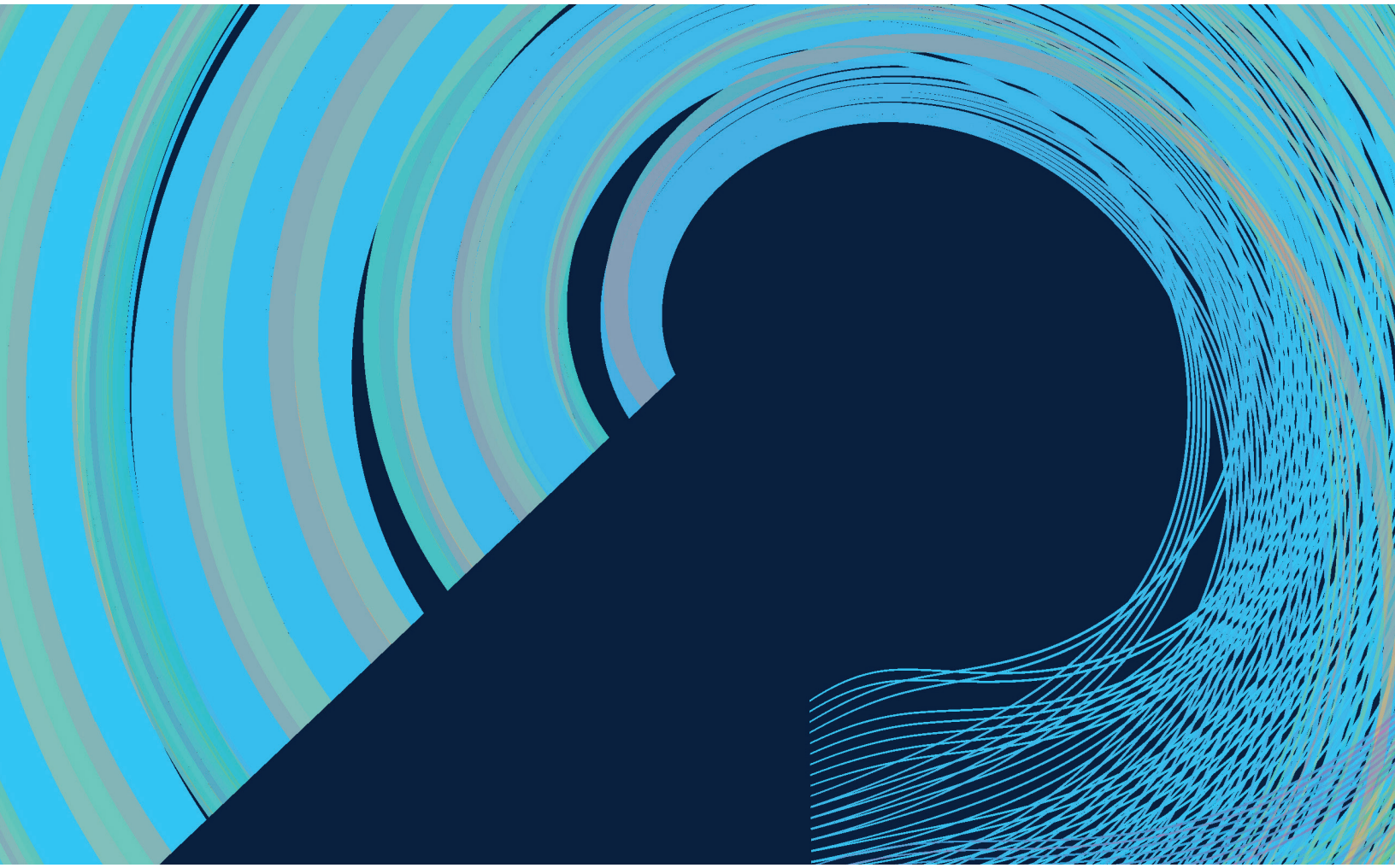
# Value and resilience through better risk management

In a risk environment that is growing more perilous and costly, boards need to help steer their companies toward resilience and value by embedding strategic risk capabilities throughout the organization.

Daniela Gius, Jean-Christophe Mieszala, Ernestos Panayiotou, and Thomas Poppensieker



SEPTEMBER 2018 • RISK PRACTICE

Today's corporate leaders navigate a complex environment that is changing at an ever-accelerating pace. Digital technology underlies much of the change. Business models are being transformed by new waves of automation, based on robotics and artificial intelligence. Producers and consumers are making faster decisions, with preferences shifting under the influence of social media and trending news. New types of digital companies are exploiting the changes, disrupting traditional market leaders and business models. And as companies digitize more parts of their organization, the danger of cyberattacks and breaches of all kinds grows.

Beyond cyberspace, the risk environment is equally challenging. Regulation enjoys broad popular support in many sectors and regions; where it is tightening, it is putting stresses on profitability. Climate change is affecting operations and consumers and regulators are also making demands for better business conduct in relation to the natural environment. Geopolitical uncertainties alter business conditions and challenge the footprints of multinationals. Corporate reputations are vulnerable to single events, as risks once thought to have a limited probability of occurrence are actually materializing.

## The role of the board and senior executives

Risk management at nonfinancial companies has not kept pace with this evolution. For many nonfinancial corporates, risk management remains an underdeveloped and siloed capability in the organization, receiving limited attention from the most senior leaders. From over 1,100 respondents to McKinsey's Global Board Survey for 2017, we discovered that risk management remains a relatively low-priority topic at board meetings (exhibit).

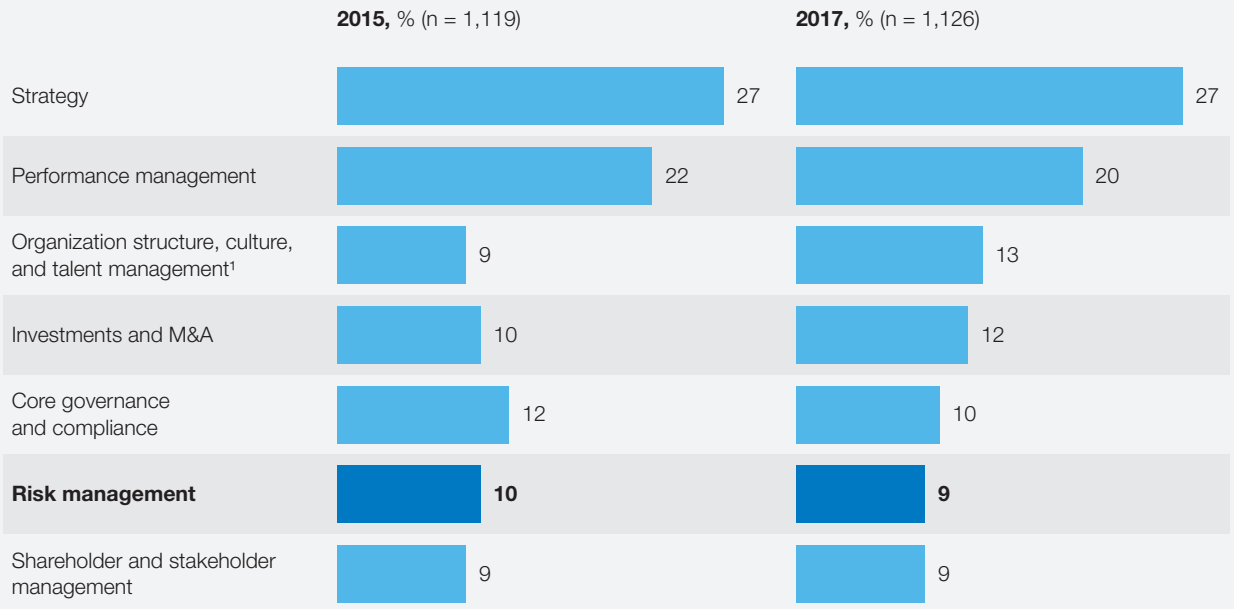
Boards spend only 9 percent of their time on risk—slightly less than they did in 2015. Other questions in the survey revealed that only 6 percent of respondents believe that they are effective in managing risk (again, less than in 2015). Some individual risk areas are relatively neglected, and even cybersecurity, a core risk area with increasing importance, is addressed by only 36 percent of boards. While many senior executives stay focused on strategy and performance management, they often fail to challenge capabilities or strategic decisions from a risk perspective (see sidebar, "A long way to go"). A reactive approach to risks remains too common, with action taken only after things go wrong. The result is that boards and senior executives needlessly put their companies

# A long way to go

In 2016, McKinsey interviewed a sample of large listed companies in the United Kingdom that had included viability statements in their annual reports. The viability statement—a reporting requirement for London listed companies introduced in 2014—is designed to provide investors with an assessment of the long-term viability of the company. Responses revealed that many non–financial services corporates had never before modeled the impact of an adverse scenario on their financials prior to the new reporting requirement. Some of the companies that undertook analytical exercises on the impact of macroeconomic variables as part of their analysis for the statement had not also modeled for individual crises, such as a cybersecurity attack. Furthermore, most of the non–financial services companies that we interviewed had not yet used the lessons and insights from analytical exercises to inform their strategic decision making.

Exhibit **McKinsey surveys of more than 1,100 leading global companies reveal that boards devote a relatively small share of time to risk management.**

**"Please indicate the % of time your board spends on the following topics during its meetings"**




Note: Figures may not sum to 100%, because of rounding

[1] In the past, this category was called "organizational health and talent management."

Source: McKinsey Global Board Survey, April 2015 and 2017

at risk, while personally taking on higher legal and reputational liabilities.

Boards have a critical role to play in developing risk-management capabilities at the companies they oversee. First, boards need to ensure that a robust risk-management operating model is in place. Such a model allows companies to understand and prioritize risks, set their risk appetite, and measure their performance against these risks. The model should enable the board and senior executives to work with businesses to eliminate exposures outside the company's appetite statement, reducing the risk profile where warranted, through such means as quality controls and other operational processes. On strategic opportunities and risk trade-offs, boards should foster explicit discussions and decision making among top management and the businesses. This will enable the efficient deployment of scarce risk resources and the active, coordinated management of risks across the organization. Companies will then be prepared to address and manage emerging crises when risks do materialize.

## A sectoral view of risks

Most companies operate in a complex, industry-specific risk environment. They must navigate macroeconomic and geopolitical uncertainties and face risks arising in the areas of strategy, finance, products, operations, and compliance and conduct. In some sectors, companies have developed advanced approaches to managing risks that are specific to their business models. These approaches can sustain significant value. At the same time companies are

challenged by emerging types of risks for which they need to develop effective mitigation plans; in their absence, the losses from serious risk events can be crippling.

- *Automotive companies* are controlling supply-chain risks with sophisticated monitoring models that allow OEMs to identify potential risks upfront across the supply chain. At the same time, auto companies must address the strategic challenge of shifting toward electric-powered and autonomous vehicles.

- *Pharma companies* seek to manage the downside risk of large investments in their product portfolio and pipeline, while addressing product quality and patient safety to comply with relevant regulatory requirements.

- *Oil and gas, steel, and energy companies* apply advanced approaches to manage the negative effects of financial markets and commodity-price volatility. As social and political demands for cleaner energy are increasing, these companies are actively pursuing growth opportunities to shift their portfolios in anticipation of an energy transition and a low-carbon future.

- *Consumer-goods companies* protect their reputation and brand value through sound practices to manage product quality as well as labor conditions in their production facilities. Yet they are constantly challenged to meet consumers' ever-changing tastes and needs, as well as consumer-protection regulations.

## Toward proactive risk management

An approach based on adherence to minimum regulatory standards and avoidance of financial loss creates risk in itself. In a passive stance, companies cannot shape an optimal risk profile according to their business models nor adequately manage a fast-moving crisis. Eschewing a risk approach comprised of short-term performance initiatives focused on revenue and costs, top performers deem risk management as a strategic asset, which can sustain significant value over the long term. Inherent in the proactive approach are several essential components.

### Strategic decision making

More rigorous, debiased strategic decision making can enhance the longer-term resilience of a company's business model, particularly in volatile markets or externally challenged industries. Research shows that the active, regular reevaluation of resource allocation, based on sound assessments of risk and return trade-offs (such as entering markets where the business model is superior to the competition), creates more value and better shareholder returns.[1] Flexibility is empowering in a dynamic marketplace. Many companies use hedging strategies to insure against market uncertainties. Airlines, for example, have been known to hedge future exposures to fuel-price fluctuations, a move that can help maintain profitability when prices climb. Likewise, strategic investing, based on a longer-term perspective and a deep understanding of a company's core proposition, generates more value than opportunistic moves aiming at a short-term bump in the share price.

### Debiasing and stress-testing

Approaches that include debiasing and stress-testing help senior executives consider previously overlooked sources of uncertainty to judge whether the company's risk-bearing capacity can absorb their potential impact. A utility in Germany, for example, improved decision making by taking action to mitigate behavioral biases. As a result, it separated its renewables business from its conventional power-generation operations. In the aftermath of the Fukushima disaster, which sharply raised interest in environmentally friendly power generation, the utility's move led to a significant positive effect on its share price (15 percent above the industry index).

### Higher-quality products and safety standards

Investments in product quality and safety standards can bring significant returns. One form this takes in the energy sector is reduced damage and maintenance

costs. At one international energy company, improved safety standards led to a 30 percent reduction in the frequency of hazardous incidents. Auto companies with reputations built on safety can command higher prices for their vehicles, while the better reputation created by higher quality standards in pharma creates obvious advantages. As well as the boost in demand that comes from a reputation for quality, companies can significantly reduce their remediation costs—McKinsey research suggests that pharma companies suffering from quality issues lose annual revenue equal to 4 to 5 percent of cost of goods sold.

### Comprehensive operative controls

These can lead to more efficient and effective processes that are less prone to disruption when risks materialize. In the auto sector, companies can ensure stable production and sales by mitigating the risk of supply-chain disruption. Following the 2011 earthquake and tsunami, a leading automaker probed potential supply bottlenecks and took appropriate action. After an earthquake in 2016, the company quickly redirected production of affected parts to other locations, avoiding costly disruptions. In high-tech, companies applying superior supply-chain risk management can achieve lasting cost savings and higher margins. One global computer company addressed these risks with a dedicated program that saved $500 million during its first six years. The program used risk-informed contracts, enabling suppliers to lower the costs and risks of doing business with the company. The measures achieved supply assurance for key components, particularly during market shortages, improved cost predictability for components that have volatile costs, and optimized inventory levels internally and at suppliers.

### Stronger ethical and societal standards

To achieve standing among customers, employees, business partners, and the public, companies can apply ethical controls on corporate practices end to end. If appropriately publicized and linked to corporate social responsibility, a program of better ethical standards can achieve significant returns in the form of heightened reputation and brand recognition. Customers, for example, are increasingly willing to pay a premium for products of companies that adhere to tighter standards. Employees too appreciate being associated with more ethical companies, offering a better working environment and contributing to society.

## The three dimensions of effective risk management

Ideally, risk management and compliance are addressed as strategic priorities by corporate leadership and day-to-day management. More often the reality is that these areas are delegated to a few people at the corporate center working in isolation from the rest of the business. By contrast, revenue growth or cost savings are deeply embedded in corporate culture, linked explicitly to profit-and-loss (P&L) performance at the company level. Somewhere in the middle are specific control capabilities regarding, for example, product safety, secure IT development and deployment, or financial auditing.

To change this picture, leadership must commit to building robust, effective risk management. The project is three-dimensional: 1) the risk operating model, consisting of the main risk management processes; 2) a governance and accountability structure around these processes, leading from the business up to the board level; and 3) best-practice crisis preparedness, including a well-articulated response playbook if the worst case materializes.

### 1. Developing an effective risk operating model

The operating model consists of two layers, an enterprise risk management (ERM) framework and individual frameworks for each type of risk. The ERM framework is used to identify risks across the organization, define the overall risk appetite, and implement the appropriate controls to ensure that the risk appetite is respected. Finally, the overarching framework puts in place a system of timely reporting and corresponding actions on risk to the board and senior management. The risk-specific frameworks

address all risks that are being managed. These can be grouped in categories, such as financial, nonfinancial, and strategic. Financial risks, such as liquidity, market, and credit risks, are managed by adhering to appropriate limit structures; nonfinancial risks, by implementing adequate process controls; strategic risks, by challenging key decisions with formalized approaches such as debiasing, scenario analyses, and stress testing. While financial and strategic risks are typically managed according to the risk-return trade-off, for nonfinancial risks, the potential downside is often the key consideration.

As well as assessing risk based on likelihood and impact, companies must also assess their ability to respond to emerging risks. Capabilities and capacities needed to manage these risks should be evaluated and gaps filled accordingly. Of particular importance in crisis management is the timeliness of an effective response when things go awry. The highly likely, high-impact risk events on which risk management focuses most of its attention often emerge with disarming velocity, taking many companies unawares.
To be effective, the enterprise risk management framework must ensure that the two layers are seamlessly integrated. It does this by providing clarity on risk definitions and appetite as well as controls and reporting.

- *Taxonomy.* A company-wide risk taxonomy should clearly and comprehensively define risks; the taxonomy should be strictly respected in the definition of risk appetite, in the development of risk policy and strategy, and in risk reporting. Taxonomies are usually industry-specific, covering strategic, regulatory, and product risks relevant to the industry. They are also determined by company characteristics, including the business model and geographical footprint (to incorporate specific country and legal risks). Proven risk-assessment tools need to be adopted and enhanced continuously with new techniques, so that newer risks (such as cyberrisk) are addressed as well as more familiar risks.

## Finding the right level of risk appetite

Companies need to find the right level of risk appetite, which helps ensure long-term resilience and performance. Risk appetite that is too relaxed or too restrictive can have severe consequences on company financials, as the following two examples indicate:

**Too relaxed.** One nuclear energy company set its standards for steel equipment in the 1980s and did not review them even when the regulations changed. When the new higher standards were applied to the manufacture of equipment for nuclear power plants, the company fell short of compliance. An earlier adaptation of its risk appetite and tolerance levels would have been significantly less costly.

**Too restrictive.** A pharma company set quality tolerances to produce a drug to a significantly stricter level than what was required by regulation. At the beginning of production, tolerance intervals could be fulfilled, but over time, quality could no longer be assured at the initial level. The company was unable to lower standards, as these had been communicated to the regulators. Ultimately, production processes had to be upgraded at a significant cost to maintain the original tolerances.

- *Risk appetite.* A clear definition of risk appetite will translate risk-return trade-offs into explicit thresholds and limits for financial and strategic risks, such as economic capital, cash-flow at risk, or stressed metrics. In the case of nonfinancial risks like operational and compliance risks, the risk appetite will be based on overall loss limits, categorized into inherent and residual risks (see sidebar, "Finding the right level of risk appetite").

- *Risk control processes.* Effective risk control processes ensure that risk thresholds for the specified risk appetite are upheld at all levels of the organization. Leading companies are increasingly building their control processes around big data and advanced analytics. These powerful new capabilities can greatly increase the effectiveness and efficiency of risk monitoring processes. Machine-learning tools, for example, can be very effective in monitoring fraud and prioritizing investigations; automated natural language processing within complaints management can be used to monitor conduct risk.

- *Risk reporting.* Decision making should be informed with risk reporting. Companies can regularly provide boards and senior executives with insights on risk, identifying the most relevant strategic risks. The objective is to ensure that an independent risk view, encompassing all levels of the organization, is embedded into the planning process. In this way, the risk profile can be upheld in the management of business initiatives and decisions affecting the quality of processes and products. Techniques like debiasing and the use of scenarios can help overcome biases toward fulfilment of short-term goals. A North American oil producer developed a strategic hypothesis given uncertainties in global and regional oil markets. The company used risk modelling to test assumptions about cash flow under different scenarios and embedded these analyses into the reports reviewed by senior management and the board. Weak points in the strategy were thereby identified and mitigating actions taken.

## 2. Toward robust risk governance, organization, and culture

The risk operating model must be managed through an effective governance structure and organization with clear accountabilities. The governance model maintains a risk culture that strongly reinforces better risk and compliance management across the three lines of defense—business and operations, the compliance and risk functions, and audit. The approach recognizes the inherent contradiction in the first line between performance (revenue and costs) and risk (losses). The role of the second line is to review and challenge the first line on the effectiveness of its risk processes and controls, while the third line, audit, ensures that the lines one and two are functioning as intended.

- *Three lines of defense.* Effective implementation of the three lines involves the sharp definition of lines one and two at all levels, from the group level through the lines of business, to the regional and legal entity levels. Accountabilities regarding risk and control management must be clear. Risk governance may differ by risk type: financial risks are usually managed centrally, while operational risks are deeply embedded into company processes. The operational risk of any line of business is managed by the business owning the product-development, production, and sales processes. This usually translates into forms of quality control, but the business must also balance the broader impact of risk and P&L. In the development of new diesel engines, automakers lost sight of the balance between compliance risk and the additional cost to meet emission standards, with disastrous results. Risk or compliance functions can only complement these activities by independently reviewing the adequacy of operational risk

management, such as through technical standards and controls.

- *Reviewing the risk appetite and risk profile.* Of central importance within the governance structure are the committees that define the risk appetite, including the parameters for doing business. These committees also make specific decisions on top risks and review the control environment for enhancements as the company's risk profile changes. Good governance in this case means that risk decisions are considered within the existing divisional, regional, and senior-management governance structure of a company, supported by risk, compliance, and audit committees.

- *Integrated risk and compliance governance setup.* A robust and adequately staffed risk and compliance organization supports all risk processes. The integrated risk and compliance organization provides for single ownership of the group-wide ERM framework and standards, appropriate clustering of second-line functions, a clear matrix between divisions and control functions, and centralized or local control as needed. A clear trend is observable whereby the ERM layer responsible for group-wide standards, risk processes, and reporting becomes consolidated, whereas the expert teams setting and monitoring specific control standards for the business (including standards for commercial, technical compliance, IT or cyberrisks) become specialized teams covering both regulatory compliance as well as risk aspects.

- *Resources.* Appropriate resources are a critical factor in successful risk governance. The size of the compliance, risk, audit, and legal functions of nonfinancial companies (0.5 for every 100 employees, on average), are usually much smaller than those of banks (6.9 for every 100 employees). The disparity is partly a natural outcome of financial regulation, but some part of it reflects a capability gap in nonfinancial corporates. These companies usually devote most of their risk and control resources in sector-specific areas, such as health and safety for airlines and nuclear power companies or quality assurance for pharmaceutical companies. The same companies can, however, neglect to provide sufficient resources to monitor highly significant risks, such as cyberrisk or large investments.

- *Risk culture.* An enhanced risk culture covers mind-sets and behaviors across the organization. A shared understanding is fostered of key risks and risk management, with leaders acting as role models. Especially important are capability-building programs on risk as well as formal mechanisms to assess and reinforce sound risk management practices.

An enhanced risk culture covers mind-sets and behaviors across the organization. A shared understanding is fostered of key risks and risk management, with leaders acting as role models.

### 3. Crisis preparedness and response

A high-performing, effective risk operating model and governance structure, with a well-developed risk culture minimize the probability of corporate crises, without, of course, completely eliminating them. When unexpected crises strike at high velocity, multinational companies can lose billions in value in the first days and soon find themselves struggling to keep their market position. A best-in-class risk management environment provides the ideal conditions for preparation and response.

- *Ensure board leadership.* The most important action companies can take to prepare for crises is to ensure that the effort is led by the board and senior management. Top leadership must define the main expected threats, the worst-case scenarios, and the actions and communications that will be accordingly rolled out. For each threat, hypothetical scenarios should be developed for how a crisis will unfold, based on previous crises within and beyond the company's industry and region.

- *Strengthen resilience.* By mapping patterns that arose in previous crises, companies can test their own resilience, challenging key areas across the organization for potential weaknesses. Targeted countermeasures can then be developed in advance to strengthen resilience. This crucial aspect of crisis preparedness can involve reviewing and revising the terms and conditions for key suppliers, shoring up financials to ensure short-term availability of cash, or investing in advanced cybersecurity measures to protect essential data and software in the event of failures and breaches.

- *Develop action plans and communications.* Once these assessments are complete and resilience-building countermeasures are in place, the company can then develop action plans for each threat. The plans must be well articulated, founded on past crises, and address operational and technical planning, financial planning, third-party management, and legal planning. Care should be taken to develop an optimally responsive communications strategy as well. The correct strategy will enable frontline responders to keep pace with or stay ahead of unfolding crises. Communications failures can turn manageable crises into irredeemable catastrophes. Companies need to have appropriate scripts and process logic in place detailing the response to crisis situations, communicated to all levels of the organization and well anchored there. Airlines provide an example of the well-articulated response, in their preparedness for an accident or crash. Not only are detailed scripts in place, but regular simulations are held to train employees at all levels of the company.

- *Train managers at all levels.* The company should train key managers at multiple levels on what to expect and enable them to feel the pressures and emotions in a simulated environment. Doing this repeatedly and in a richer way each time will significantly improve the company's response capabilities in a real crisis situation, even though the crisis may not be precisely the one for which managers have been trained. They will also be valuable learning exercises in their own right.

- *Put in place a detailed crisis-response playbook.* While each crisis can unfold in unique and unpredictable ways, companies can follow a few fundamental principles of crisis response in all situations. First, establish control immediately after the crisis hits, by closely determining the level of exposure to the threat and identifying a crisis-response leader, not necessarily the CEO, who will direct appropriate actions accordingly. Second, involved parties—such as customers, employees, shareholders, suppliers, government agencies, the media, and the wider public—must be effectively engaged with a dynamic communications strategy. Third, an operational and technical "war room" should be

set up, to stabilize primary threats and determine which activities to sustain and which to suspend (identifying and reaching out to critical suppliers). Finally, a deliberate effort must be made to address and neutralize the root cause of the crisis and so bring it to an end as soon as possible.

In a digitized, networked world, with globalized supply chains and complex financial interdependencies, the risk environment has grown more perilous and costly. A holistic approach to risk management, based on the lessons, good and bad, of leading companies and financial institutions, can derive value from that environment. The path to risk resilience that is emerging is an effort, led by the board and senior management, to establish the right risk profile and appetite. Success depends on the support of a thriving risk culture and state-of-the-art crisis preparedness and response. Far from minimal regulatory adherence and loss avoidance, the optimal approach to risk management consists of fundamentally strategic capabilities, deeply embedded across the organization.

[1] See, for example, Yuval Atsmon, "How nimble resource allocation can double your company's value," August 2016, McKinsey.com; William N. Thorndike, Jr., *The Outsiders: Eight Unconventional CEOs and Their Radically Rational Blueprint for Success,* Boston, MA: Harvard Business Review Press, 2012; Rebecca Darr and Tim Koller, "How to build an alliance against corporate short-termism," January 2017, McKinsey.com.

**Daniela Gius** is a senior expert in McKinsey's Hamburg office, **Jean-Christophe Mieszala** is a senior partner in the Paris office, **Ernestos Panayiotou** is a partner in the Athens office, and **Thomas Poppensieker** is a senior partner in the Munich office.