should be responsible for the risks, and which processes and policies need to be updated or written anew? How should we deal with the shortcomings of the chosen approach (for example, how can we ensure sound and consistent models using a decentralized approach, and how can we strengthen risk culture in a centralized approach)?

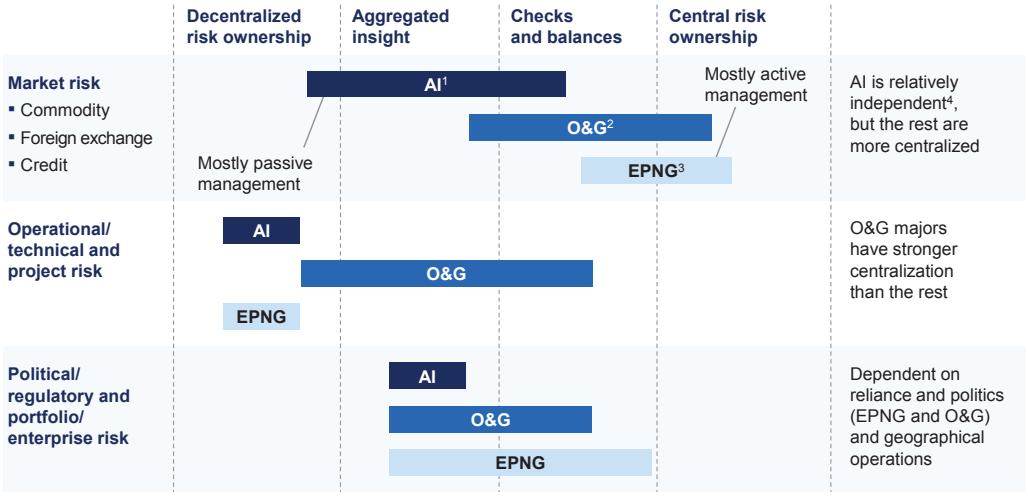
Industry preferences

Our survey revealed that the two industries we studied show different degrees of centralization across different risk types. Generally speaking, corporates in AI follow a decentralized approach, whereas energy companies are much more centralized. This can be explained by reminding ourselves of the core risks laid out earlier.

The quality risks in the AI industry can hardly be managed centrally; they must be taken care of by the line functions themselves (for example, on the production lines). On the other hand, the core risks in the energy industry respond well to centralized management: interaction with regulators and politicians is best dealt with by the regulatory-management group (which often reports directly to the CEO) in close cooperation with the management board.

Within that broad pattern, however, if we look at three main types of risk, the picture becomes more nuanced (Exhibit 3).[1]

Exhibit 3 The archetypes of different industries' risk DNA differ by risk type.



1 Advanced industries.
2 Oil and gas.
3 Energy, petroleum ,and natural gas.
4 Commodity risk in particular.

For market risk (that is, commodity, credit, and FX risks), we see different approaches. Consider commodity risk. In the energy industry, commodity-risk management is typically centralized within the trading group, which receives input from risk managers in the trading units. In advanced industries, however, commodity risks often reside with the business departments. For instance, we have seen a global AI corporation that had no central understanding of its exposure to changes in the price of steel. The reason was that product lines and plants typically signed their own contracts with suppliers, and these were not gathered in a central database—and so it was impossible for this company to hedge its steel-price exposure with any accuracy.

For credit risk, the approach used by companies in both industries is inconsistent, both between and within firms. Credit models are not the same in all parts of the organization; some sales teams, for example, do not explicitly consider counterparty risk.

For currency risk, most players in both industries have a central treasury that is responsible for controlling and managing FX risk for the whole organization.

Across industries, operational and technical risk is typically controlled and managed within businesses. This seems a rather natural setup given the diversity of operational risks and the expert knowledge needed to deal with them. However, some companies we observed are now striving to centralize their management of operational risk. This is no doubt due to recent major operational-risk events (such as the Macondo oil spill in the Gulf of Mexico) that appear to have resulted, at least in part, from slack execution of on-site procedures and inadequate risk control by contractors. A more rigorous centralization of operational-risk management will allow companies to identify and define standards of good practice and roll them out throughout the enterprise—and beyond, to contractors.

1 Note that in this exhibit, we split the energy sector into two segments: first, energy, petroleum, and natural gas (typically the incumbents that provide or are mostly concerned with electricity generation and the distribution of energy), and second, oil and gas (in particular, the oil majors).

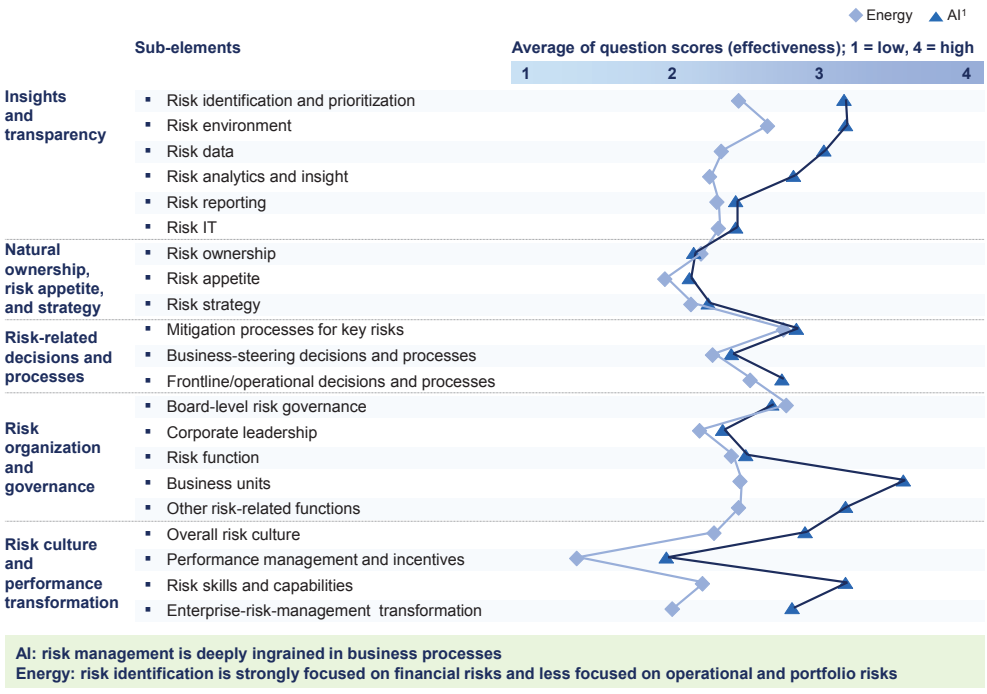
Management of political and regulatory risks is typically handled in all industries by a specialized department that operates in close contact with the management board and other departments (such as the businesses to understand their needs) and by the compliance function.

Industries' ERM performance and ways to improve

Across our survey sample, we noticed that advanced industries in general fared better than the energy industry in most parts of the risk framework shown in Exhibit 2. This is particularly evident in two elements: risk insight and transparency, and risk organization and governance, especially with regard to collaboration between risk and other functions (Exhibit 4). AI's better performance can be explained by the risk-champion networks mentioned earlier, which allow for an unbiased view of exposure across all risk types and involve the whole organization more forcefully than the centralized approach typically favored by energy companies.

Still, companies in both industries could further improve risk management in selected dimensions. We have compiled some suggestions for AI, energy, and both kinds of companies that can add value for most players.

Exhibit 4 Industries show different strengths and weaknesses across the risk framework.



1 Advanced industries.

Advanced industries

Most AI companies use fairly sophisticated models in departments such as logistics and supply-chain management and in managing specific technical risks. In contrast, their risk-management departments often rely on relatively simple models to assess the impact of individual risks. The industry could benefit from a more quantitative approach to assessing the exposures that reside in different parts of the organization. In particular, companies should consider a more robust application of the risk-book approach (that is, the rigorous mapping and aggregation of long and short positions in order to understand net exposure) to

improve transparency into core commodity exposures such as steel, aluminum, and energy, as well as a more rigorous application of forward price models and Monte Carlo simulations to quantify risks. Company-wide hedging strategies can then accurately limit and mitigate these risks. However, we would not suggest centralizing specialized models in the risk-management department, because this would detach these models from experts in the line functions.

In general, the risk-management department in AI companies could often take more of a leading role in harmonizing risk assumptions and approaches throughout the enterprise—for example, in defining limits, developing scenarios, and linking these scenarios to strategic and annual plans.

In other dimensions, the central risk function could move toward a stronger role as a sparring partner for the businesses and other groups. This will require the assignment of dedicated individuals within the central risk-management department to certain risk types; these people must then develop stronger capabilities. This would allow the risk group to challenge and double-check the identification and assessment of individual risks made by the businesses. Even better, the group can develop recommendations for individual businesses and better support other departments in tracking and controlling mitigation measures.

Energy
In the energy industry, we typically see strong transparency on core commodity exposures (via risk books) and sophisticated models used to define and execute hedging strategies. However, we also observe a bias toward focusing on those risks that are relatively easy to quantify (such as trading-related risks) while treating other risks (such as operational risk) in a comparatively superficial way. To counteract this bias, energy companies should foster a dedicated network of risk practitioners and ensure common risk-management standards throughout the organization. This would allow the central risk function to stay in the loop on risks emerging throughout the enterprise and foster the involvement of individual departments with risk topics. In turn, this moves companies closer to an integrated view of the various risk types and allows them to make educated trade-offs.

Overarching
For both kinds of companies, a number of moves could help extract more value from ERM. Five will be most powerful:

1. developing a better definition of risk appetite and limit setting

2. improving stress testing

3. developing a strong risk culture

4. deploying the “three lines of defense”

5. improving the management of credit risk

Risk appetite and limit setting. Many of the companies we spoke to consider the most crucial elements of risk to be risk appetite (that is, the definition of the nature of risks the company wants to take, along with quantitative limits to the amount of those risks it assumes) and risk strategy (that is, the implications of risk appetite on corporate strategy). However, they often struggle with implementation. Companies sometimes fail to develop limits for each relevant risk type; in other cases, the chosen risks can seem to users to have been pulled out of thin air, with no consistency among them.

An integrated view is necessary because risks are often strongly interdependent. Consider the case of a derivative deal that is done for hedging purposes; it can be struck “over the counter” or executed through

a clearinghouse. In the first case, the corporate bears the full counterparty credit risk; if the counterparty defaults, the company may never receive any payment due under the derivative contract. In the second case, the company suffers no counterparty credit risk (its counterparty is the clearinghouse, which protects itself through margin agreements with its members) but instead faces liquidity risk; the company will need to post collateral with the clearinghouse if the derivative moves against it. In both cases, the size of the exposure is driven by market risk, since market prices determine whether and by how much the derivative is in the money.

In order to bring the concepts of risk appetite and risk strategy to life, companies must first define measurable key performance indicators (KPIs) for all essential risks. Naturally, these will differ by risk type. Importantly, management needs to agree on "severity thresholds" for each risk type: for example, what extent of negative media coverage would qualify a reputational-risk event as severe? What kind of gap in the liquidity profile makes a severe event for liquidity risk? Which price fluctuations would do the same for market risk?

After having agreed on the KPIs and their thresholds, the company needs to decide where it is the natural owner of particular risks. A natural owner of a risk can achieve competitive advantages from taking it on and can generate attractive returns from it. The company should keep such risks, but it must also decide how to deal with those risks of which it is not the natural owner. Should it pass them on? Avoid them? Insure against them? Additionally, the company should decide how much of each risk it can bear.

These decisions ultimately need to be made by the board since they are intrinsically linked to corporate strategy. However, we often see boards struggle in the absence of a framework for meaningful discussions of their risk appetite. A matrix such as the one shown in Exhibit 5 can be a useful tool to facilitate the discussion by allowing board members to prioritize which risks to take and to decide in which parts of the company to take them.

After undertaking this qualitative prioritization exercise, companies should translate the "moons"—the low, medium, and high indicators of risk appetite—into thresholds for the KPIs they defined earlier.

Exhibit 5 The board should link risk appetite for individual risk types and units to the overall strategy.

Quality assurance for the risk appetite and strategy is essential. Companies can periodically challenge these documents and compare them with the risks that competitors take when this information is available. Moreover, they can detect breaches of the risk appetite and trigger predesigned contingency and escalation measures, thus making the risk appetite and strategy a meaningful tool for steering the company.

Stress testing. Most companies that participated in our survey make sure that they not only calculate the expected trajectory of their strategic plan but also consider upside and downside scenarios related to it. However, for many, the calculation of downside scenarios—that is, the stress testing of the business plan—does not have real impact on the decisions that are made. Specifically, we see four main areas where modifications to current stress-testing approaches could increase the relevance of the activity.

— **Stress-testing goals and scenario definition.** Often, corporates are not explicit on the objectives of calculating downside scenarios. In particular, they often are not specific about the probabilities they attach to each scenario. This obviously makes it difficult for management to use stress-test results as the basis for decisions—how can you gauge the trade-offs among benefits and costs of risk-mitigation measures if you don't know with what probability certain negative effects might materialize?

  In defining their downside scenarios, corporates should ensure a balanced mix between severe but very improbable events (such as major natural disasters) and more moderate, but more probable, scenarios (such as a further tightening of macroeconomic conditions).

  It is worthwhile to include senior management in defining the scenarios early on so that their opinions and insights are taken into account. That also makes it more likely that they will deem the stress-testing results relevant.

— **Technical stress testing and scenario calculation.** We typically see corporates focus only on the "first order" effects of shocks. Often, however, the dynamic that evolves after a shock needs much more thorough modeling. How might supply and demand change, and what are the dynamics until they reach a new equilibrium? How would the company and its competitors react to shocks? What might the midterm effects be on the sector? The trick to approaching such questions lies in the combination of thorough multiperiod modeling and the employment of complementary tools, such as the Delphi methodology or war-gaming exercises.

— **Derivation of implications.** Once the model is set up and parameterized correctly, it is essential to highlight implications for the balance sheet and the P&L and to break these down to individual business units or product lines. Discussion of stress-testing results at this level of detail moved one company, for example, to keep a product line despite its general low profitability due to the resilience it adds in crises.

  Moreover, stress-testing scenarios should come with a set of predefined contingency plans (actions and responsibilities) that allow for a swift reaction if crisis hits. To ensure resilience, corporates should develop a dashboard containing the most important business-plan drivers and ensure their timely and convenient tracking (for example, using a traffic-light system).

— **Alignment throughout the company.** Overall, it is important that stress testing is not an exercise that is simply performed by the risk-management group. It should involve the entire organization. This includes senior management being involved in scenario definition, but it also means coordinating experts throughout the company (for example, experts in macroeconomic

forecasting, technical areas, and strategic planning) to ensure the stress-testing exercise is relevant—and to encourage a sound understanding of the discipline's limitations. A stress-testing model will almost certainly not give "the ultimate correct result." But it can serve as a powerful communication device to structure the discussion on business-plan assumptions and strategic options.

Risk culture. Many corporates recognize that risk culture is one of the most essential pillars of a comprehensive risk-management approach. As discussed earlier, this holds true in particular for a decentralized approach, but many that follow a centralized approach also recognize the necessity of ensuring a sound risk culture permeates all departments. However, most of the companies we talked to continue to struggle with dedicated measures to build and continuously improve their risk culture; it is seen more as something that just happens than as a topic that can be actively shaped and built.

A systematic approach to risk culture can be established, and it's not rocket science. The first step is to obtain transparency on the current state of risk culture throughout the enterprise. For this, it is useful to run a risk-culture survey, either via in-depth interviews of selected respondents or through a broader web-based survey. Typically, we assess ten key dimensions of risk culture (Exhibit 6).

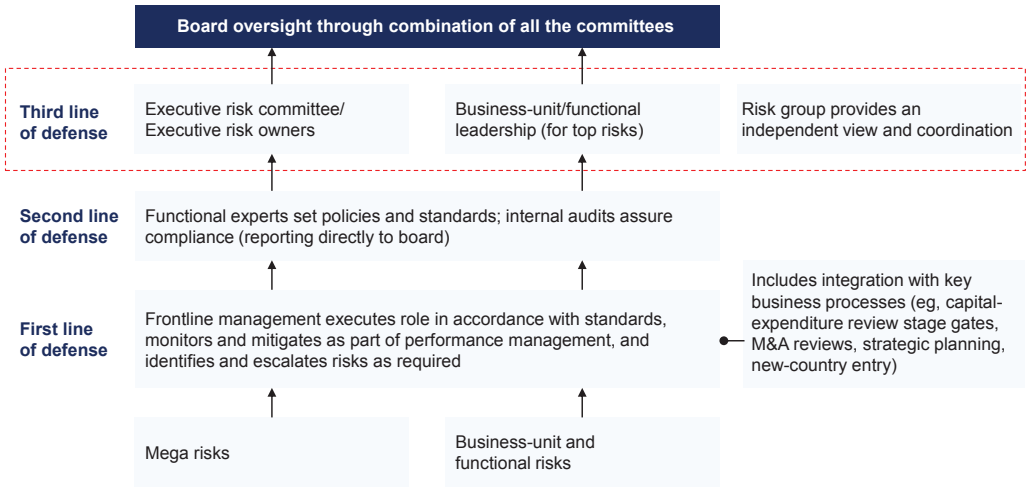
Exhibit 6 Risk culture can be qualified in ten dimensions.

Transparency of risk: definition, communication, and tracking of risks	**Acknowledgement of risk:** methodical and direct approach to recognizing and surfacing risks
1 ***Communication:*** a culture where warning signs of both internal or external risks are shared 2 ***Tolerance:*** a culture where leadership has communicated a clear risk appetite or has presented a coherent approach or strategy 3 ***Level of insight:*** a culture where the organization understands the risks it is running	4 ***Confidence:*** a culture where people do not believe their organization is immune to or insulated from risk as a result of its superior position or people, that it doesn't have an "edge" 5 ***Openness:*** a culture where management and employees feel empowered about passing on bad news or learning from mistakes 6 ***Challenge:*** a culture where individuals challenge one another's attitudes, ideas, and actions
Responsiveness to risk: rapid responses to and a proactive attitude toward risk	**Respect for risk:** adherence to rules and culture that fosters cooperation rather than competition
7 ***Level of care:*** a culture which instills a responsibility to react to situations or to care about the outcome of actions and decisions 8 ***Speed of response:*** a culture where the organization perceives external changes, reacts quickly, and embraces innovation or impact of change	9 ***Cooperation:*** a culture where groups do not take risks or embrace projects which benefit them to the detriment of the wider organization or are not in line with the broader organization's risk appetite 10 ***Adherence to rules:*** a culture where people's risk appetites are aligned with the organization's, reducing the probability of fraud or an operational or reputational event

After identifying the current status and potential shortcomings, the company can articulate target risk norms and any necessary mind-set shifts, then implement these through a variety of processes. Potential measures include a dedicated communication program and visible actions, the review of training programs, the revision of compensation programs and promotion mechanisms, the modification of risk-governance structures (for example, escalation mechanisms and rewards for accountability), the harmonization and specification of guidelines, or the reinforcement of values and professional standards.

Three lines of defense. A typical approach to risk management in financial industries is to establish three lines of defense (Exhibit 7). Although elements of this concept exist implicitly in many corporates, a more formal approach might further improve risk management by clarifying roles and responsibilities. This would help to avoid a "blame game" arising when risks materialize.

Exhibit 7 A 'lines of defense' risk-governance framework can help in managing risk throughout the organization.



The three lines typically include the following:

— **Frontline management.** In nonfinancial companies, frontline management is typically closest to most risks, including operational, project, or counterparty risks. Consequently, it plays a key role in managing risk, both with respect to which risks to take and the amount of risk to assume. This almost always includes trade-off decisions that go hand in hand with managing these risks (for example, the cost of risk-mitigation measures). Assessing these and deciding on the path forward is one of frontline management's core competencies, though the front line often thinks of these decisions as entrepreneurship rather than risk management. These trade-off decisions can be clearer in some areas (for example, production of high-quality products with almost no margin for error) and more blurry in others (for instance, risks taken on when signing a large and complex sales contract with a customer), but it is frontline management's duty to make these decisions with a conscious consideration of the risks involved.

— **Risk-management experts and internal audit.** The second line of defense usually encompasses two key tasks: setting the frame for frontline management and monitoring compliance using this frame. The first task is typically performed by the risk function. It strives to identify key elements to build the company's risk-management framework (for example, quantitative measures and qualitative guidance), supports the risk committee in establishing this framework in the form of policies and standards, and monitors frontline management in several ways. Depending on the risk type and the corresponding risk-management archetype, a variety of tools can help. Examples include the calculation of qualitative metrics, the derivation of a limit system, and engagement in an active dialogue with frontline management on risks taken. Internal audit is fully focused on compliance with company's internal policies and standards and with external guidelines (for example, regulation and laws).

— **Executive risk committee and business-unit leadership.** The third line of defense bears the ultimate responsibility for risk management across a company. Its responsibility is to guarantee the proper functioning of the risk wheel, ensure that the company is aware of its key risks, define the appetite with respect to these risks, and cascade this down into the organization via an appropriate framework to promote sound implementation of processes, organization, and culture. It must also ensure through the internal-audit function that this framework is adhered to properly.

Credit risk. Credit risk arises in many areas, such as in treasury (deposits with banks, short- and long-term investments), business units (advance payments with suppliers, accounts receivable from customers), or the trading department (the counterparty credit risk of uncleared over-the-counter derivatives deals for hedging purposes).

A comprehensive approach to credit risk requires the combination of central standards (for limit setting, reporting, and methodology development) and decentralized management. The key body is the credit-risk committee, which should include participants from various departments such as ERM, treasury, sales, control, trading, and origination. Typically, the credit-risk committee convenes at least quarterly, though organizations should be able to call ad hoc meetings within one week. Among the responsibilities of the credit-risk committee are the definition of limits, remediation of conflicts among departments (for example, if deals by different units with the same counterparty in aggregate exceed individual exposure limits), review and authorization of individual large-exposure cases, and evaluation of overall performance in credit-risk management and potential decisions on credit-risk policy adaptations.

However, the actual management of credit risk (in accordance with limits) should be done by the units where credit risk arises. These units should hold responsibility for managing their counterparties, as well as for choosing the right instruments for their purposes (for example, the mix of unsecured, collateralized, and cleared deals for the trading department) because they typically know the peculiarities of their counterparties much better than a central risk department.

There is no single approach to ERM that can be considered the holy grail for all companies in all sectors. The application of risk management must take into account the biggest risks a company faces alongside specifics such as its current risk culture. By carefully tailoring the approach to a company's individual characteristics, however, risk management can become an extremely powerful tool to help senior management reach its objectives.

Sven Heiligtag is a principal in McKinsey's Hamburg office, **Andreas Schlosser** is a consultant in the Munich office, and **Uwe Stegemann** is a director in the Cologne office.

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**
   André Brodeur and Gunnar Pritsch
3. **Incorporating risk and flexibility in manufacturing footprint decisions**
   Eric Lamarre, Martin Pergler, 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**
   Andrew Freeman, Gunnar Pritsch, and Uwe Stegemann
6. **Probabilistic modeling as an exploratory decision-making tool**
   Andrew Freeman and Martin Pergler
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**
   Eric Lamarre and Martin Pergler
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**
    Gabriel Brennan, Martin Fest, Matthias Heuser, Luca Martini, Thomas Poppensieker, Sebastian Schneider, Uwe Stegemann, and Eckart Windhagen
13. **Developing a postcrisis 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

41. **Between deluge and drought: The divided future of European bank-funding markets**
Arno Gerken, Frank Guse, Matthias Heuser, Davide Monguzzi, Olivier Plantefeve, and Thomas Poppensieker

42. **Risk-based resource allocation: Focusing regulatory and enforcement efforts where they are needed the most**
Diana Farrell, Biniam Gebre, Claudia Hudspeth, and Andrew Sellgren

43. **Getting to ERM: A road map for banks and other financial institutions**
Rob McNish, Andreas Schlosser, Francesco Selandari, Uwe Stegemann, and Joyce Vorholt

44. **Concrete steps for CFOs to improve strategic risk management**
Wilson Liu and Martin Pergler

45. **Between deluge and drought: Liquidity and funding for Asian banks**
Alberto Alvarez, Nidhi Bhardwaj, Frank Guse, Andreas Kremer, Alok Kshirsagar, Erik Lüders, Uwe Stegemann, and Naveen Tahilyani

46. **Managing third-party risk in a changing regulatory environment**
Dmitry Krivin, Hamid Samandari, John Walsh, and Emily Yueh

47. **Next-generation energy trading: An opportunity to optimize**
Sven Heiligtag, Thomas Poppensieker, and Jens Wimschulte

48. **Between deluge and drought: The future of US bank liquidity and funding**
Kevin Buehler, Peter Noteboom, and Dan Williams

49. **The hypotenuse and corporate risk modeling**
Martin Pergler

50. **Strategic choices for midstream gas companies: Embracing Gas Portfolio @ Risk**
Cosimo Corsini, Sven Heiligtag, and Dieuwert Inia

51. **Strategic commodity and cash-flow-at-risk modeling for corporates**
Martin Pergler and Anders Rasmussen

52. **A risk-management approach to a successful infrastructure project: Initiation, financing, and execution**
Frank Beckers, Nicola Chiara, Adam Flesch, Jiri Maly, Eber Silva, and Uwe Stegemann

53. **Enterprise-risk-management practices: Where's the evidence? A survey across two European industries**
Sven Heiligtag, Andreas Schlosser, and Uwe Stegemann

McKinsey Working Papers on Risk
February 2014
Designed by Global Editorial Services

www.mckinsey.com