McKinsey & Company

McKinsey on Risk

New risk challenges and enduring themes for the return

Table of contents

Risk and resilience

Risk culture

Extraordinary risks

Derisking

Introduction

The tenth issue of *McKinsey on Risk* arrives as spirits, battered by public-health and economic hardships, have been lifted by the appearance of COVID-19 vaccines. Vaccines are beginning to reach priority and vulnerable populations, such as healthcare workers and long-term care residents. Governments and institutions are promising ever-wider distribution in the months ahead. Serious questions remain about production timelines and the completeness of vaccine delivery. For most economies, epidemiological uncertainty is the main factor complicating the conditions of return. Yet nations, sectors, companies, and individuals have endured different challenges and will travel different recovery paths, depending on the damage done.

At the far end of the pandemic tunnel, some economies are demonstrating vibrant life. In other regions, the time for countries and organizations to grow again approaches at varying speeds. Those that prepare will benefit, as our lead article on the "emerging resilients" reveals. In the last recession, companies able to take thoughtful actions to balance growth, margin, and optionality separated themselves quickly from less resilient peers. Coming out of the current recession, which companies are poised to achieve "escape velocity"? Our authors—some of McKinsey's most influential leadership voices—discuss the dynamic business landscape while pointing to a venerable metric that can help companies adjust for the needed balance.

Taken as a whole, these discussions present McKinsey's latest thinking and recommendations on risk and resilience—including optimal strategies and necessary transformative actions. Resilience as a business concept took on significance during the financial crisis of 2008–09. As cyclical stress levels rose in the global economy, challenges were magnified and new uncertainties were generated. Faced with proliferating risks and spiking volatility, organizations began to realize the need for dynamic risk management, by which serious threats can be prioritized and addressed as they arise.

Today, as companies emerge from the pandemic-triggered economic crisis, risk organizations face extraordinary discontinuities on top of more familiar ongoing challenges. The highly complex risk landscape is marked by an accelerating digital revolution; massive environmental, regulatory, and industry changes precipitated by the changing climate; and rising stakeholder expectations about corporate behavior. Cost pressures, furthermore, mean that organizations must make significant, simultaneous improvements in risk efficiency and effectiveness.

In pursuit of these improvements, companies in all industries are applying advanced quantitative capabilities to support faster operational decision making. Most are launching digital and analytics transformations—digitizing services and processes, increasing efficiency with agile approaches and automation, improving customer engagement, and capitalizing on new analytical tools. The present crisis is also creating a moment in which financial institutions can rethink their entire model landscape and model life cycle. Artificial intelligence, which promises to redefine how businesses work, is already marshaling the power of data to transform a range of business activities and functions.

The inevitable consequences of all this innovation are elevated risk profiles, which many existing organizational approaches are incapable of addressing systematically. The following discussions illuminate the most compelling risk issues that companies in all sectors and geographies are confronting. Here, readers will find deep industry insight and structured risk-management approaches that are helping leaders build risk capabilities, strengthen institutional resilience, and navigate through this crisis toward restored performance.

Let us know what you think, at McKinsey_Risk@McKinsey.com and on the McKinsey Insights app.

Thomas Poppensieker
Chair, Risk & Resilience Editorial Board

Risk and resilience

The emerging resilients: Achieving 'escape velocity'

The experience of the fast movers out of the last recession teaches leaders emerging from this one to take thoughtful actions to balance growth, margins, and optionality.

by Cindy Levy, Mihir Mysore, Kevin Sneader, and Bob Sternfels
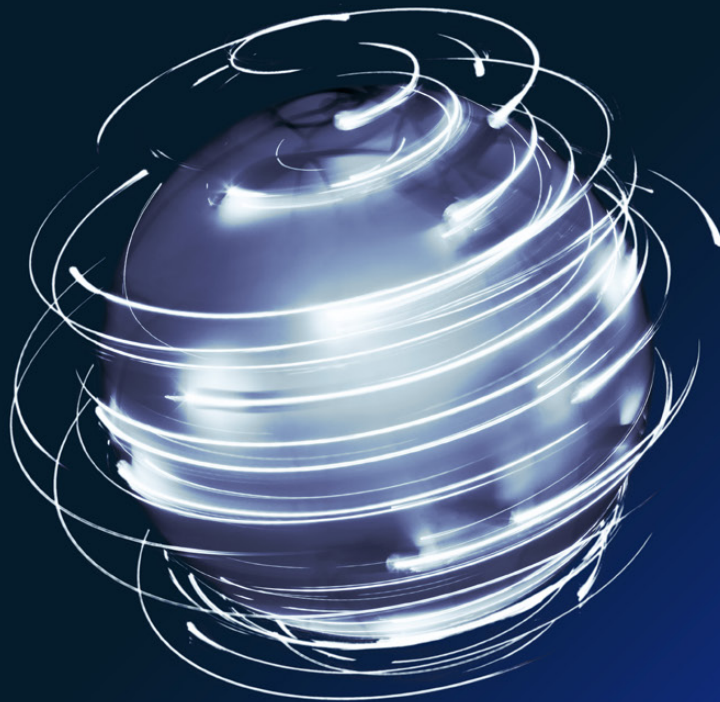
In 2019, McKinsey asked companies to prepare for the possibility of a recession. Of course, we had no idea then that the COVID-19 pandemic would be the trigger, nor that the recession would cut as deeply as it has. But it was clear then that the foregoing growth cycle was already of unusual duration. The pace was slowing, furthermore, and the potential for shocks was greater than for renewed growth. In the same article, we discussed what top-performing companies had done in the previous downcycle, the financial crisis of 2008–09. We looked at 1,500 public companies in Europe and the United States, analyzing performance on a sector-by-sector basis. Companies in the top quintile of their peers through that crisis were dubbed the "resilients."

Once economic and business results of the second quarter of 2020 became known, we began to hunt for the clues that were contained in nearly 1,500 earnings releases across Europe and the United States. This article seeks to understand whether the shape of the next class of resilients is visible in the data, and what lessons this would hold for companies within each sector.

The present downcycle: Six times faster than the previous one

Today, we are in the middle of the deepest recession in living memory. As pandemic-triggered lockdowns took hold around the world in early 2020, economies contracted quickly. The International Monetary Fund and World Bank foresee a global contraction in economic output in 2020 of around −5 percent; the Organisation of Economic Cooperation and Development estimates an even worse result, at −7.6 percent. At any rate, the drop will far exceed the last global contraction, which was −1.7 percent in 2009.

The distress has hit all industry sectors, some harder than others. Yet even in the relatively protected sectors of healthcare, pharmaceuticals, and technology, companies are seeing moderate declines in revenue. Heavily affected sectors have experienced revenue declines of between 25 percent and 45 percent. These include transportation and tourism, automotive, and oil and gas—sectors containing some of the largest employers in Europe and the United States.

We recognized that this downturn was driving stress into the economy at a much faster rate than was experienced in the financial crisis of 2008–09. To measure the extent and speed of the damage, we wanted a sounder guide than stock-market performance. An investigation of the companies in our database using the "Altman Z-Score" yielded promising results. This measurement was developed in 1968 by Edward I. Altman, now a professor emeritus of Finance at New York University's Stern School of Business. It is an equation originally designed to predict the probability of corporate bankruptcy. A company's Z-Score goes up if it has a well-established ability to grow margins (measured as EBIT[1]/assets) while increasing revenues (measured by revenue/assets) and maintaining optionality (measured by retained earnings/assets).[2]

We calculated the Z-Scores for approximately 1,500 European and North American companies in our database for both the last downcycle (2008–09) and the current one.[3] We used three categories in the results: "good standing," "gray zone," and "experiencing stress."[4] The Z-Scores revealed that in the financial crisis of 2008–09, 30 percent of companies moved to a higher-stress category by 2009, compared with where they were in precrisis 2007. Only 3 percent of observed companies improved their standing. By comparison, in 2020, 25 percent of companies had moved to a higher-stress category and 3 percent improved. The dynamics of 2009 and 2020 differ in one glaring respect: in the last recession, this movement occurred over 18

---

[1] Earnings before interest and taxes.
[2] Our research used a common form of the Z-Score, whose weighted determinants are as follows: $Z = 1.2X_1 + 1.4X_2 + 3.3X_3 + 0.6X_4 + 1.0X_5$, where X_1 = working capital/total assets, X_2 = retained earnings/total assets, X_3 = earnings before interest and taxes/total assets, X_4 = market value equity/book value of total liabilities, X_5 = sales/total assets, and Z = overall index. Edward I. Altman, "Predicting financial distress of companies: revisiting the Z-Score and ZETA® models," Leonard N. Stern School of Business, July 2000, stern.nyu.edu.
[3] Some companies were excluded from results because data or financial reports were unavailable at the time or because they were extreme industry outliers.
[4] These were the titles of Professor Altman's original categories except for "experiencing stress"; we substituted that title for his original, "headed for bankruptcy," since our research is not focused on bankruptcy.

months, while in the present crisis, the economy has arrived at about the same point in three months' time—six times faster (Exhibit 1).

Fast and deep—but for how long?

Our recent conversations with business leaders suggest that the high level of external uncertainties—political, social, and epidemiological—will likely be with us well into 2021. This will be true whether or not a COVID-19 vaccine becomes available during that time. New challenges can also be expected, such as when governments pull back on the levels of fiscal stimulus that might have been nourishing green shoots of recovery.

Leaders can thus assume dynamic business conditions through 2021 as they begin this year's planning cycle. Wise planners will prepare for a number of outcomes, including a further drift in present conditions or a worsening downturn. In our view, however, they must also be open to the appearance of more positive trends and ready to shift quickly to a growth stance. This means building optionality balanced with tangible, trigger-based growth bets into their plans.

Leaders can do this by taking an owner's view of their business, comparing it to their peers' rather than their own past performance. Peer benchmarking can more readily become the starting point for developing a strategy to achieve full business potential. Companies need to know: What are tomorrow's resilients doing today to achieve "escape velocity" when the time comes?

Exhibit 1

Corporate stress is now at the same point as it was in the 2009 trough, arriving in only months versus two years.

Corporate stress by Altman Z-Score, %   ● Took on stress   ● Stayed roughly same   ● Reduced stress

	2009					Q1–Q2 2020			
	Experiencing stress	Gray zone	Good standing			Experiencing stress	Gray zone	Good standing	
Good standing	6	27	67	100%	Good standing	8	25	68	100%
Gray zone	38	55	7	100%	Gray zone	41	55	5	100%
Experiencing stress	92	7	●1	100%	Experiencing stress	94	6	●1	100%

2007 (left axis) — 2019 (right axis)

(n = 967)   (n = 1,300)

- In 2 quarters, 2020 recession has caused stress equal to that in 2008–09 recession
- Companies in good standing or gray zone in 2019 were experiencing stress by 2020

Note: Figures may not sum to 100%, because of rounding. For 2020 vs 2019 analysis, companies without reported financials for Q2 2020 were excluded. For 2020 vs 2019 and 2009 vs 2007 analyses, financial institutions, utilities, and some other companies, including those with Z-Scores of >10 or <–10, were excluded. Good standing: Z-Score >3.0; gray zone: Z-Score 1.8–3.0; experiencing stress: Z-Score <1.8.
Source: S&P Capital IQ; McKinsey analysis

Finding tomorrow's resilients

In this crisis, business leaders sometimes take solace in the relative ebullience of the stock market or the fact that peers are suffering from the same issues that they are. A quick look back tells us, however, that stock markets are poor predictors of success during a recession. The companies that led equity markets during the recessionary trough of 2009 did worse by the end of the cycle relative to the companies that made up the middle tier (Exhibit 2).

The Altman Z-Score turns out to be a better directional indicator of post-downturn market performance than does the market itself. The Z-Score helps highlight three outstanding attributes of resilience: margin improvement, revenue growth, and optionality (retained additional

optional investment opportunities).[5] Our research clearly suggests that coming out of the trough of the last recession, the top performers had achieved balanced improvements in all three of these measurements of organizational health—irrespective of whether they had spikes in any one of them. We have concluded that to be counted among the new resilients, companies must find this balance.

Accordingly, in the last recession, the companies whose Z-Scores fell the most between 2007 and the 2009 trough of the recession provided the lowest shareholder returns in 2011. The companies whose Z-Scores improved the most were the most likely to provide the best returns as the economy emerged from the recession (Exhibit 3).

Exhibit 2

The Altman Z-Score is a better leading indicator of company strength through a crisis than is stock-market performance.

Excess shareholder return, 2007–11, %

Companies grouped by market performance (TSR[1]) in the trough of the 2007–09 financial crisis (Q1 2009)
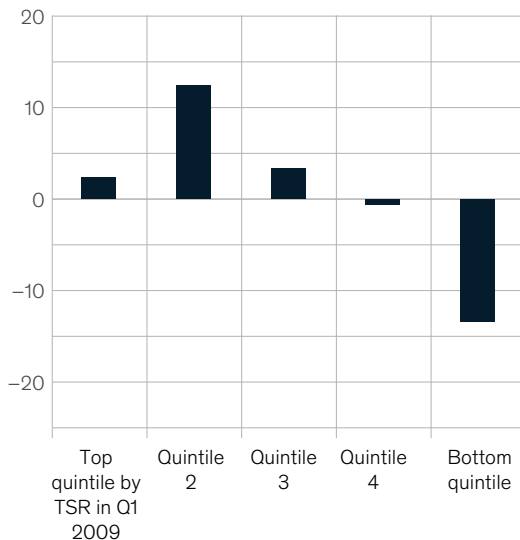
Companies grouped by Altman Z-Score movement, 2007–09
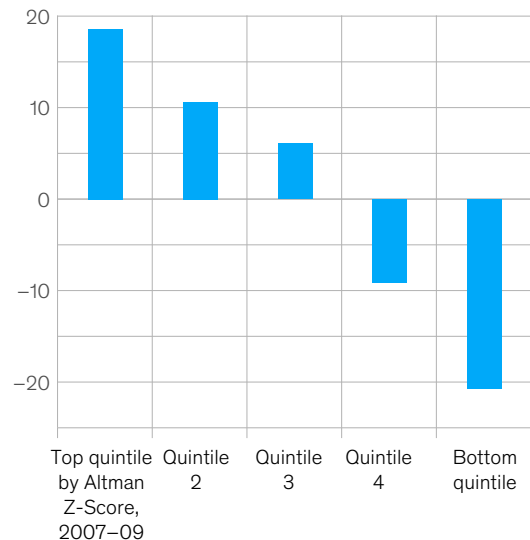
[1]Total shareholder return (TSR) for Q1 2009 was calculated as an average of medians for each industry sector of ~1,000 companies in total; excess shareholder return over the 2007–11 period was derived by subtracting the median of TSR for each industry sector with actual TSR for each company.
Source: S&P Capital IQ; McKinsey analysis

---

[5] Working capital and market equity value were part of Professor Altman's original score; for the purposes of our research we included the former determinant as part of optionality and recognized that the latter, market value, is externally driven and ultimately a product of the other factors.

Learning from the emerging resilients

In every sector, we identified the top 20 percent of companies that have driven the highest increases in their Z-Scores through the 2020 recession. We then compared their performance with that of the rest. This is what we found:

— *Margins.* The gap in margins between the emerging resilients and the rest of their peer group is striking. The typical emerging resilient in 2020 has increased the EBITDA[6] margin by 5 percent while the rest have lost −19 percent by this measure, a gap of nearly 25 percent. The difference is much greater than the EBITDA-margin gap was among the resilients in the last recession. This would suggest that today's margin leaders will dominate their sectors more firmly coming out of this recession.

— *Revenue.* The emerging resilients seem to be powering their margin advantage primarily through revenue rather than costs. The revenue gap between emerging resilients and the rest is around 16 percent in this cycle, whereas the gap was 10 percent in the last cycle.

— *Optionality.* The emerging resilients—and companies overall—seem to be leaving less optionality on the table today compared with what happened in the last cycle. Retained-earnings growth for emerging resilients is 11 percent today, whereas it was 30 percent at the time of the 2009 recessionary trough. For nonresilients, the optionality measurement is 1 percent in this cycle, while it was 6 percent in the last.

Exhibit 3

Resilient companies demonstrate balanced performance in margin, growth, and optionality.

Change in EBITDA[1] margin, growth, and optionality, resilients vs nonresilients,[2] in last and current recessions

■ Margin: EBITDA margin   ■ Growth: revenues   ■ Optionality: profits retained for reinvestment

2007–09, %

RESILIENTS: 6, 4, 29

NONRESILIENTS: −13, −5, 7

Q2 2020 vs Q2 2019, %[3]

EMERGING RESILIENTS: 5, −1, 11

EMERGING NONRESILIENTS: −16, −17, 1
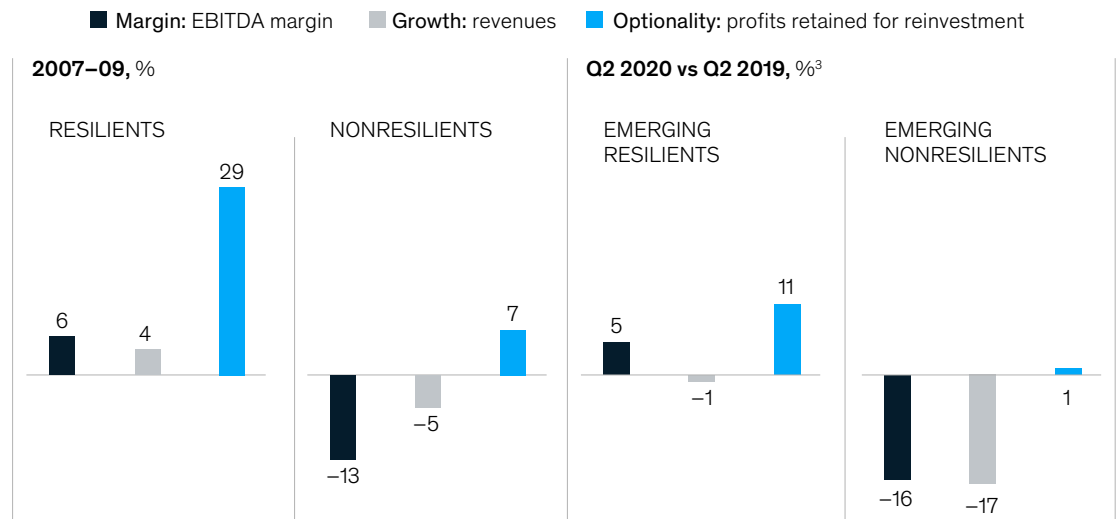
[1]Earnings before interest, taxes, depreciation, and amortization.
[2]Resilients in the last recession (2007–09) are defined as those companies in each sector in the top 20% in excess total return to shareholders (TSR); nonresilients are defined as the remaining 80%. Excess TSR is calculated by subtracting the median TSR for each sector from the actual TSR for the period of 2007–11.
[3]For the current recession, emerging resilients are defined as those companies in each sector in the top 20% on the Altman Z-Score (for Q2 2020 vs Q2 2019); emerging nonresilients are defined as the remaining 80%.
Source: S&P Capital IQ; McKinsey analysis

---

[6] Earnings before interest, taxes, depreciation, and amortization.

Exhibit 4 demonstrates the relative performance of the emerging resilients in 2020 and the resilients in 2009.

By sector, we discovered that the emerging resilients are more likely to demonstrate consistent, balanced performance across a number of metrics, as opposed to having a leadership spike in one and lagging performance in the others. This brings us to our final insight: tomorrow's resilients are more likely to be the companies that are driving value-added growth while balancing optionality, rather than those that focus most of their attention on maintaining operating margins, at the expense of other proportionate measures.

Zeroing in on what matters

Z-Score insights can help leaders take an ownership view and think more clearly about what their organizations can achieve—especially by freeing themselves of unnecessary traditional limitations. In this recession, we have already been afforded

meaningful glimpses of the possibilities. Faced with a global health crisis requiring physical distancing and other restrictions, companies shifted quickly to remote operating models.

In a matter of weeks, companies provided the workforce with new flexibility and skills where needed while maintaining or even increasing productivity. They massively expanded digital and online capacities to maintain customer relationships and deliver goods and services remotely and efficiently. They reconfigured supply chains to drive greater resilience. And they set higher standards for diversity and inclusion, providing a much needed leadership stance on making social change happen through better corporate citizenship. Imagine what companies might be able to do in 2021.

Let's start with the companies in the top quintile of their sectors according to the Z-Score. They are already creating the conditions that allow them to generate value-added growth while maintaining optionality. They are therefore best positioned to

Exhibit 4

Balanced performers across margin, growth, and optionality are more likely to emerge as resilients than are top performers in only one metric.

Composite ranking of company grading on margin, growth, and optionality

Share of total, %	Probability of being in emerging resilients, %	Margin	Growth	Optionality	Typical grade[1]	
9	59	A	A	A	Top performer	(A in at least 2 metrics)
11	**39**	**B**	**B**	**B**	**Balanced**	(B in all metrics; A in 1 metric and B in at least 1 metric)
24	**23**	**A**	**C**	**C**	**Mixed or spiky**	(A in 1 metric and C in at least 1 metric)
56	9	B	C	C	Underperformer	(B or below in all metrics, with C in at least 1 metric)

[1]A: top 20%; B: top 20–40%; C: bottom 60%.

realize their full potential. For these companies, first on the planning agenda is setting high aspirations for 2021. These can be defined by bold moves to drive rapid revenue growth, portfolio reallocation, value-creating M&A, and revamped technology spending.

Companies that are behind the top Z-Score performers in their sectors need to discover what is holding them back. They may be overemphasizing cost cutting or pursuing a strategy of growth at all costs. They might be overprioritizing investor payouts at the expense of their organizational health. They may be spreading their efforts thinly across many priorities instead of focusing tightly on driving margins and productivity. Leaders should also consider rethinking their supply chains end to end, especially to improve resilience.

Depending on their standing, lagging companies may need to focus their efforts on different drivers of growth. Almost universally, however, all companies will need to continue strengthening

their organization, so that they may provide more flexibility to the workforce while executing operations at full speed. The experience of most sectors demonstrates that companies which execute faster tend to outperform.

———————

Companies' experiments with creating new postpandemic operations models are yielding some interesting results. Digital platforms are allowing some companies to share skills across operations, providing support in ways that were very difficult before. The same approach is also allowing workers to enjoy more opportunities while creating an effective postpandemic operating model that solves for speed and rapid decision making. These are the next-horizon powers that will drive productivity and propel the emerging resilients into the next wave of growth.

Resilience in a crisis: An interview with Professor Edward I. Altman

One of the leading researchers in corporate financial health discusses what executives can do to help their companies endure the financial stresses of crisis times.

Professor Edward I. Altman of the Stern School of Business, New York University, is a leading expert in credit and debt. He has written or edited two dozen books and more than 160 articles on finance, accounting, and economics. He is also the creator of the Altman Z-Score, developed originally as a means of predicting bankruptcy probabilities. McKinsey researchers successfully used the Z-Score to test company resilience through a crisis.[1] We spoke with Professor Altman about how executives can best face financial stress in times of crisis.

McKinsey: The Z-Score has had a variety of practical applications. Do any stand out as particularly helpful? Have any applications of the model surprised you?

Professor Altman: I didn't know of McKinsey's use of the Z-Score to indicate resilience. Interestingly, you found it useful in gauging firm performance before and after a crisis. Banks have used the model in making lending decisions, and some use it to complement their own internal-ratings-based models for expected loss provisioning under the Basel rules. It is also used by investors in making bond or stock purchases. I was surprised, for example, that several investment banks have used the Z-Score as one of several criteria they apply to customers. Some investment banks offer a basket of common stocks with the highest Z-Scores and sell short the lowest. That came as a surprise—that the Z-Score was generating profit for investment banks selling a structured product.

I used the model in my testimony in December 2008 before the US House Finance Committee, at the onset of the financial crisis. The hearing would help determine whether General Motors and Chrysler would receive government bailouts. The Z-Score model showed very clearly that GM was heading for bankruptcy. I recommended against a bailout for GM and in favor of restructuring under Chapter 11.

That was the path, in my view, that gave GM its main chance of survival. They were really on the brink at that time, having hemorrhaged $2 billion per month for several months. I was not very popular at that hearing. Congress did not want to hear my "B word"—*bankruptcy;* they preferred the other one, *bailout.* The House voted for a bailout, but the Senate voted against it. President Bush eventually bailed out GM and Chrysler under the funding that Congress had given for financial institutions (using GMAC as the entry point).

But the bailout didn't work. Six months later, under the Obama administration, GM filed for bankruptcy and received about $50 billion in debtor-in-possession loans, exactly as I had predicted should happen. The rest is history. GM survived and is now an investment-grade company. That status may be a stretch, but it is certainly a solvent company with operations globally, and much healthier today *because* of going bankrupt, not despite it.

Finally, an application that really surprised me is the use of the Z-Score by managers to make strategic decisions. In 1981, I learned of a turnaround strategy used by the CEO of a large manufacturer of precision equipment in which he simulated business decisions like selling assets, reducing personnel, consolidating locations, paying back some debt. He plotted the effects of each simulated decision on the firm's Z-Score. No action was taken that would depress the Z-Score, at least in his estimation. And it was amazingly successful.

McKinsey: Professor Altman, you have studied the credit market for years. What fundamental changes have you observed? Today, we see many alternative financing instruments, and high-yield bonds have gained steam as well. Would you say that the Z-Score can account for such new developments? Has it proved timeless as a tool for measuring credit risk? Should we do anything

---

[1] McKinsey's results were published in an article by Cindy Levy, Mihir Mysore, Kevin Sneader, and Bob Sternfels, "The emerging resilients: Achieving 'escape velocity'," October 6, 2020, McKinsey.com. The authors used a common form of Professor Altman's Z-Score, with the following weighted determinants: $Z = 1.2X_1 + 1.4X_2 + 3.3X_3 + 0.6X_4 + 1.0X_5$, where X_1 = working capital/total assets, X_2 = retained earnings/total assets, X_3 = earnings before interest and taxes/total assets, X_4 = market value equity/book value of total liabilities, X_5 = sales/total assets, and Z = overall index. Edward I. Altman, "Predicting financial distress of companies: Revisiting the Z-Score and ZETA® models," Leonard N. Stern School of Business, July 2000, stern.nyu.edu.

differently today, compared with what you were doing 50 years back?

Professor Altman: Those are great questions. I would say most companies are riskier today than they were back in the 1960s when I built the model. Amazing progress has been made in technology, in strategy, over those 50-plus years, but the credit posture and structure of corporations have radically changed too. Back in the 1960s, and as late as the early 1990s, maybe 100 companies in the United States were rated AAA, and probably as many or more rated AA. Today, there are two AAA-rated companies in the US: Microsoft and Johnson & Johnson. And who knows how long those ratings will last?

An A rating is no longer the objective of companies. When I surveyed CFOs in the 1970s, as a visiting professor at Hautes Études Commerciales in Paris, the A rating was their predominant choice. Today, the preference is clearly for BBB. The reasons are low interest rates, certainly, but the lower rating also makes it easier to use leverage to raise earnings per share. Now there are other ways to raise earnings, as McKinsey and most CFOs well know. But a tried-and-true method is to increase leverage, especially where the cost of capital is low, and then invest in projects for which the return will be greater than the cost of debt and hopefully better than the cost of capital.

You mention high-yield bonds—we can add leveraged loans and shadow banking and so forth. The amount of leverage in the system now is far greater than it was 50 years ago. Is the Z-Score model still robust enough to be used today as it was then? The answer is yes. But I've learned some things over the years about the evolution of credit risk. I no longer use the cutoff scores from 1968. At that time, a company needed a Z-Score above 3.0 to be designated as a safe company. Companies with a score of less than 1.8 were considered distressed and likely to go bankrupt. Today, the cutoff score is much lower—*about zero.* A score of 1.8 is actually above average now for B-rated companies—and the dominant junk bond out there is a B-rated company.

There are more B ratings than any other for high-yield bonds—more Bs than double-Bs or triple-Cs. And the probability of a B-rated company's bond issue defaulting is about 28 percent in the first five years. So, 72 percent of Bs survive. And if you invest in a portfolio of Bs, assuming you receive interest compounded over five years, you will do quite well, relative to the risk-free rate—even given the default rate of 28 percent and the loss rate of about 20 percent (adjusted for recoveries).

I now use the bond-rating-equivalent technique to adapt to the changes over time in the capital structures of corporations. We look at the median score, by bond rating—AAA down to CCC—and assign a bond-rating equivalent to each firm, based on its score. And then we assess the probability of default given that bond-rating equivalent, using a mortality-rate approach, like an actuarial approach. That is the way I have adapted the original Z-Score model, and that model, with its original coefficients, is still quite effective.

You can go with the flow, in other words, making changes in rating equivalents over time, rather than building a new model each year or each five years. The Z-Score was originally based on a small sample of comparatively small companies. Today, companies are much larger, and the incidence of default for large companies is so much greater. Already in 2020 more than 50 companies in the United States with more than $1 billion in liabilities have gone bankrupt. Of course there were none of these "billion-dollar babies," as I call them, back in the '60s. So it is striking that a model built on smaller companies is still effective, generally, and for much larger companies as well.

McKinsey: Speaking of bankruptcies, we observe that companies continue to issue bonds—trillions of dollars worth in 2020. They are short of funds, as demand has dried up, and they are locking in the low interest rates as well. But the great volumes of debt are eroding companies' credit health. Do you expect filings for bankruptcy protection to rise in the months to come?

Professor Altman: I was worried about a potential debt bubble before the pandemic. I was in the minority then because the economy was doing well, bankruptcies were few, and defaults in the high-yield market were below the historical average. But I saw a lot of vulnerability. Not only for companies going bankrupt but also for the triple Bs, which were so popular, to be downgraded as fallen angels into the high-yield and junk categories. Well, things of course changed in March.

Because of extraordinary government support around the globe, companies with low Z-Scores are surviving. In some countries, it is even verboten, impossible to go bankrupt. The bankruptcy code is suspended in Germany and some other countries, except where fraud was involved. Italy and other countries have applied a moratorium on interest payments, a measure which reduces bankruptcies.

But the reduction in bankruptcies is temporary, in my view. We will have a second wave once government supports are reduced. I remain concerned about a debt bubble. Record amounts of new bonds and loans are being issued, both investment grade and noninvestment grade. Companies are doing this to raise cash as a reserve against problems stemming from the pandemic. Not all can do this—only those with reasonably good credit profiles. However, even companies that have been downgraded from investment grade to high yield are eligible for support from the Federal Reserve, for example, in purchasing in the secondary market of their bonds. This has given investors the confidence they need to buy the bonds even if they think that the issuing company is going to suffer during the pandemic. Because the price will be supported—as long as they don't default, of course. So the market is bifurcated: the haves are issuing debt and the have-nots are not.

There are zombie firms out there—companies artificially kept alive by banks and nonbanks. What can companies do to keep a debt bubble from building and to avoid potentially defaulting themselves with overwhelming amounts of new bonds and loans? I see two positive developments.

One is that companies are buying back their debt, reducing the amount of debt in their capital structure, using a lot of the cash that they raised over these past four or five months, since April of this year. Second is the issuance of new equity. I am surprised this has happened so quickly. But both IPOs and established companies (with secondary equity issuances) are beginning to do this. In my opinion, the sooner the better.

The easiest way to reduce your debt-equity ratio, as McKinsey well knows as strategists in the corporate-finance area, is an equity-for-debt swap. And the best time to do that is when the stock price is high. You raise new equity at a very attractive rate and then, instead of investing in a new plant and equipment, you buy back debt with it. Now the debt comes at low interest rates, so equity-for-debt swaps might be less attractive for some companies. But most have a target capital structure in mind, at least I believe so. And such a swap is one way to get back to it, if you are overweighted in debt.

For companies that cannot buy back debt because they don't have the cash, or those unable to issue new equity at attractive prices because their performance has been poor—these are the companies that I believe are going to default in increasing numbers in 2021, but probably not before then. Other forecasters agree with me on this, including investment banks and rating agencies.

McKinsey: As you know, some economists see things the way that you just laid out, while others are less concerned about the buildup of debt right now. Given the stressed economic environment, what advice do you think the Z-Score offers to executives today, as they approach the 2021 planning period?

Professor Altman: One of the interesting applications of the model is as an early-warning system. Executives of companies tend toward a biased view of their strengths and weaknesses, overestimating the former and underestimating the latter. If they see problems on the horizon, they think they can handle them. They may not realize the seriousness of a situation until late in the day. Once

the crisis hits, then they begin to react. If leaders are open-minded, however, they can use the Z-Score as an objective model. It will show where the company stands in terms of a bond-rating equivalent or a zone of distress. Applied early enough, this approach can help executives take action—selling assets, cutting back on debt, for example.

In this pandemic, some companies—high-tech companies and big banks in the United States, for example—have actually thrived. But many companies are in survival mode and preparing for that second wave. Banks are preparing with respect to capital provisioning, because they are regulated, and they know they should be doing so. Most companies are not regulated. I think a Z-Score or similar technique could help them see, unambiguously, how they are deteriorating during this pandemic. It might also show that they will recover when the economy recovers. Or maybe they will realize that they were deteriorating before the pandemic began, if they look at their Z-Scores for 2018, 2019, 2020. At any rate, they will see their vulnerabilities to financial distress. I would hope that companies use the Z-Score in that fashion. I know that investors are.

The McKinsey study shows that resilient companies can be identified as those whose Z-Scores decline less in a crisis. Scores for nonresilient companies are affected more negatively. You are not the only ones to have discovered this: as I mentioned, some investment banks have products that depend on the Z-Score for their investment (and divestment) choices.

McKinsey: Can you give us your view on the apparent disconnection between the stock market and the real economy? One much discussed factor is the overrepresentation of technology companies on the markets compared with their weight in the real economy.

Professor Altman: I am as surprised as anyone that the stock market is doing so well when the real economy is not. Noneconomic as well as economic and financial reasons play into this. Forecasts show overall GDP contractions for most economies in 2020. And yet, the stock market has rebounded

dramatically. The S&P, where technology companies have an outsize role, and the Dow as well, where they don't. And bond prices have also rebounded dramatically.

Puzzled as we may be, we economists and financial analysts need to have a view on why the markets have been buoyant. Of course, very low interest rates play a part. Where else will you put your money? In a safe? In government bonds? Not very attractive, unless you believe the market is headed for a real fall soon. The US Federal Reserve and other central banks have said that interest rates will remain low for quite a while. And so the outlook for the bond market is not very rosy. A second reason I think is that many people are spending more time following the market and investing. They are focused now on safeguarding their money or making profits—because they are at home, can't travel, are unemployed, or whatever. Day and retail traders have been an important force in this market. Many individual and institutional investors, furthermore, believe that the economy is going to rebound dramatically and feel that the time is right to buy cheap stocks.

Nevertheless, many investors have been losing in this stock market. Many funds are down, even though the stock market is up overall. The average investor is probably down in their own portfolio—except for those perhaps who picked some of the zooming companies like Zoom or Tesla or the tech giants. But will stock-market growth continue if economic recovery lags? I am being cautious in my own portfolio, taking into account the potential for another big downturn in the financial markets. This could be triggered by one or more factors—continued spread of the virus, delayed or ineffective vaccines, or a lagging recovery in the real economy. Investors could lose patience with companies.

McKinsey: I'd like to finish with a question about how business executives might best use the Z-Score. It's the product of several weighted variables, including earnings, margins, stock price, optionality. Should executives steer toward improvements in particular metrics or look to strike a balance among them?

Professor Altman: A balance. Companies need a multivariate approach, maintaining or improving performance on a number of metrics. Key drivers in the Z-Score are total assets and total liabilities. Companies concerned about their future could therefore seek to concentrate assets. Consolidate where you can while reducing investment in fixed assets if your situation is deteriorating. That would be part of a prudent strategy. It would raise cash needed, either for new investments (in products that are at an earlier point in their life cycles) or to pay back some debt. Companies are doing that also, to reduce vulnerability should conditions worsen. But it's hard. Reducing exposures to protect yourself in case things don't improve—that is not part of executive psychology. Executives think about how to improve earnings or market share. They don't want to think about reducing exposures by selling assets. Companies also need to better understand their liquidity positions. Inventories that are not selling well now should not be stockpiled in anticipation of better times in the future—unless, of course, companies have good reason to be very confident. So, working capital is

an important factor. And of course, stay away from borrowing, especially short-term borrowing, when in a vulnerable position.

McKinsey advises CEOs all the time, and likely well understands this issue. When a company encounters major problems, the executives whose decisions led to the situation have a hard time turning it around themselves. They can only be effective if they can take an objective view toward their own past, and act without bias. Very hard to do. At such times, companies need an adviser or an interim CFO or CEO to make the hard choices. CEOs could help themselves by recognizing that they can't do this alone. They need a clearly objective model. I have always said that there is help out there, but whether leaders can embrace help in times of crisis—that is the question.

McKinsey: That is golden advice. Thank you very much, Professor Altman.

Professor Altman: Thank you.

Edward I. Altman is the Max L. Heine Professor of Finance, emeritus, at the Stern School of Business, New York University, and director of research in credit and debt markets at the NYU Salomon Center for the Study of Financial Institutions. This interview was conducted by **Jeffrey Caso,** an expert in McKinsey's Washington, DC, office; **Peeyush Karnani,** a senior expert in the New York office; and **Mihir Mysore,** a partner in the Houston office.

Meeting the future: Dynamic risk management for uncertain times

The world is changing in fundamental ways, leading to dramatic shifts in the landscape of risks faced by businesses.

by Ritesh Jain, Fritz Nauck, Thomas Poppensieker, and Olivia White
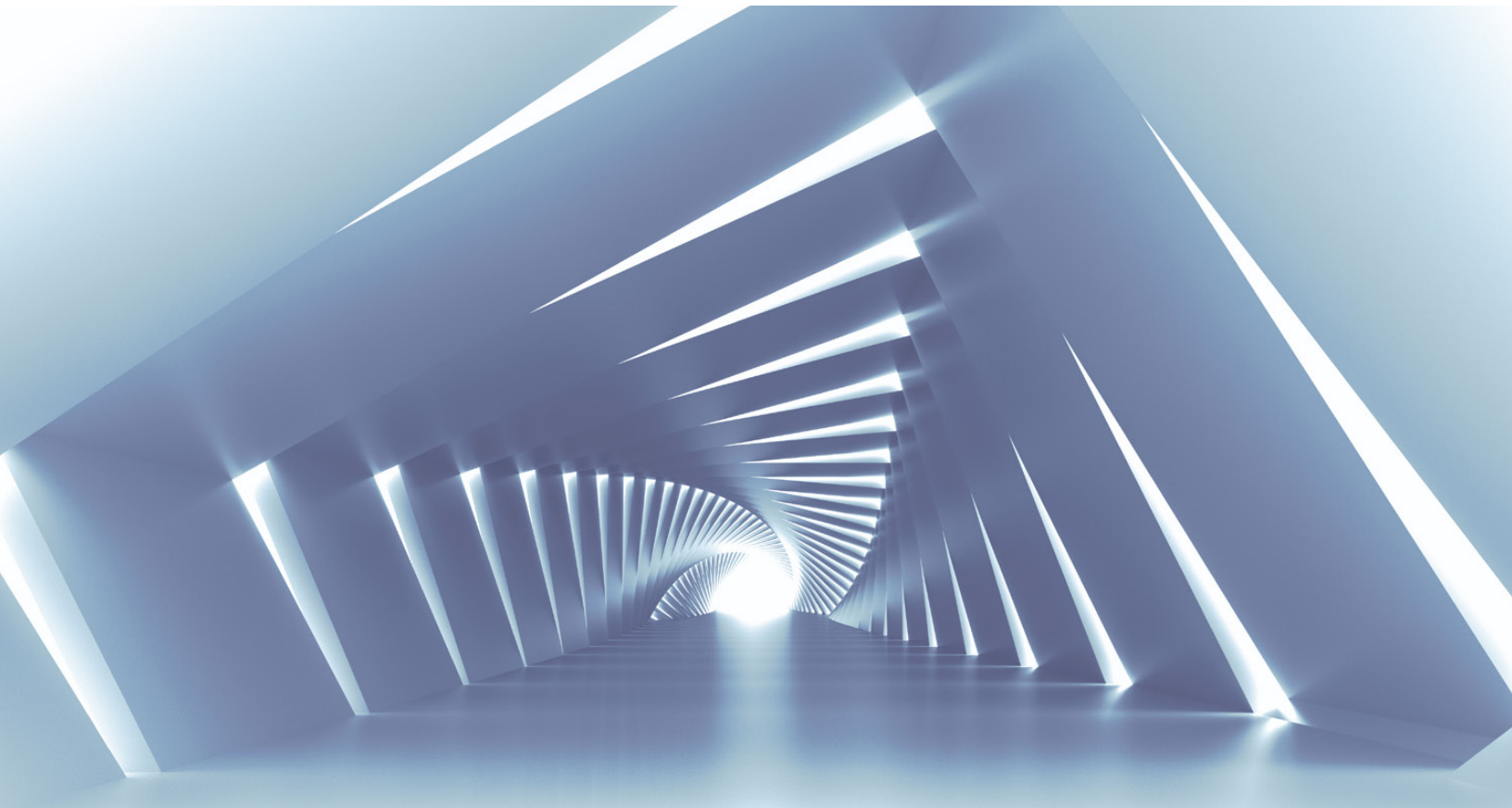
Beyond the profound health and economic uncertainty of our current moment, catastrophic events are expected to occur more frequently in the future. The digital revolution, climate change, stakeholder expectations, and geopolitical risk will play major roles.

The digital revolution has increased the availability of data, degree of connectivity, and speed at which decisions are made. Those changes offer transformational promise but also come with the potential for large-scale failure and security breaches, together with a rapid cascading of consequences. At the same time, fueled by digital connectivity and social media, reputational damage can spark and spread quickly.

The changing climate presents massive structural shifts to companies' risk-return profiles, which will accelerate in a nonlinear fashion. Companies need to navigate concerns for their immediate bottom lines along with pressures from governments, investors, and society at large. All that, and natural disasters, too, are growing more frequent and severe.

Stakeholder expectations for corporate behavior are higher than ever. Firms are expected to act lawfully but also with a sense of social responsibility. Consumers expect companies to take a stand on social issues, such as those fueling the #MeToo and Black Lives Matter movements. Employees are increasingly vocal about company policies and actions. Regulator and government attention is reflecting societal concerns in areas ranging from data privacy to climate change.

An uncertain geopolitical future provides the backdrop for such pressures. The world is more interconnected than ever before, from supply chains to travel to the flow of information. But those ties are under threat, and most companies have not designed robust roles within the global system that would allow them to keep functioning smoothly if connections were abruptly cut.

Companies require dynamic and flexible risk management to navigate an unpredictable future in which change comes quickly. The level of risk-management maturity varies across industries and across companies. In general, banks have the most mature approach, followed by companies in industries in which safety is paramount, including oil and gas, advanced manufacturing, and pharmaceuticals. However, we believe that nearly all organizations need to refresh and strengthen their approach to risk management to be better prepared for the next normal. The following discussion describes the core of dynamic risk management and outlines actions companies can take to build it.

The core of dynamic risk management

Dynamic risk management has three core component activities: detecting potential new risks and weaknesses in controls, determining the appetite for risk taking, and deciding on the appropriate risk-management approach (Exhibit 1).

Detecting risks and control weaknesses
Institutions need both to predict new threats and to detect changes in existing ones. Today, many companies maintain a static and formulaic view of risks, with limited linkages to business decision making. Some of these same companies were caught flat footed by the COVID-19 pandemic.

In the future, companies will require hyperdynamic identification and prioritization of risks to keep pace with the changing environment. They will need to anticipate, assess, and observe threats based on disparate internal and external data points. Dynamic risk management will require companies to answer the following three questions:

— *How will the risk play out over time?* Some risks are slow moving, while others can change and escalate rapidly. Independent of speed, risks can be either cyclical and mean reverting or structural and permanent. Historically, most firms have focused on managing cyclical, mean-reverting risks, like credit risk, that go up and down with macroeconomic cycles. Historically, the fundamental long-term economics of business lines have held firm, requiring only tweaks through the cycle. Credit risk in financial services is an example of such a risk. However,

Exhibit 1

Companies require dynamic and flexible risk management to navigate an unpredictable future in which change comes quickly.

3 core components of dynamic risk management

Detect risks and control weaknesses

Ability to anticipate, predict, and observe threats rapidly and accurately based on disparate internal and external data points and to assess risk magnitude, risk-impact duration, and internal-control effectiveness

Delimit risk appetite

Ability to set limits on risk taking dynamically, accounting for business's values, strategy, risk-management capabilities, and competitive environment

Decide on risk-management approach

Ability to decide promptly if risk requires immediate or more prolonged response, design and undertake appropriate response or mitigation, and institute feedback loop to track response effectiveness

the traditional principles of trajectory and cyclicality of risks are increasingly becoming less relevant. The global economic shock caused by the COVID-19 pandemic has demonstrated that many companies were not prepared for events with profound and long-lasting impact that could fundamentally change how business is conducted.

— *Are we prepared to respond to systemic risks?* In today's world, risk impact can go well beyond next quarter's financial statements to have longer-term reputational or regulatory consequence. Institutions must also consider whether the event triggering the risk has broad implications for their industry, the economy,

and society at large—and what that means to them. The COVID-19 pandemic has had a direct impact on most companies but has also meaningfully shifted the global economy and societal terrain. Companies should consider whether they have the controls, mitigants, and response plans in place to account for worst-case-scenario, systemic risks. For example, as companies house more personal data, the risks associated with data breaches become more systemic, with the potential to impact millions of customers globally. These firms need to consider proactively how to protect against and react to such breaches, including by working with external stakeholders, such as customers, law-enforcement agencies, and regulators.

— *What new risks lurk in the future?* Companies will need to cast nets wide enough to detect new and emerging risks before they happen. Traditional risk-identification approaches based on ex post facto reviews and assessments will not suffice. Most institutions have not had historical losses linked to climate change, and many have not encountered significant reputational blowback from being on the wrong side of a social issue. Institutions will need to work across business and functional divisions to maintain forward-looking, comprehensive taxonomies of the fundamental drivers of their risks. To get a real-time view of those drivers, companies should look to internal performance metrics, external indicators, and qualitative views of what business leaders see in their day-to-day work. Scenario-based approaches and premortems also play a critical role by letting leaders play out what might go wrong before it does.

Determining risk appetite

Companies need a systematic way to decide which risks to take and which to avoid. Today, many institutions think about their appetite for risk in purely static, financial terms. They can fall into the simultaneous traps of being both inflexible and imprudent. For example, companies that do not take sufficient risk in innovating can lose out to more nimble competitors. But at the same time, companies that focus on purely financial metrics can unwittingly take risks—for example, with their reputation by continuing a profitable business process that runs counter to societal expectation.

In the future, companies will need to set appetites for risk that align with values, strategies, capabilities, and the competitive environment at any given time. Effective enterprise risk management will help them dynamically delimit risk taking, directly translating financial and nonfinancial principles and metrics into a concrete view of what the firm will and will not do at any given time. Companies will need to be able to answer the following three questions:

— *How much risk should we take?* Rapid changes can quickly uproot companies' risk profiles. They will need to adjust their risk appetites to accommodate shifting customer behaviors,

digital capabilities, competitive landscapes, and global trends. For example, many companies that categorically refused to use the cloud five years ago are migrating to cloud-based storage and software solutions today, driven by improved technology and security. Geopolitical instability has the potential to increase counterparty and currency risk considerations for the travel and infrastructure industries when considering engineering, procurement, and construction contracts for megaprojects lasting several years. The COVID-19 pandemic has sparked pharmaceutical companies to consider afresh which risks they are willing to take to develop and produce treatments quickly.

— *Should we avoid any risks entirely?* Companies will want to draw some clear lines in the sand: no criminality; no sexual harassment of employees. But for many risks, the lines are not clear, and each company will need a nuanced perspective built on a strong, objective fact base. For example, will risk drivers such as climate change render risks in certain businesses fully untenable (for example, developing real estate in certain coastal regions)? Or should the reputational risk of being caught in the middle of highly charged environmental and social-responsibility issues drive a company out of certain business segments altogether (for example, in the way some retailers made the decision to stop selling guns)? Companies will need to develop views on such questions and update them continuously as their environments and corresponding fact bases evolves.

— *Does our risk appetite adequately reflect our control effectiveness?* Companies are more comfortable taking the risks for which they have strong controls. But the increased threat of new and severe nonfinancial risks challenges status quo assumptions about control effectiveness. For example, many businesses have relied on automation to speed up processes, lower costs, and reduce manual errors. At the same time, the risks of large-scale breaches and violations of data privacy have increased dramatically, heightening during the COVID-19 crisis as digitization accelerates substantially across many

industries. With less risk of manual errors but greater risk of large-scale failures, institutions will need to adjust their risk appetites and associated controls to reflect evolving risk profiles.

Deciding on a risk-management approach

Firms need to decide on how to respond as they detect new risks or control weaknesses. Today many rely on linear, committee-based governance processes to make decisions about risk taking, slowing their ability to act.

In the next normal, however, institutions will need to make risk decisions rapidly and flexibly, laying out and executing responses, whether immediate or prolonged, about how to avoid, control, or accept each risk. The decisions should actively engage leaders from across an organization to determine the mitigation and response efforts that have worked well in the past, as well as those that have not. In that way, the organization can develop the ways it manages risks in today's world. Companies will have to be able to answer the following questions:

— *How should we mitigate the risks we are taking?* Historically, many companies have relied heavily on manual controls and on human assessments of control effectiveness. That approach can generate excess, costly layers of controls in some areas while leaving gaps or insufficient controls in others. Today, the art of the possible in defending against adverse outcomes is rapidly evolving. Automated control systems are built into processes and detect anomalies in real time. Behavioral nudges influence people to act in the right ways. Controls guided by advanced analytics simultaneously guard against risks and minimize false-positive results.

— *How would we respond if a risk event or control breakdown occurs?* In the event of a major control breakdown, companies need to be able to switch quickly to crisis-response mode, guided by an established playbook of actions. Most companies have done little to prepare for crises, seemingly taking the attitude that "it won't happen here." However,

in the evolving world, firms will need to build crisis-preparedness capabilities systematically. As the COVID-19 crisis has demonstrated, companies with well-rehearsed approaches to managing through a crisis will be more resilient to shocks. Preparation should involve identifying the possible negative scenarios unique to an organization and the mitigating strategies to adopt before a crisis hits. That includes periodic simulations involving both senior management and the board. Companies should maintain and periodically update detailed crisis playbooks. Their strategies should include details on when and how to escalate issues, preselected crisis-leadership teams, resource plans, and road maps for communications and broader stakeholder stabilization.

— *How can we build true resilience?* Resilient companies not only withstand threats, but they emerge stronger. Companies can learn from every actual risk event and control breakdown, honing risk processes and controls through a dynamic feedback loop. On a grander scale, firms also have the chance to turn the fallout from true crises into competitive advantage, as the COVID-19 crisis is demonstrating. For example, some companies providing vacation rentals realized that they would need to do more than provide amenities and hygiene measures. They have started offering tailored customer experiences, including games, virtual cooking classes, and remote nature tours, built on an understanding of customer microsegments. These companies have started to differentiate themselves from their competitors and are positioned to emerge more resilient, even within a very hard-hit sector. Companies should prepare to ensure five types of resilience: financial, operational, organizational, reputational, and business-model resilience. Business-continuity, financial, and other plans can provide buffers against shock. But true resilience also stems from a diversity of skills and experience, innovation, creative problem solving, and the basic psychological safety that enables peak performance. Those characteristics are helpful in good times and indispensable when

quick, collaborative adaptation is needed for an institution to thrive.

Five actions to build dynamic risk management

Today, many firms see enterprise risk management as a dreary necessity but hardly a source of dynamism or competitive advantage. It can suffer from being static, siloed, and separate from the business. But dynamic and integrated risk management, which includes the ability to detect risks, determine appetite, and decide on action in real time, is growing ever more critical. Leaders can take five actions to establish the necessary capabilities (Exhibit 2).

1. Reset the aspiration for risk management

To meet the needs of the future, companies need to elevate risk management from mere prevention and mitigation to dynamic strategic enablement and value creation. This requires clear objectives, such as ensuring that efforts are focused on the risks that matter most, providing clarity about risk levels and risk appetite in a way that facilitates effective business decisions, and making sure that the organization is prepared to manage risks and adverse events.

In practice, risk managers should engage in a productive dialogue with business leaders to gain an in-depth understanding of how the business thinks about risk day to day and to share the risk capabilities they can bring. Businesses typically approach decisions with a reasonable risk-versus-return mindset but lack key information to do this effectively alone. For example, business units often do not have a full systematic understanding of the full range of risk drivers or a clear view of how a stressed environment could affect the company.

More broadly, businesses typically also lack an enterprise-wide view of how a risk might unfold. For example, climate risk may affect most aspects of some companies' businesses, from the impact of physical climate risk on operational facilities and supply chains to market repricing of carbon emissions to shifts in market demand and

competitive landscape. The COVID-19 pandemic has had a similarly cross-enterprise impact on nearly every company. It should be an objective of dynamic risk management to provide an enterprise view.

2. Establish agile risk-management practices

The increasingly volatile, uncertain, and dynamic risk environment will demand more agile risk management. Companies will need to tap into people with the right skills and knowledge in real time, convening cross-functional teams and authorizing them to make rapid decisions in running the business, innovating, and managing risk.

Building teams and decision bodies dynamically requires the ability to understand quickly the nature of the risk at hand, including its significance and how quickly it may play out. This helps determine who needs to be involved and how people should work together. One fintech company, for example, runs daily huddles to discuss customers, bringing together a cross-functional team of business and risk leaders and other subject-matter experts to review new customer complaints. This enables executives to review funnel metrics for the day side by side with customer complaints and helps teams triage and remediate those complaints promptly, avoiding larger issues down the road.

Decisions themselves should receive appropriate transparency, but managers should not get bogged down in excessive bureaucracy. Companies can formulate a clear, principled view of what sorts of decisions require committee review versus execution by single responsible parties. In some cases, previously unforeseen issues and risks that have the potential to evolve rapidly may require special, fast-track decision-making mechanisms. One organization does regular crisis-preparedness exercises and has developed relevant playbooks that assign decision-making power if needed, depending on the type of issue.

3. Harness the power of data and analytics

Companies can embrace the digital revolution to improve risk management. Automation technologies can digitize transaction workflows end to end,

reducing human error. Rich data streams from traditional sources, such as ratings agencies, and nontraditional sources, such as social media, provide an expanding and increasingly granular view of risk characteristics. Sophisticated algorithms enable better error detection, more accurate predictions, and microlevel segmentation.

One global pharmaceutical company adopted advanced analytics to help it prioritize clinical-trial sites for quality audits. The company used a model to identify higher-risk sites and the specific type of risk most likely to occur at each site. The company is now tightly integrating its analytics with its core risk-management processes, including risk-remediation and monitoring activities of its clinical operations and quality teams. The new approach identifies issues that would have gone undetected under its old manual process while also freeing 30 percent of its quality resources.

Another area in which advanced analytics can capture significant value is in the predictive detection of risk. One railway operator applied

advanced analytics to predict major component failures. The company improved safety and reduced its total failure cost for rolling stock by 20 percent. Companies can also use natural-language processing to build real-time, digital dashboards of internal and market intelligence, enabling more effective risk detection, including in customer complaints, employee allegations, internal communications, and suspicious-activity reports.

4. Develop risk talent for the future
To meet the demands of the future, risk managers will need to develop new capabilities and expanded domain knowledge. Strong knowledge of how the business operates provides a critical foundation by supporting true understanding of the landscape of risk. This enables risk professionals to provide better oversight and more effective challenge while also acting as effective counselors and partners as their company navigates the risk landscape.

Risk managers will also need strong understanding of data, analytics, and technology, which are driving shifts in how most companies operate—a trend only

Exhibit 2

Dynamic and integrated risk management, which includes the ability to detect risks, determine appetite, and decide on action, is growing ever more critical.

5 actions to establish capabilities needed for dynamic risk management

Reset aspiration for risk management	Establish agile risk-management practices	Harness power of data and analytics	Develop risk talent for future	Fortify risk culture
Move risk from prevention and mitigation to dynamic strategic enablement and value creation	Authorize cross-functional teams to make rapid decisions in business, innovation, and risk management	Digitize transaction workflows; use data to expand view of risk characteristics; deploy algorithms to enable better error detection, more accurate predictions, and microsegmentation	Develop new capabilities and expanded domain knowledge to support full understanding of risk landscape	Build true risk-culture ownership in front line; hold executives accountable for cultural failings; link risk culture with daily business activities and outcomes

accelerated by the COVID-19 crisis. This is true for how data and digital interfaces are affecting firm processes, how companies are employing artificial intelligence to support day-to-day decisions, and how the digital revolution is shaping risk management itself.

To put this all together, risk managers will need to develop agile capabilities and mindsets, allowing them to identify opportunities to convene stakeholders and contributors across functions rapidly and generate quick solutions. People will need the leadership and personal capabilities to tap into colleagues with the right skills and knowledge in real time.

5. Fortify risk culture

Risk culture refers to the mindsets and behavioral norms that determine how an organization identifies and manages risk. In moments of high uncertainty—such as those we are living through during the COVID-19 pandemic—risk culture is of exceptional importance. Companies cannot rely on reflexive muscles for predicting and controlling for risks. A good risk culture allows an organization to move with speed without breaking things. It is an organization's best cross-cutting defense.

Beyond today's travails, a strong risk culture is a critical element to institutional resilience in the face of any challenge. In our experience, those organizations that have developed a mature risk culture outperform peers through economic cycles and in the face of challenging external shocks. At the same time, companies with strong risk cultures are less likely to suffer from self-inflicted wounds in the form of operational mistakes or reputational

difficulties and have more engaged and satisfied customers and employees.

Companies with strong risk cultures share several essential characteristics. Most important, true ownership and responsibility for risk culture sits with the front line, with executive-level accountability for cultural failings. To be truly lived, culture must be linked with the day-to-day business activities and outcomes of an institution. At the same time, someone needs to be responsible for coordinating the definition, measurement, reporting, and reinforcement of risk culture—for example, within a risk function, a COO organization, or HR. Without an enterprise-wide view and vocabulary, it is not possible to effect true, coordinated cultural change. Finally, attention to risk culture must be ongoing. Strong culture takes maintenance and requires reinforcement.

One fast-growing technology company announced a culture transformation as the CEO's top priority. It selected 30 culture leaders from across the company to lead the effort. The initiative mobilized around one-fifth of its staff through workshops aimed at helping managers make risk-informed decisions and creating a new risk culture and mindset.

———

The world is facing both uncertainty and rapid change. For companies, risk levels are rising—as are the expectations of employees, customers, shareholders, governments, and society at large. Against this backdrop, we believe companies need to rethink their approach to risk management, to make it a dynamic source of competitive advantage.

Ritesh Jain is an associate partner in McKinsey's New York office, **Fritz Nauck** is a senior partner in the Charlotte office, **Thomas Poppensieker** is a senior partner in the Munich office, and **Olivia White** is a partner in the San Francisco office.

A fast-track risk-management transformation to counter the COVID-19 crisis

An accelerated transformation to enhance efficiency and effectiveness will enable risk organizations to deal with the pandemic while addressing rising regulatory and cost pressures.

by Javier Martinez Arroyo, Marc Chiapolino, Matthew Freiman, Irakli Gabruashvili, and Luca Pancaldi

Before the coming of the pandemic, banks had been reducing the complications and costs that arose over the years as they dealt with escalating regulations and emerging risks by adding policies, processes, and people to their risk and compliance functions.

Then COVID-19 happened and threatened to complicate things all over again.

When banks shut branches and corporate offices, this altered how customers interact with them, forcing changes to long-held risk-management practices. Activities that typically happened in person were no longer possible, such as credit-committee meetings to approve underwriting for a new corporate client, or office visits by potential small borrowers to verify their creditworthiness or sign loan documents.

The banks' risk-management functions, which act as a second line of defense between frontline employees who work directly with customers and the department's backstop internal risk-audit teams, also had to adjust the way they operate. For starters, they had to manage employees who would now work from home and to prepare for the pandemic-triggered problems of small-businesses and other customers. They also had to adopt new practices to monitor existing risks and guard against new ones, including cyberrisks triggered by the pandemic. Such changes, we estimate, could raise the operating expenses of risk functions by 10 to 30 percent. That's reason enough to make processes as efficient and effective as possible.

McKinsey had previously found that risk managers can improve their operations by digitizing and applying advanced analytics to a variety of department functions and by optimizing the organization, among other changes. Those directives still hold. Our latest research shows that to address the business problems COVID-19 has created and to mitigate the cost and regulatory pressures risk organizations still face, they must roll out digital and advanced analytics more aggressively and tie these moves to tactical improvements in governance.

More specifically, to win in the next normal, the risk-management function must make itself more efficient and effective—something high-performing risk organizations have already done. We have prioritized six specific moves risk organizations must make:

— Redesign underwriting to streamline processes and add automated ones.

— Enhance monitoring.

— Optimize and automate reporting.

— Improve processes for reporting financial crimes.

— Streamline the market-risk operating model.

— Make other changes by taking a big-picture look at risk management's overall organization, governance, and performance management.

These changes are often part of a larger transformation that can take years to implement. Yet some risk-management functions have adopted the practices we've outlined much more quickly—in some cases, in only three months. When these changes are successful, we estimate that they can improve efficiency and effectiveness enough to raise the productivity of specific activities by 40 percent or more. Banking-sector risk organizations that had been relatively efficient before implementing these moves can use them to raise their productivity by 15 to 25 percent. Less efficient bank risk organizations can raise it by 30 percent or more.

Roadblocks to improving risk management

Well before the pandemic, risk organizations had to deal with the external pressures of increased industry regulation, and internal pressure to cut costs. Around the world, both the depth and breadth of banking regulations have increased. The reasons include the shift to digital channels and tools, a greater reliance on third parties and the cloud, and the threats that all these pose to the strength and integrity of risk functions. On top of that, bank leaders working to make their organizations more

competitive expect the risk function to contribute to overall cost-cutting efforts.

COVID-19 has added to those challenges. Risk managers must understand the pandemic's impact on credit and market portfolios to mitigate the effects on their own operations. They've had to track emerging threats to the newly remote workforce, to current and potential borrowers, and to other bank customers. They've implemented government-directed moratoriums on loan collections and abided by other local or national measures adopted in the pandemic's wake. Those actions have cut into top-line revenues at a time when banks are adding expensive new risk-management practices.

But coping with the new requirements doesn't have to mean adding staff. Risk-management activities—including resources in first-, second-, and third-line

defense roles—already account for up to half of a bank's employees and costs. Risk-organization staff in the second line of defense account for approximately 2 to 3 percent of the total number of bank employees, not including compliance and financial-crimes personnel. Although our research shows that scale is the single most important driver of efficiency, we have also found that the size and cost of multiple risk activities do not correlate directly with scale (Exhibit 1). For these activities, the different operating models of banks explain the variations.

Lower costs don't necessarily make a bank's risk operations less effective. In fact, a McKinsey analysis found that banks with the strongest risk operations have 10 to 15 percent fewer full-time-equivalent employees than their less effective counterparts do (Exhibit 2).[1]

---

[1] As measured by 2019 Supervisory Review and Evaluation Process (SREP) ratings and corrected for the impact of scale.

Exhibit 1

Some risk-management activities appear to be more fixed and suitable for economies of scale.

Total cost of risk management by activity and size of bank
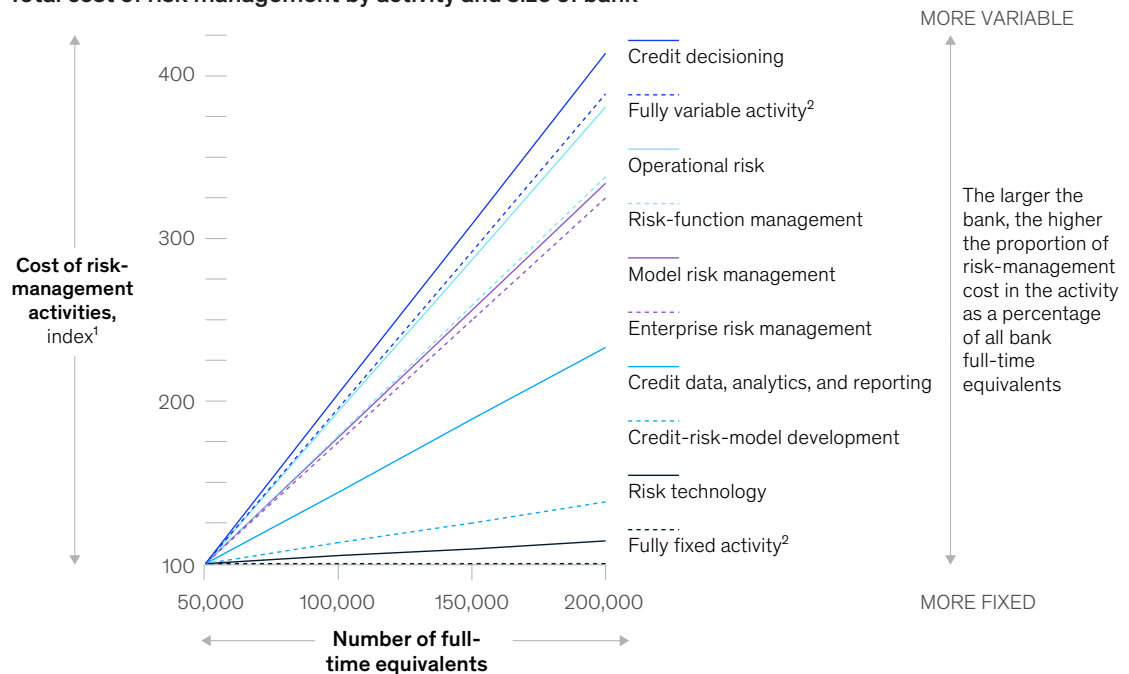
[1] To ensure comparability across functions, total cost of risk organization was rebased to 100 for each function for a bank with 50,000 full-time equivalents to capture marginal increase over institutions' size. Noise deriving from initial size of each function was removed to observe correlation between overall institution size and function size.
[2] Same proportion of risk-management cost for banks of all sizes.
Source: McKinsey Global Risk Benchmark, 2019

Six actions that improve risk-management productivity

Risk functions can face their old and new challenges, without increasing their size or costs, if they operate more efficiently and effectively. Banks have a number of options. They can deploy some of the moves outlined below relatively quickly to make themselves more efficient and effective while also adapting their risk-management practices to the COVID-19 environment (Exhibit 3).

1. Redesign underwriting

Assessing a borrower's creditworthiness is a long, labor-intensive process that's prone to inefficiencies, which make it ripe for improvement. The desire of borrowers for more transparency into the underwriting process has exacerbated the existing complexities. Customers—in particular,

Exhibit 2

Banks with more effective risk operations are also more efficient.

Correlation of risk-operation size and SREP[1] evaluations for Tier 1–3 banks, %[2]

Tier 1: 2.8
Tier 2: 3.0
Tier 3: 3.5

20%
10–15% when adjusted for scale impact[3]

Tier 1   Tier 2   Tier 3

[1]SREP: Supervisory Review and Evaluation Process.
[2]Risk-operation size: risk-operation full-time equivalents (FTEs) vs total-bank FTEs; risk-operation FTEs exclude compliance, anti–money laundering, and risk-IT functions. Pillar 2 requirements for European Banking Authority (EBA) and Pillar 2A requirements for UK; SREP evaluation used as proxy for risk-function effectiveness, as internal risk-governance framework is 1 of 4 pillars of SREP process. Tier 1: <1.75% for EBA and <2% for Bank of England Prudential Regulation Authority (PRA); Tier 2: 1.75–2% for EBA and 2–2.5% for PRA; Tier 3: >2% for EBA and ≥2.5% for PRA. Sample size of 10 EU and UK banks.
[3]Adjusted for size using correlation inferred from McKinsey Global Risk Benchmark, 2019.
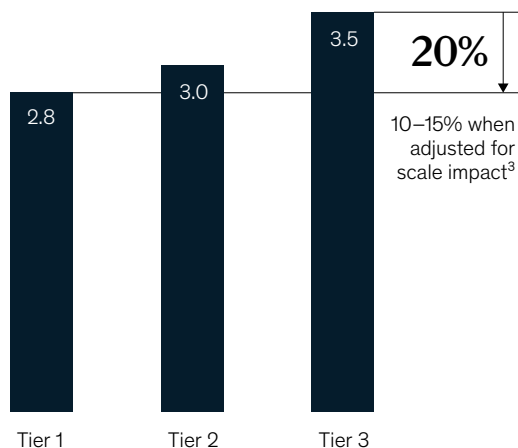Source: Bank of England; individual Pillar 3 reports; "Supervisory review (SREP)," European Central Bank, 2019, bankingsupervision.europa.eu

retail companies and small and medium-size enterprises (SMEs)—want to know immediately if they qualify for a loan and when they can access the funds. That didn't change when COVID-19 hit: risk functions must still meet customers' expectations even while dealing with them remotely.

Credit underwriting already accounts for a substantial part of the total resources of the risk organization—an average of 30 percent (and up to 50 percent) of its employees. Adding staff therefore isn't the answer. In fact, our research indicates that the workforce at the most efficient organizations tends to be substantially smaller than it is at the least efficient ones.

In the next normal, the ability to speed up underwriting turnaround times will become an important differentiator. Risk teams that had already digitized underwriting before the pandemic responded more successfully under the lockdown. By 2021, we expect others to follow suit, pushing up the adoption of digital channels for credit underwriting by 5 to 15 percent.

Banks have three primary avenues to improve the efficiency and effectiveness of their credit-underwriting processes:

— *Adopt straight-through processing (STP) for credit-underwriting workflows.* Upgrading to digital from manually inputting data, through data spreading or other means, could help reduce end-to-end workflow costs by up to 40 percent. STP applications include tools that prepopulate credit forms with data from clients or internal or external databases as well as incorporate delegation and structure information.

— *Automate underwriting for retail and SME customers.* Using software to calculate the creditworthiness of a small business by standard criteria, rather than having staff make these decisions, could raise margins by 5 to 10 percent. Software could also improve (by 10 to 25 percent) an underwriting department's ability to correctly predict whether an SME is a good credit risk. Banks that have already automated the function might consider increasing underwriting thresholds— for example, to $500,000, from $250,000.

Exhibit 3

Risk-management functions can take action in six areas to realize productivity gains of 30 percent or more in a matter of months.

Productivity opportunity, % difference between top and median performers

Redesign underwriting[1]	Enhance monitoring[2]	Optimize and automate reporting[3]	Optimize financial-crime detection	Streamline market-risk operating model	Improve organization, governance, and performance[4]
~50	~15	~25	~30	~20	~30
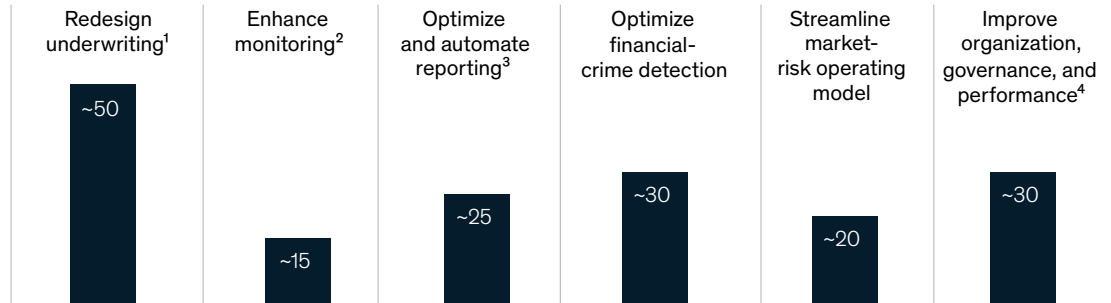
Potential productivity improvements

Redesign underwriting[1]	Enhance monitoring[2]	Optimize and automate reporting[3]	Optimize financial-crime detection	Streamline market-risk operating model	Improve organization, governance, and performance[4]
• ~10–25% improvement in accuracy of underwriting predictions through advanced analytics • ~5–10% credit-margin growth through instant credit decisions	• ~40% portfolio-level decisions supported by advanced analytics • ~15–20% reduction in manual data entry through natural-language processing	• ~50% reduction in data-reporting errors, reducing need for manual corrections and improving monitoring quality	• ~40% increase in know-your-customer (KYC) process accuracy • ~50% decrease in KYC documents and process steps • ~80% improvement in accuracy of anti–money laundering alerts	• ~50% reduction in data errors and exceptions • ~20% reduction in data and pricing discrepancies between front line and risk	• ~30% reduction in complexity • Increased awareness of risk effectiveness and efficiency through monitoring

[1]Includes credit decisions.
[2]Includes credit-risk portfolio management and enterprise-risk-management (ERM) risk review and tracking.
[3]Includes credit, market, operational, and ERM reporting.
[4]Includes management and overhead for all risk types.

To mitigate the increased potential for fraud that typically accompanies changes in this area, automated banks must also improve their controls.

— *Simplify corporate-credit underwriting.* Banks can streamline underwriting that cannot be automated, because of the counterparty's size or the complexity involved, by reducing the credit-application documentation and analysis required. For large, well-established, or public companies, risk managers could review a dozen documents instead of 50 and reserve the more intensive scrutiny for less prominent or smaller enterprises. Other methods to rework corporate underwriting processes include defining credit limits by company type or industry (rather than on a deal-by-deal basis) and creating a special-case system to handle the most complex or urgent requests.

2. Enhance monitoring

The widespread economic fallout from COVID-19 has forced risk managers to rethink how and

what they monitor to evaluate risks, including creditworthiness and the ability to repay loans. The virus's spread and reactions to it continue to shift, often quickly. These developments have helped some industries and hurt others—boosting the revenues of grocery chains, for example, while cutting into restaurant sales. They have also affected segments within industries differently, so risk managers have to monitor trends at a more granular level. On top of that, risk managers need to account for the actions that governments are taking to help constituencies respond to the virus. Many of these actions, including moratoriums on payments for mortgages and business loans, affect the environment for credit.

Before the pandemic, risk-monitoring activities accounted for about 15 percent of risk-management costs. Banks traditionally executed a not insubstantial portion of these activities manually, so they are ripe for change. Risk departments can adopt a range of digital systems and tools to automate risk-monitoring tasks:

— *Digitize counterparty-level credit-monitoring tools.* Risk functions can program advanced analytics into early-warning systems to improve reviews of earnings releases, real-time financial news, transaction data to find information that could affect a client's credit outlook. We estimate that algorithms could support 40 percent of counterparty-level credit-monitoring decisions. Banks that have already implemented these techniques reduced their credit losses by 20 to 30 percent, through early detection of potential deterioration of counterparty creditworthiness—while reducing monitoring costs by 30 to 40 percent (Exhibit 4).

— *Digitize portfolio-level credit-monitoring tools.* Historically, risk-monitoring personnel manually reviewed industry news to extract data that could be used to make decisions about the changing credit landscape of different economic sectors. Risk departments that adopt applications using artificial intelligence (AI) and machine learning to track industry news and developments could reduce related data entry by up to 15 percent.

Some of these AI-based monitoring tools can trigger real-time alerts based on sector-level indicators, such as point-of-sales systems. To estimate the impact of new information on sector-wide rating scores, these tools may also use machine-learning models (such as hyperparameter random-forest modeling) tailored to specific industries or clients. In addition to analytics engines, digital-monitoring suites typically include smart-workflow capabilities that focus analytic work on areas where human judgement is necessary, such as parameter changes in the models that are not associated with a high level of confidence.

— *Monitor portfolios in a more granular way.* Risk functions typically use back testing and internal ratings–based models to evaluate the soundness of their credit portfolios. Because the pandemic has had such a profound impact on the global economy, which continues to shift unpredictably, the typical indicators of creditworthiness have been affected. Risk functions that in the past may have analyzed 20 to 30 economic sectors may need to review ten times that number of industry subsectors to understand how they are faring in the crisis. Some institutions have gone as far as to subdivide the restaurant industry, for example, into 15 subsegments, the better to distinguish between top and bottom performers and predict nonperforming loans. Instead of analyzing the beverage industry, therefore, banks may need to review what's happening in soft drinks, bottled water, soft alcohol, and hard alcohol, to name a few subsegments.

3. Optimize and automate reporting

Banking regulators have increased their reporting requirements—for example, by asking for more and better data on risk practices and more closely scrutinizing these data. We estimate that as a result, the risk functions of banks devote 10 to 15 percent of their total resources to comply with such reporting requirements. Automation gives risk managers additional insights into the risk profiles they must review to meet these requirements—but without adding personnel to a low-value task. As circumstances and requirements change, automation can also help managers adjust what reports cover.

Several moves could make risk functions more efficient and effective in this area:

— *Actively monitor reporting requirements.* By constantly tracking what regulators want and managers need, risk functions can manage the risks their banks face and provide what's required, without wasting resources sharing unnecessary information. Some banks that have started to merge regulatory and internal reports have cut the number of reports they produce in half.

— *Offer self-service reports.* Risk managers can use self-service reporting tools to update or review reporting information directly, including both high-level data and the underlying information it's based on. We estimate that self-service reporting, by itself, could cut the costs of risk departments by up to 30 percent.

— *Improve data architecture and management.* It's not unusual for banks' risk data to reside in several databases or other applications—the result of mergers, expansion into new markets, divisions that use different systems, or operations that span several countries or continents. For such institutions, complying with

Exhibit 4

To reduce credit-risk losses and boost monitoring, banks can categorize financial flows to leverage transaction data.

Small and medium-size enterprise (SME) transactions by category, % of total transactions

Inflows		Outflows	
Goods and services payments	76	Goods and services payments	50
		Internal self-transfers	14
		Payments by check	7
Internal self-transfers	14	Other categorized	12
Payments by check	6	Uncategorized	4
Other categorized	3	Employees	6
Uncategorized	2	Government services	8

100
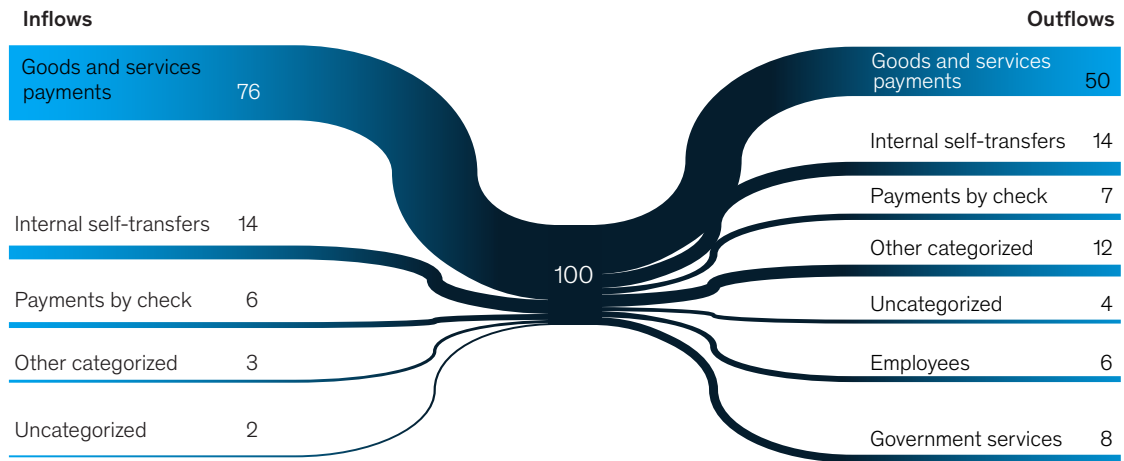
Credit loss, index (100 = 100%)

Traditional monitoring[1]

Transactional monitoring[2]

−20% to −30%
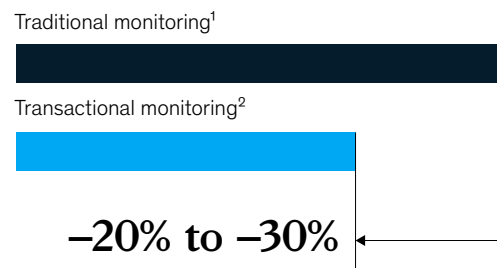
Cost of full-time equivalents for SME-credit monitoring, index (100 = 100%)

Traditional monitoring[1]

Transactional monitoring[2]

−30% to −40%
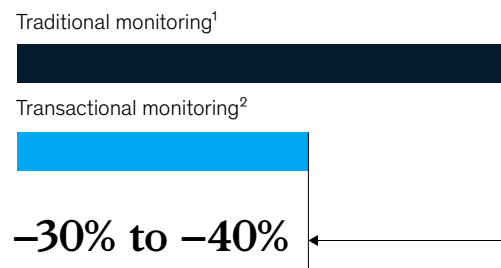
Note: Figures may not sum to 100%, because of rounding.
[1]Traditional, bureau-based monitoring, using manual analysis.
[2]Enhanced monitoring and upgraded team setup, using transactional data.

reporting requirements may involve manually culling data from these manifold sources.

— A data architecture that can pull information from disparate databases into a central location can not only alleviate the need for manual processes but also provide other benefits. As part of such an upgrade, risk functions could create reporting-competence centers for frontline and risk-management personnel in multiple business units or subsidiaries. We estimate that automating and unifying data architecture and management could cut risk-reporting costs by 10 to 20 percent and halve the number of reports that include errors. Depending on how a bank is structured, these efficiency changes could take place within either the operations or IT organization.

4. Optimize processes for detecting financial crimes

Since global regulators began to intensify financial-crime-compliance activities a decade ago, they've launched scores of enforcement actions and levied $36 billion in fines around the world. An average of 2 to 3 percent of a bank's total staff therefore works in second-line financial-crime monitoring and reporting efforts. For a global bank with 100,000 employees, this means that 2,000 to 3,000 people could be tracking anti–money laundering (AML) and another compliance processes.

When COVID-19 measures forced banks to send their risk-management staffs home to work, it disrupted the face-to-face activities these employees rely on to know their customers—still one of the strongest ways to assess the risk of financial crime. But regulators are not giving institutions a pass because of the pandemic, so risk organizations face the added burden of finding ways to assess, monitor, and report on financial-crime compliance under remote working conditions.

We see three ways to make these practices more efficient and effective:

— *Automate customer onboarding.* Risk organizations could automate the collection and verification of the documents that prospective customers must present to open a credit or

savings account. Risk functions that do so, we estimate, could reduce their financial-crime-compliance spending by 10 to 20 percent and improve the accuracy of customer data by 40 percent. In addition to costing less, algorithms that read and extract data from verification documents eliminate the possibility that employees could be paid to falsify information. This would also free up time that first-line bank staff and internal audit teams could use for other work.

— *Optimize AML alerts.* All banks use AML alerts to flag unusual transactions that could signal irregularities. But false positives are common—in some cases, accounting for more than nine alerts out of ten. The use of advanced analytics to monitor transactions, often in parallel with existing rules-based tools and models, can improve the accuracy of alerts and thereby reduce the number of false positives to six or fewer out of ten (Exhibit 5). More accurate alerts can reduce the need for manual interventions and free up risk-management personnel for other tasks.

— *Streamline know-your-customer (KYC) processes to meet local requirements.* The customer documentation that risk functions must provide to satisfy financial-crime-compliance requirements vary from region to region. Many risk functions apply the same standards throughout the organization, creating unnecessary work and expense. By adjusting monitoring and reporting to local requirements, risk functions can meet their obligations and reduce costs. That kind of streamlining could reduce the number of required KYC documents by 50 percent and speed up the onboarding of new customers.

5. Streamline the market-risk operating model

Some banks use dated or very complex operating models, data systems, and architectures to buy and sell fixed-income equities or engage in other large-market investment activities for clients. A front-to-back review of this data architecture and systems, as well as of the associated roles, responsibilities, and processes, can result in significantly lower costs and sizable improvements in risk management. We see three important actions that market-risk managers can take in such a review:

— *Use the same valuation models throughout the organization.* Different functions not uncommonly use separate means or models to estimate the worth of the same asset, and that makes it hard or impossible to come up with a consensus value. Front-office staff may use one equity-derivatives valuation model to calculate profit and loss (P&L) estimates and projections, while the risk department uses a different model to determine regulatory P&L and key risk indicators. If the front office and risk organizations use the same market, counterparty-credit-risk (CCR), and liquidity models and systems, they can reduce data inconsistencies by 80 to 90 percent and valuation-related reworks by 20 to 30 percent. Risk management's model-risk-management (MRM) function could challenge and validate these models and develop different ones only when supervisors require them or if the models truly diverge from front-office practices.

— *Integrate the system architecture of the front office and the risk function.* In addition to adopting the same valuation models, risk functions can use front-office data architecture to calculate P&L and risk. When data sources are centralized through integrating data architecture, run-the-bank and change-the-bank technology costs and external spending decline. Some banks that integrated these functions have become up to 20 percent more efficient, though the extent of the improvement depends largely on a particular institution's operations and starting point.

— *Integrate front-office and risk reporting.* Integrated reporting creates a single source of truth that can minimize data reconciliations, and improve the risk function's efficiency and effectiveness. Institutions can adopt different organizational models: the integrated reporting function can sit in risk, finance, the front office, or operations. Banks that integrate reporting have reduced related costs by 40 percent or more. But to get there, risk functions need strong management to push for collaboration

and overcome the challenges that such an integration effort might encounter.

6. Improve organization, governance, and performance

Over the past half-dozen years, risk and compliance functions added resources, controls, and policies to contend with increased regulation and other demands. Meanwhile, their budgets increased twice as much as those of other bank functions.

When a function expands so quickly, the big picture of how it is performing can be obscured by daily demands. Policies or committees are created piecemeal, sometimes duplicating work done elsewhere. On top of all these problems, the pandemic forced risk functions to set up new ways of working, including the addition of new (and often ad hoc) committees and policies to assess and monitor

Exhibit 5

Advanced analytics can help reduce false-positive results in anti–money laundering alerts.

Share of false-positive results by type of anti–money laundering alert, %
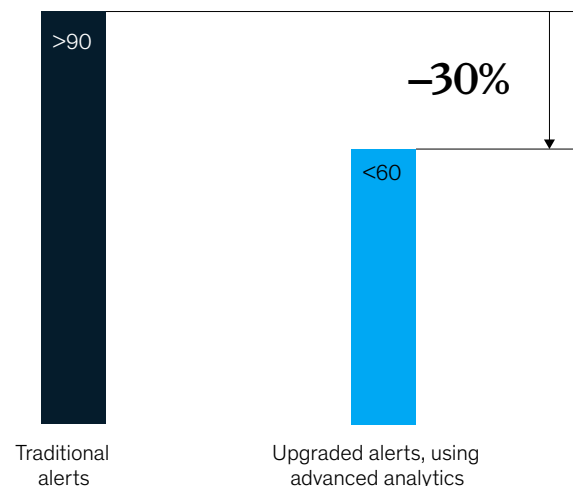
>90

<60

−30%

Traditional
alerts

Upgraded alerts, using
advanced analytics

Many banks do have multiyear transformation projects in the works. Yet risk managers can take a number of steps that yield high-impact results in far less time.

risks. The new structures sometimes overlap with ongoing work or obscure its importance.

To ensure that risk functions are structured in the most effective way, they can examine four key organizational elements:

— *Clarify roles and responsibilities for all three lines of defense.* Regulatory scrutiny of risk practices led many institutions to add controls (and the jobs associated with them) haphazardly, with limited clarity about who does what. Some banks switched oversight for technology and cyberrisk from the risk function to a technology group and then back to the risk function—moves that not only sowed confusion about roles and responsibilities but also created potential gaps in coverage and duplicate responsibilities. Banks can improve efficiency by mapping out the duties of the front line, the risk organization, and internal audit departments to identify gaps, fix overlaps, and ensure accountability. A clearer organizational chart could result in cost savings of up to 5 percent.

— *Centralize shared resources and add agile practices.* Risk managers can move these haphazardly added activities and staff into centers of excellence—both virtually and physically—which handle common activities such as risk data and analytics, reporting,

testing, and monitoring. We estimate that if risk functions adopt both centers of excellence and agile methodologies, they can increase the efficiency of the centralized activities by 10 to 20 percent and save up to 20 percent of their outsourcing costs. A number of the 20 largest North American banks have already created centers of excellence that report directly to a chief risk officer. Many of these groups focus on data, analytics, and reporting.

— *Rationalize risk governance and policies.* To focus on what matters most, banks should consider streamlining their downstream procedures and policies. Reducing the number of committees, for example, can not only improve focus, accountability, and lines of escalation but also save executives' time. It's not uncommon for midsize and large banks to have thousands of risk and compliance policies spawning dozens of procedures, which in turn influence processes and the design of controls. If banks structure their policies to focus on the areas of highest risk, they can remove needless red tape. We have seen institutions eliminate up to 30 percent of their policies while improving the quality of the rest, reducing costs and efforts associated with policy administration and management. Institutions undertaking such a transformation may find that they could adjust or rewrite nearly all of their policies to

make them more clear, reflect their current risk appetite, or achieve the appropriate level of detail. The renovation of risk policies can start with the establishment of design principles to understand the challenges and identify the end goals that policies are meant to achieve.

— *Put a performance-management system in place.* Historically, risk organizations have monitored key risk indicators—for example, the percentage of nonperforming loans or performance against controls—but not their own key performance indicators (KPIs). They may not, for example, track how many credit files a risk-function employee processes a day, how many models each validator manages, and the way those figures trend over time. By failing to measure their own performance, risk operations

neglect opportunities to fine-tune the way they work and thus to make themselves more efficient and effective. We recommend that risk organizations track their KPIs for credit risk, market risk, operational risk, and the like, as well as the related outcomes (Exhibit 6).

How to update risk-management practices in the short term

Transforming risk management across the six areas we've described could take at least a year if a bank adopted any traditional approach. Many banks do have multiyear transformation projects in the works. Yet risk managers can take a number of steps that yield high-impact results in far less time. In this way, banks can make the entire risk organization upward of 30 percent more productive—including

Exhibit 6

Banks can use key performance indicators to help ensure that risk management meets targets.

Sample risk categories and metrics to measure performance

Credit underwriting and adjudication	Detecting financial crimes	Monitoring and tracking	Data	Reporting	Model development and validation
Touch time for loans • Auto • Credit cards • Personal lending • Mortgage or home-equity line of credit • Commercial underwriting, up to $5 million • Commercial underwriting, up to $5 million adjudication • Wholesale **Straight-through processing** • Auto • Credit cards • Personal lending • Mortgage (assisted lending) • Commercial, up to $2 million	• Ratio of STR/SAR[1] filings to alerts • Ratio of alerts to STRs • Average time to clear alert • Ratio of nonalerts to investigation personnel • Know-your-customer personnel as percentage of total anti–money laundering personnel	• Qualitative/quantitative breakdown of KRIs[2] • Percentage of automated KRIs (gathered through system checks) • Percentage of controls tested within centralized utility • Number of required risk assessments • Percentage of fully automated controls	• Percentage of time spent on low-value activities (eg, sourcing, processing, quality assurance) • Number of teams performing data-related activities	• Number of risk reports • Average cost per report • Average cost per report category • Report frequency • Average report length	• Number of models by tier/category (eg, internal ratings, stress test, internal capital needs) • Number of models managed by modeler • Number of models managed by model validator • Percentage of models reviewed per year • Number of model-risk corrective actions issued in past year

[1]Suspicious-transaction report/suspicious-activity report.
[2]Key risk indicators.

cost efficiencies of 40 percent or more in selected activities—in as little as three months.

Analyze and prioritize activities that must change

To determine which aspects of operations would gain from the kinds of changes we propose, look at the risk organization's cost base and workforce to uncover functions or processes that increase costs unnecessarily and to benchmark your operations against those of comparable institutions. Conduct workshops, observe people at work, and interview risk-function managers and staff to understand how work gets done and which practices could improve.

These insights can serve as the basis for a list of actions and their expected short-term impact or productivity gains. Risk managers can use such a list to decide which actions to take first based on the overall health or goals of the risk organization or the bank. From there, they can create a full implementation plan.

Launch and execute priority actions

Once an implementation plan is in place, risk managers have to create an infrastructure that defines how the work will be done and who will do it. In addition, they must determine if they have the right tools for the work, the staff has the necessary skills, and change-management and skill-building programs are required. Finally, they need to establish regular check-ins and delivery milestones; provide support, coaching, and other kinds of help for the teams running the program; and map out how to measure outcomes, such as tracking the cost reductions resulting from the changes.

———

Risk-management functions increase the odds of creating lasting change if the moves they make are part of a well-conceived, well-executed plan, are supported by top leaders, and are part of a broader shift in behavior across the organization. Organizations that have successfully navigated this path know that while it may not be easy, the rewards of more effective—yet less expensive—risk management are well worth the challenge.

Javier Martinez Arroyo is a partner in McKinsey's Paris office, where **Marc Chiapolino** is a partner; **Matthew Freiman** is a partner in the Toronto office, **Irakli Gabruashvili** is a consultant in the New York office, and **Luca Pancaldi** is a partner in the Milan office.

Risk culture

Strengthening institutional risk and integrity culture

Many of the costliest risk and integrity failures have cultural weaknesses at their core. Here is how leading institutions are strengthening their culture and sustaining the change.

by Richard Higgins, Grace Liou, Susanne Maurenbrecher, Thomas Poppensieker, and Olivia White

The COVID-19 pandemic has created a time of unprecedented change for both public and private organizations across the globe. Executives and boards have had to move quickly to address threats and seize opportunities, all while continuing to protect employee and customer health and safety and evolving to adopt new digital and work-from-home norms.[1]

Risk and integrity culture refers to the mindsets and behavioral norms that determine how an organization identifies and manages risk. In this challenging and highly uncertain moment, risk culture is more important than ever. Companies cannot rely on reflexive muscles for predicting and controlling risks. A good risk culture allows an organization to move with speed without breaking things. It is an organization's best cross-cutting defense.

Beyond today's travails, a strong risk culture is a critical element to institutional resilience in the face of any challenge. In our experience, those organizations that have developed a mature risk and integrity culture outperform peers through economic cycles and in the face of challenging external shocks. At the same time, companies with strong risk cultures are less likely to suffer from self-inflicted wounds, in the form of operational mistakes or reputational difficulties, and have more engaged and satisfied customers and employees.

This article explores the steps involved in setting up an effective risk-culture program, when to launch such a program, and the factors we have found to be critical for long-term success.

Understanding and measuring risk culture

The starting point for most organizations looking to improve their risk culture is to diagnose the current state. Organizations that have built strong risk and integrity cultures seek to understand (and then address) three mutually reinforcing drivers: risk mindsets, risk practices, and contributing behavior.

Risk mindsets can be understood as the set of

assumptions about risk that individuals hold within the organization; risk practices are the daily actions that determine the effectiveness of risk management; contributing behavior comprises the collective actions that build risk attitudes. Ideally, these actions will be systematic and deliberately intended to strengthen individuals' risk attitudes, with desired risk behavior built into everyday functioning.

Concrete definition
Companies that seek to understand risk culture can best begin by establishing concrete, detailed definitions. They should clearly spell out the specific elements of risk culture to set aspirations and measure progress. For example, we define ten dimensions of risk culture, based on a wide range of experiences with companies across all major industries, and incorporating close study of a range of real-world risk-culture failings (Exhibit 1).

Systematic measurement
Once risk and integrity culture is defined, measurement can begin. Leading companies assess themselves systematically, looking at mindsets, practices, and behavior.

This assessment is often based on interviews among units and functions, then followed by a more comprehensive organization-wide survey.

The survey will typically include 20 to 30 questions that measure performance against the elements of risk culture (covering mindsets, practices, and behavior) and will set the organization-wide baseline. The team can complement results with qualitative insights gleaned from follow-up interviews to provide further detail on the particular strengths or weaknesses revealed, and help uncover their root causes.

Instead of using a dedicated risk and integrity survey, many organizations falter by relying on a combination of employee-engagement surveys, focus groups, and analyses of incidents and near-misses to measure their risk culture. Each of these tools can bring useful results when used with sufficient rigor. However, typical employee-

---

[1] Aaron De Smet, Elizabeth Mygatt, Iyad Sheikh, and Brooke Weddle, "The need for speed in the post-COVID-19 era—and how to achieve it," September 9, 2020, McKinsey.com.

Exhibit 1

Risk culture can be understood as having ten dimensions, covered under four topics.

Acknowledgement			Responsiveness	
Confidence	**Openness**	**Challenge**	**Speed of response**	**Level of care**
An assured understanding of an organization's exposure to risk without any false sense of security	The degree to which management and employees exchange bad news or learnings from mistakes	Scrutiny of the quality, appropriateness, and accuracy of others' attitudes, ideas, and actions	Perception of external changes and reaction speed to innovation or change	Responsibility to care about the outcome of actions and decisions

Transparency			Respect	
Communication	**Tolerance**	**Level of insight**	**Adherence to rules**	**Cooperation**
The degree to which warning signs of both internal and external risks are shared	Understanding of risk appetite and its linkage to overall strategy and decision making	Identification and understanding of risks present in the business	Alignment of individuals' risk appetites to the organization's	Consideration of broader organizational consequences and impact on overall risk appetite when any one team acts or makes decisions

engagement surveys contain only a few relevant questions and therefore do not usually uncover enough insight to create an effective measure. These approaches, furthermore, do not provide a view over time or ready comparisons between organizational units.

We believe that a dedicated survey is an indispensable tool for obtaining a broad measure of a company's risk culture. It is the only way to set a true initial baseline. A comprehensive survey creates hard data, comparable across divisions, geographies, and roles; with repeated use, it traces trends through time. The results allow fact-based conversations about risk culture, fostering engagement while deepening executive-level understanding.

Sharing results

Once an initial baseline is developed, the results should be shared with leadership teams and the broader organization. Transparent results are an important first step in increasing the focus on

risk culture. While maturity levels across different dimensions matter, outliers (both strengths and weaknesses) or areas of change where a survey is repeated over time tend to drive the greatest insights for an organization. Differences among units, functions, geographies, and tenure levels can also be illuminating.

In one example of this process, a government-owned corporation held a series of town-hall meetings to share the results of its risk-culture survey. The town halls were the first active communications on risk culture and demonstrated to employees a new openness. The comparative data shared showed divergent strengths and weaknesses, which stimulated strong interdepartmental conversations in what was a traditionally siloed organization.

As a second example, a high-performing financial institution created tailored readout packs for a series of thoughtful discussions between the chief risk officer and the leader of each major line of business

and function. The readout materials highlighted areas of opportunity for each business and function, including dimensions where their risk culture was weaker than the organization as a whole or where results were at odds with stated strengths or goals of the leader. For instance, with one leader who had taken pride in his organization's openness to sharing bad news, the conversation centered around weak scores in this area in some geographies.

Addressing risk-culture shortcomings

With the help of measured risk-culture results, companies can act to address weaknesses in risk culture. The leadership team, with support from the team coordinating risk-culture efforts, can use the strengths, weakness, and cultural differences identified to agree on a set of prioritized interventions or intervention areas based on enterprise-wide and divisional aspirations.

Some interventions will affect the entire organization—for example, certain compensation or recruiting changes. These warrant group-led approaches, and a dedicated team should be created or assigned to take charge of them.

Many, however, will be specific to and driven by particular parts of the organization. For instance, affected business units would take charge of work to redesign problematic product-approval processes; likewise, business-unit leaders might "localize" a groupwide focus on a topic like accountability. Where possible, interventions or their application should be driven, and owned, by the front line to ensure that cultural change is truly lived locally and linked to day-to-day business activities and outcomes. Successes and lessons from these localized efforts can be shared across the organization by a central coordinating team.

The process of developing interventions end to end is well illustrated by the experience of one insurance company. The company explored the results of an initial risk-culture survey at a top-team offsite. The survey data allowed leaders to move from discussions based on intuition to those based on evidence. The leaders discovered that the organization was universally strong in some dimensions and universally weak in others. Clear

differences also emerged among business units. The CEO probed the comparative differences, challenged executives to understand the causes of low scores, and explored ways for everyone to learn and apply lessons from higher-performing business units. Coming out of the discussions, the team agreed on focus areas and assigned responsibility for carrying out the improvements.

Designing and deploying tailored interventions

To lift risk culture, organizations move from measuring and planning to taking action. A broad range of techniques can be summoned to inspire change. Successful efforts are usually the result of several kinds of actions taken together. In thinking about how to generate meaningful, lasting changes in risk and integrity culture, leaders can be guided by the "influence model" schematized in Exhibit 2. This model has proven useful in ensuring that change programs draw upon a breadth of approaches, and its use increases the chance of success for a transformation by three or four times.

The effort to address risk-culture gaps usually involves a balance of short- and long-term interventions. Targeted short-term interventions allow organizations to respond flexibly to changing needs while longer-term programs constantly reinforce core elements of desired risk culture. Long-term interventions are often formal programs like speak-up hotlines or training and compensation standards (based on risk criteria) that continually reinforce desired behaviors.

In an effective example of a long-term intervention, one bank developed a program that both encouraged employees to speak up on risk issues and increased the level of responsive actions. The program includes an externally managed channel for employees to register concerns, with the option of confidential help from internal speak-up champions on navigating the process. The board receives regular reports on both internal and external complaints, with resolution rates and common themes and trends.

The following short-term initiatives are just a few examples of how organizations have addressed gaps in risk culture:

— A government agency developed a short-term program to increase its speed of response, which was identified as a major weakness. This was done with walk-throughs of key processes, which identified bottlenecks; components were then redesigned as needed to speed up the process and ensure future clarity on escalation and resolution.

— A bank discovered weaknesses in its approval process for new products. Its investigation led to the creation of a dedicated challenger role, filled by rotating members of the approval committee.
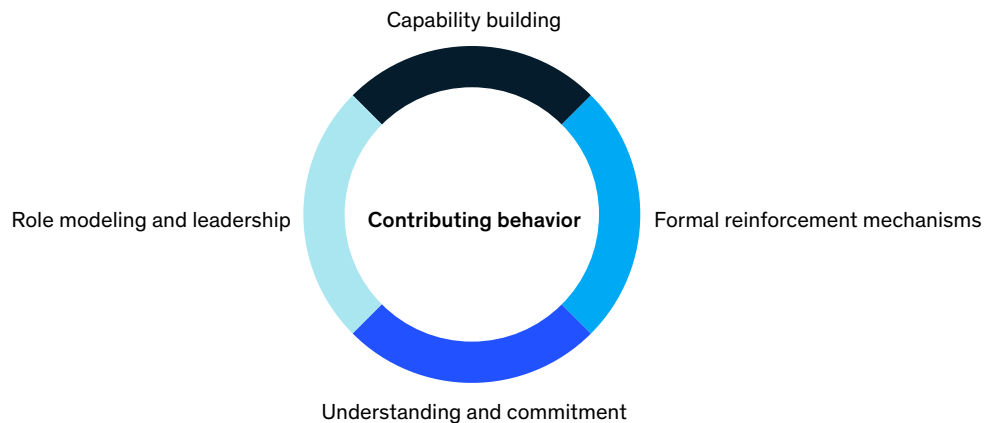
The role is charged with taking deliberately contrarian positions and pressure-testing proposed products on how well they served the long-term interests of the customer and the bank.

— A pharmaceutical company sought to address a weak culture of challenge by training new and junior colleagues on how to constructively question leadership decisions. To encourage the best results, senior leaders acted as role models, visibly promoting nonhierarchical decision making.

Exhibit 2

The 'influence model' defines four dimensions of risk-culture-change programs, ensuring that a breadth of approaches are used.

Influence model for risk-culture change

"I have the skills to behave in the new way"	"Systems reinforce desired change"	"I know what I need to change, and I want to do it"	"I see my leaders behaving differently"
● Employees are coached to consider client needs plus other business concerns ● Employees receive training on available communication channels, both formal and informal, to identify and escalate risks ● Top management is coached on communication methods for discussing risks	● The organization appoints senior leaders with the right expertise to understand and manage risks ● Systems and processes are in place to quickly identify potential policy or guideline breaches ● The organization compensates and promotes people to encourage them to act in the organization's best long-term interests	● When things go wrong at a competitor's, the company considers how to change its approach ● Internal communications prominently feature success stories of change across different employee tenures ● Workshops with a cross section of staff are used to brainstorm improvement opportunities around risk	● Leaders share risk knowledge that supports decisions and actions ● Leaders demonstrate appreciation when employees raise mistakes, rather than avoiding the issue or penalizing the employee ● Leaders expect and encourage people to challenge their views and decisions ● Leaders systematically and effectively communicate key risks faced by the business as well as mitigation approaches

Launching a risk-culture program

Risk-culture programs can have multiple triggers. Leading companies take proactive steps to maintain strong risk cultures in normal times, in times of stress (such as under the COVID-19 crisis), and when they are undergoing transformations.

Proactively shaping risk culture

Building and sustaining strong risk culture requires proactive attention. In normal times, this means addressing risk culture before issues arise. Under the stress of the COVID-19 pandemic, which has disrupted the traditional mechanisms that reinforce an organization's risk culture, this includes understanding how risk culture is evolving and then taking action to protect or improve it. Because of the pandemic, people are working together differently, often from home. In addition, many individuals and organizations are under added stress (including financial stress), increasing the risk of nearsighted decision making and cultural problems.

Once a crisis with roots in risk culture hits, existing leadership, including boards, will find it difficult to lead change as they themselves become increasingly associated with the cultural problems. The problems tend to be seen as leadership failings in the eyes of the public, investors, and regulators.

By taking a preemptive look, leaders might see early signs of concern or inadequate processes for understanding the state of risk culture. An initial deep dive into the root causes of seemingly isolated incidents or complaints can be a starting point, eventually expanded into a broader risk-culture review to build a comprehensive picture. Today, the preemptive look should also seek to understand the impact the COVID-19 crisis is having on employees and develop interventions to strengthen the culture by filling the gaps created by remote working.

The effort might be triggered by the need to understand whether an organization is vulnerable to incidents experienced by peers, either before or during the pandemic. By proactively driving this topic, leaders can avoid larger problems and demonstrate that they are part of the solution and not the problem. For example, a company in the advanced industries sector built a speak-up program after leadership recognized the devastating impact of other failures in the industry. The leaders methodically created formal mechanisms to support desired behavior, helping to ward off potential crises before the point of no return was reached.

Maintaining risk culture under company transformation

Many organizations are transforming their operations, particularly to become more digital and more efficient. The COVID-19 crisis has served to accelerate many planned change programs. Large transformations can themselves raise risk levels, as risk-management practices are disrupted, core processes are redesigned, and teams and organizational structures shift. "Change fatigue," a species of anxiety that comes with a transformation, can contribute its own share of risk. But transformations also afford organizations the opportunity to reset their model to their desired risk-management culture. They must include programs to promote desired behaviors, in transparent, organization-wide efforts, as opposed to siloed, business-as-usual approaches.

For example, one global manufacturing company undertook a major transformation in response to a series of product- and regulatory-compliance incidents. Front and center were issues of culture, integrity, and compliance, which became the core focus of the groupwide transformation.

In a second example, a bank undertook a major transformation and restructuring effort, partly in response to COVID-19-triggered considerations. The program included a dedicated cultural component with a specific risk-culture stream. As the transformation progressed, business units incorporated risk-culture initiatives into their broader program of activities, ensuring risk-culture changes became core elements of the new ways of working.

Getting started

Whatever the original motivation for a risk-culture program, a one- or two-year plan covering a range of intervention types can begin with a small set of priority initiatives targeting key weaknesses. In addition to achieving progress in important areas, these initiatives will create visibility and momentum for the entire plan. An example campaign would be

one that encourages employees to speak up where they see risk concerns. The initiative might include a confidential speak-up line, communications from the top to set the tone on the importance of speaking up, and, for a dedicated period, an explicit focus on speaking up in team meetings. Results would be conveyed to the board in a report covering internal and external complaints, whistleblower activity, overarching themes, and resolutions. This would serve as a first step and a gesture of commitment to the larger effort of changing risk culture.

Setting yourself up for risk-culture success

Careful risk-culture definition, measurement, and initiative work plans are not enough. Successful risk-culture programs share five essential characteristics that leaders should put in place as part of their focus on risk culture:

1. *True ownership and responsibility for risk culture sits with the front line.* To be truly lived, culture must be linked with the day-to-day business activities and outcomes of an institution. First-line leaders must feel accountability for their role in supporting the company's risk culture.

2. *Dedicated ownership is assigned for coordinating the definition, measurement, reporting, and reinforcement of risk culture.* These responsibilities should sit centrally—either within enterprise risk management, with a risk chief operating officer or an enterprise chief operating officer, or within HR. It is helpful to have a central point, as too often varying language is used to discuss culture within a bank. Without an enterprise-wide view and vocabulary, it is not possible to effect true, coordinated cultural change.

3. *The case for change is visible and compelling.* The strengths and weaknesses of the prevailing risk and integrity culture need to be spelled out, supported by data. The vision for an enhanced culture and how it will benefit the organization and individuals can then be articulated.

4. *The effort is sustained over time.* Cultural change takes time, and gains must be regularly reinforced. Successful programs combine periodic measurement of organizational risk culture with a multiyear change program encompassing short- and long-term initiatives. Too often organizations bring a burst of energy to the initial diagnostic but then fail to implement initiatives or sustain the changes needed to drive long-term improvement.

5. *The C-suite holds leaders accountable for success.* Risk-culture programs need someone to provide overarching direction and drive, but to succeed, leadership across the organization should be actively engaged. Business-unit owners in particular should champion initiatives. Leaders need to show they are serious about change if they want their people to adopt new risk behaviors, which may themselves be perceived as risky—for example, speaking up.

As senior leaders navigate the complexity of the current crisis, they must ensure the organization as a whole maintains its cultural health. Organizations that nurture their risk and integrity culture will be better positioned to serve their clients, team members, and society effectively, and to avert risks that could potentially prove catastrophic. By taking the steps outlined above, institutions can prepare, reap near-term rewards, and be ready for future uncertainties and challenges.

When nothing is normal: Managing in extreme uncertainty

In this uniquely severe global crisis, leaders need new operating models to respond quickly to the rapidly shifting environment and sustain their organizations through the trials ahead.

by Patrick Finn, Mihir Mysore, and Ophelia Usher

© Maksim Tkachenko/Getty Images

In normal times organizations face numerous uncertainties of varying consequence. Managers deal with challenges by relying on established structures and processes. These are designed to reduce uncertainty and support calculated bets to manage the residual risks. In a serious crisis, however, uncertainty can reach extreme levels, and the normal way of working becomes overstrained. At such times traditional management operating models rarely prove adequate, and organizations with inadequate processes can quickly find themselves facing existential threats.

Uncertainty can be measured in magnitude and duration. By both measures, the extreme uncertainty accompanying the public-health and economic damage created by the COVID-19 pandemic is unprecedented in modern memory. It should not be surprising, therefore, that organizations need a new management model to sustain operations under such conditions. The magnitude of the uncertainty organizations face in this crisis—defined partly by the frequency and extent of changes in information about it—means that this operating model must enable continuous learning and flexible responses as situations evolve. The duration of the crisis, furthermore, has already exceeded the early predictions of many analysts; business planners are now expecting to operate in crisis mode for an extended period. Leaders should therefore begin assembling the foundational elements of this operating model so that they can steer their organizations under conditions of extreme uncertainty.

Understanding extreme uncertainty

Due to the severity of this crisis, many organizations are in a struggle for their existence. An existential crisis puts at stake the organization's survival in recognizable form. Readers can probably call to mind numerous individual companies that faced such crises in the recent past. The crises may have been touched off by a single catastrophic incident or by a series of failures; the sources are familiar— cyber breaches, financial malfeasance, improper business practices, safety failures, and natural or

human-caused disasters. Effective action saved many; others spiraled downward.

Existential crises subject organizations to both extreme uncertainty and severe material consequences; they are often new and unfamiliar and can unfold quickly. In business terms, the present crisis more closely resembles economic crises of the past. In the financial crisis of 2008–09, for example, many organizations were simultaneously affected. Qualitatively, however, the present crisis is far more severe.

The COVID-19 pandemic and the resulting economic recession have affected most large organizations around the world. Managers continue to scramble to address rapidly developing changes in the public-health environment, public policy, and customer behavior. And then there is the economic uncertainty. The severity and speed of the crisis is reflected in the International Monetary Fund's (IMF) projections for US GDP growth. After an estimated GDP expansion of 2.2 percent in 2019 (year-on-year), the US economy, in the IMF's view, was expected to grow at a rate of 2.1 percent in 2020 (forecast of October 2019). With the onset of the pandemic, the IMF quickly shifted its estimate into contraction, of −5.9 percent in April 2020, revised to −8.0 percent in June. The latest estimate (October 2020) is less severe at −4.3 percent, but this would still be the worst result in many decades. The forecasting institution foresees the world economy shrinking at a rate of −4.4 percent in 2020, after having grown 2.8 percent in 2019 (estimate).[1]

Uncertainty levels from recent global shocks do not approach those of the present COVID-19-triggered crisis. The IMF's GDP contraction forecast for 2020 is more than double the estimated contraction that took place in 2009, the worst year of the earlier global financial crisis. As measured by the Economic Policy Uncertainty Index, a metric developed jointly by researchers at several US business schools, uncertainty on a daily basis has been elevated for nearly 200 days' running.

---

[1] *World economic outlook*, *October 2020: A long and difficult ascent*, International Monetary Fund, October 2020, pp. 141–42, imf.org.

By contrast, commensurate uncertainty was experienced during the 2008–09 financial crisis a few times for a maximum of 27 consecutive days. The COVID-19 outbreak already accounts for seven of the ten highest-ever daily readings.[2] Crises such as Hurricane Katrina or the Fukushima Daiichi nuclear disaster cause high levels of uncertainty for individual communities or particular industries. Since the uncertainty is confined by industry or geography, the magnitude decreases steadily with time. In the present crisis, however, elevated uncertainty is globally pervasive, and events trigger compounding effects. The following exhibit conveys a range of crises and their corresponding levels of uncertainty.

Why existing operating models fail

Extreme uncertainty on a global scale is rare; however, existential crises at the organizational or community level are more frequent and thus provide lessons concerning which operating models succeed and fail during periods of uncertainty. Many organizations, including publicly traded companies, operate on an annual-planning

cycle. Managers collectively decide on strategies, budgets, and operating plans once a year and then manage operations in accordance with those goals and cost limits. Between annual-planning cycles, amendments are few and usually minor. The assumptions shape how managers engage with each other: from the content of status reports to interdepartmental information sharing to the timing and structure of management meetings. Recently, some organizations have adopted more agile techniques to make planning more flexible and responsive to outcomes from pilots or trials. However, the approach is rarely deployed in the C-suite to manage the whole organization.

The COVID-19 crisis has undermined most of the assumptions of the traditional planning cycle. Existing management operating models are no longer supporting managers effectively in addressing the challenges this crisis presents. The revenue assumptions managers relied on for 2020, often worked out to two decimal points, are not relevant in an economy suddenly expected to suffer a historic contraction. Meticulously prepared status reports are now outdated before they reach senior managers. Managers seeking more up-to-date information discover that existing processes are too rigid for a timely response.

Managers thus find themselves working in ways unsuited to a highly uncertain environment. They know what they need: flexibility, the capability to act collectively, quickly, and across the whole organization as challenges arise. They need also to be able to work in this way over an extended period. Some organizations have therefore begun to experiment with new operating models that allow managers to work together. Some of the changes have been successful and others have failed.

Overcoming challenges

To increase the odds that a new operating model will be effective today, managers must ensure that it addresses the problems of operating under highly uncertain conditions. The COVID-19 operating environment requires that managers reexamine their

Exhibit

Duration and magnitude of a crisis are important determinants of uncertainty.
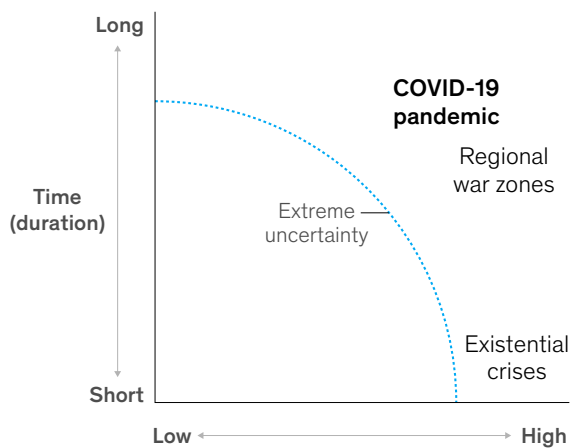
2 "US monthly EPU index," Economic Policy Uncertainty, policyuncertainty.com.

The COVID-19 operating environment requires that managers reexamine their collective thought processes and challenge their own assumptions.

collective thought processes and challenge their own assumptions. Failure to do so will create the risk of serious errors. Here are some of the pitfalls managers will likely encounter:

— *Optimism bias.* Since managers and their organizations have never seen anything like this crisis, existing heuristics learned from years of management might not apply. One common problem is that managers experience optimism bias, both individually and collectively. They will be inclined to bring forward the date of an expected revenue rebound or minimize the duration of expected business closure. Simply, managers cannot or will not believe how bad the situation could get, and the organization ends up planning for a much milder scenario than transpires.

— *Informational instability.* Information is unstable in the COVID-19 pandemic. Epidemiological data are constantly shifting: infection and mortality rates, the proportion of asymptomatic cases, the intensity and effectiveness of testing, the length of the infectious period, and the extent and duration of immunity after infection. The problem extends to poor or missing economic data whose reliability has been affected by the speed and severity of change. Conventional business strategy is most often based on assumptions about a probable course of events. In today's crisis, a single "most likely" planning scenario is unachievable. The sensitivity of statistical models to relatively small changes in assumptions on key variables creates even greater hazard. For example, projections of the

rate of transmission of COVID-19 (R0) are central to forming a view on the likely impact of the disease: even a tiny uptick in the reproduction number can create a dramatic increase in the expected infection and mortality rates and radically change expectations of likely government measures and consumer behavior.

— *Wrong answer.* In addition to the instability of information, leaders must also be sensitive to the possibility that information they thought was clear and certain could turn out to be wrong. Managers cannot take their own assumptions as facts, since new information could emerge that invalidates them. Assumptions and understanding need to be regularly revisited and revised as necessary, as part of the organization's practice of continuous learning. The operating model must be able to absorb initial wrong answers and override them quickly; organizations can even encourage managers to look for opportunities to update assumptions.

— *Paralysis by analysis.* Confusing and ever-changing data can cause managers to delay decisions as they search for more analytical rigor. They may never find it, given the extent of the crisis we are in. Delayed decision making is not advisable in a crisis as fast moving and severe as the COVID-19 pandemic. Delay is in itself a decision, since taking no action has consequences—for example, a continued, unchecked spread of the virus. Managers should rather act on what they do know, and adapt their strategy as new information becomes available.

— *Organizational exhaustion.* In extreme uncertainty, organizations are usually unable to return to business as usual for a long time, sometimes years. This exposes managers and their teams to the risk of exhaustion in the face of constant and apparently never-ending change. A crisis may galvanize a company's senior managers and employees in its initial phase. But once that adrenaline fades, continuing uncertainty becomes enervating. At worst it can take a toll on managers' mental and physical health, causing major harm to organizational effectiveness, from a decline in responsiveness to a deterioration in the overall quality of work.

A suitable organizational structure

When determining how their organization should respond to extreme uncertainty, managers need to estimate the magnitude and expected duration of the crisis. At the onset, a timely and centralized organizational response—"crisis mode"—should be activated. Then leaders need to switch to an operating model that will be sustainable but appropriately reactive to continuing uncertainty over months or even years. A celebrated example is the way the New York City Fire Department handled the aftermath of the September 11 attacks. It had to shift its operating model from one based on immediate response to one that could handle continuing fires at the World Trade Center site and sustain recovery activities for months.

Activating crisis response

The earlier managers determine that they are in a crisis, the faster and more effectively organizations can respond. Effective response is enabled by several fundamental elements.

— *Early-warning system.* A fundamental operating principle in normal times is for senior managers to develop an understanding of the kinds of events that might trigger a crisis. This will allow them to establish appropriate monitoring and early-warning systems. Such systems can be likened to the Intergovernmental Oceanographic Commission's early-warning systems, which rapidly relay data of approaching tsunamis to potentially affected communities.

— *Integrated nerve center.* Once an alarm has been triggered, leaders must have an organizational structure in which a common understanding of the crisis can be developed quickly and decisive actions taken with authority. Such a structure could be part of the organization's ready-made crisis-management plan, but leaders must prepare for the possibility that preconceived structures may be unsuitable in an existential crisis. They must therefore create a new operating model if the situation requires one. The organization needs an integrated nerve center to oversee a holistic crisis response. Within that structure, leadership must identify an inner core: a small group of managers who have the judgment and internal credibility to lead the response. Once identified, these leaders need to be given decision-making authority throughout the crisis, including the top-level support needed to make the "big bets." A recent example of rapid and radical response was the National Basketball Association's decision on March 11 to suspend play for the season. This action was one of the earliest high-profile operational changes taken in the United States in response to COVID-19.

— *Transparent operating principles.* At the outset managers need to define the high-level approach that will guide their actions during the crisis. The approach should be spelled out in a set of operating principles made available throughout the organization. These transparent principles will guide decision making throughout the crisis and provide standards against which management actions can be measured. One example of such transparency can be seen in Airbnb's response to the consequences of the pandemic for the company—a massive drop in revenue and significant layoffs. CEO Brian Chesky wrote an honest letter to the staff

explaining in detail the measures being taken to ensure the company's survival and the ways in which the travel business was being reshaped in the crisis.

Operating in crisis mode: Discover, design, execute
Rapidly moving events demand speedy decisions but also a wholesale change in the organization's managerial modus operandi. The operating cadence in which managers meet, discuss, and take action needs to match the evolution of the crisis. This does not imply a simple speedup of existing processes to accommodate the information needs of managers. Rather, it means creating entirely new procedures.

Extreme uncertainty turns an organization's operating imperatives on their heads. It demands continuous learning and constant review of assumptions. Instead of establishing a plan and ensuring the organization sticks to it, as in more normal times, managers must understand and respond continuously to dynamic and wrenching change. Rather than making periodic reviews of a static plan, they need to meet for iterative decision-making sessions structured around three imperatives: discover, design, execute. Managers must work together to diagnose the current situation, consider its practical implications, explore

how it might evolve, and establish and execute appropriate actions.

The cycle of learning and redesign must recur with frequency sufficient to ensure that responses reflect the evolving situation. Managers must doggedly question established assumptions, especially the ideas adopted under conditions of extreme uncertainty. The organization cannot treat any assumptions as sacrosanct. Organizations should accept that they will be wrong and celebrate learning quickly from experience.

To make informed decisions, managers need specialized knowledge and should actively seek expert advice. Experts can contribute to better decisions by filling gaps in existing management knowledge. For example, managers need external advice—from epidemiologists—to assess the course of the COVID-19 pandemic. Likewise, civil-society organizations can have experts who can provide valuable alternative perspectives on such important matters as racial bias, diversity, and the importance of female leaders. Internal expertise is also valuable in crisis times. Managers should reach deep into their own organization for frontline insights—such as those that a customer-service representative could provide on customer experience.

Instead of establishing a plan and ensuring the organization sticks to it, managers must understand and respond continuously to dynamic and wrenching change.

The organization should also systematically challenge proposed solutions. One established way to do this is to create a "red team" of experts to pressure test managers' decisions, identifying potential weaknesses or overly optimistic assumptions. This type of exercise has been very successful in enabling more robust solutions. Leading companies, including Microsoft and IBM, perform regular exercises in which red teams test cybersecurity infrastructure, for example.

Unprecedented crises frequently require leadership to take unprecedented actions—bold, speedy actions that would feel risky in normal times. A historic case in point is Johnson & Johnson's 1982 decision to recall 31 million bottles of the painkiller Tylenol after some product samples were found to have been laced with cyanide. The swift, decisive action saved this valuable product and enhanced the company's reputation.

As they focus intensely on making fast practical decisions, managers must also be prepared to shift course if the situation changes. Actions, furthermore, need to be prioritized. First must come actions to mitigate the worst-case scenarios for the organization. Low-cost ("no regrets") actions can also be taken quickly, to address issues that could arise in any of several potential scenarios. In an existential crisis, managers must feel comfortable making conscious decisions and taking deliberate action. Otherwise, events will take their course, decisions will be made by default, and organizational control will be lost.

A sustainable model
The global COVID-19 pandemic is in its tenth month, a protracted period defined by extreme uncertainty. Depending on their industrial sector and geography, organizations have experienced different forms of uncertainty at different times over the course of the crisis—with falling consumer demand, supply-

chain disruptions, inventory shortages, and shifting demand across channels. Today companies face economic instability as well as secondary incidents created by extreme uncertainty. To manage an extended recovery period, management structures and processes have to shift to a long-term, sustainable operating model.

One way of thinking about this problem is to imagine that a major fire strikes a company's headquarters. Once the fire itself is extinguished, a different set of challenges emerges, from damage assessment to restarting operations. The shift from crisis mode to recovery of sustainable operations is more an evolution than a transformation. As it reshapes its overall strategy and goals, the organization needs to maintain its integrated nerve center, as crisis circumstances may require reactivation. However, the nerve center would no longer own day-to-day activities. Decisions and actions can increasingly return to their traditional owners such as business units. The operating cadence established in crisis mode will not return to normal, but it will likely moderate. Teams might scale back to meeting weekly from daily but need to maintain the flexibility to ramp back up as needed if something occurs.

The issues to monitor will change, but the importance of monitoring and early warning remains critical. In the COVID-19 crisis, for example, employees continue to work from home in many countries. For this reason, IT departments must remain extraordinarily vigilant in monitoring for cyberattacks. Furthermore, when the time comes for employees to return to their offices, testing and monitoring processes will have to be in place. When infection is detected, quarantine and treatment can thereby quickly follow. The experiences of Korea and China well illustrate the importance of country-level monitoring and quick response in the recovery of public health and the economy.

Whether operating in crisis mode or in recovery mode, leaders still need to prioritize actions. Resilient organizations should be able to begin looking for opportunities once the worst of the crisis is past. Our research indicates, for example, that more resilient companies shifted to M&A quickly after the 2008–09 financial crisis, using the cash saved during the crisis to purchase new assets.

—————————

Extreme uncertainty—defined in terms of novelty, magnitude, duration, and the rapid pace of change—generates a difficult operating environment for managers and organizations. The radically changed circumstances call for new forms of leadership, new ways of working, and new operating models. Crisis-tested managers will develop a tolerance of ambiguity, a quickened operating cadence, and a culture of constant refinement, review, and revision. Management structure and processes need to be adapted, too, as the crisis unfolds, to ensure the organization is sustainable and can take advantage of new opportunities.

Patrick Finn is a senior partner in McKinsey's Detroit office, **Mihir Mysore** is a partner in the Houston office, and **Ophelia Usher** is an expert in the Stamford office.

A unique time for chief risk officers in insurance

Amid rising economic uncertainty, leading insurers are looking to their CROs to do even more than manage risks.

This article was a collaborative effort by Kevin Buehler, Marco Carpineti, Erwann Michel-Kerjan, Fritz Nauck, and Lorenzo Serino, representing views from McKinsey's Risk Practice.

As COVID-19 continues to threaten lives, communities, and industries around the world, insurers face profound disruptions. Uncertainty abounds. No one knows when the crisis will truly end, when safe vaccines will be used at scale, or whether they will stop the pandemic for good. Its ultimate impact on public health and the global economy will be measured in the months and years to come.

Underwriters are struggling to calculate their exposure to pandemic-generated vulnerabilities. Economists are trying to anticipate the direct and indirect impact of massive new government debt. Managers are wondering how long people can work productively from home and maintain healthy organizational and risk cultures. And in a long-lasting low-interest-rate environment, strategists

and product leaders are contemplating future insurance solutions—including public–private insurance partnerships—that would enable insurers to remain relevant to their customers.

Our research shows that the industry's returns to shareholders since the beginning of the year were down by 19 percent at the end of October 2020. In mid-June they had been down by 23 percent—the sharpest drop in recent memory and deeper than those recorded in many other industries (Exhibit 1).

With regard to current business impact, insurers will experience pressure on retention rates and margins as customers shop for lower prices. The impact on claims will vary by line of business: auto claims may decline because people are driving less at the moment, but homeowners' claims could rise as

Exhibit 1

Market capitalization has declined across sectors in 2020, with significant variation in the extent of the declines.

Shareholder returns in 2020 by industry,[1] % (Jan–Oct 2020)
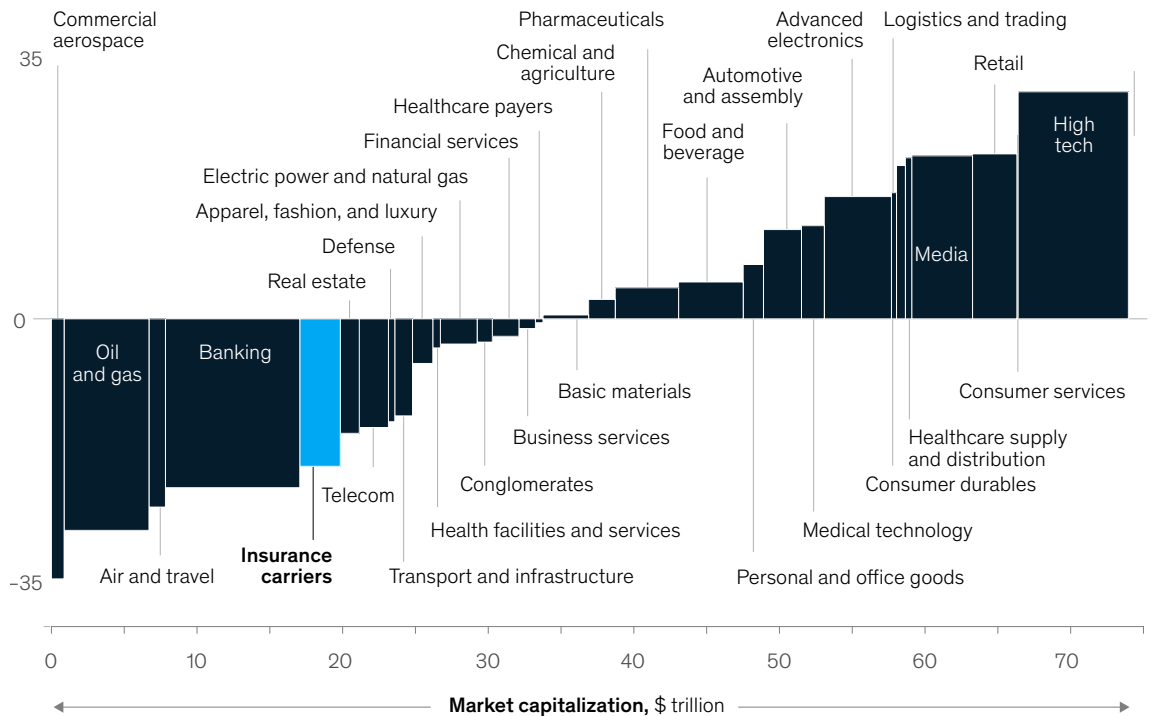
[1]Weighted average; shareholder returns calculated in local currency; width of bars is starting market capitalization in US dollars; data set includes global top 5,000 companies by market capitalization in 2019, excluding some subsidiaries, holding companies, and companies that have since delisted.
Source: S&P Capital Insights; McKinsey analysis

CROs are engaged in the most difficult decisions, providing top management with perspectives and guidance on strategic business risks.

policyholders work from home. Investment income will continue to suffer as interest rates stay low, and life and annuity carriers will be hardest hit. We also believe that the pandemic's full impact on economies around the world will be felt through 2022.

The pandemic-related challenges intersect with cost-reduction and efficiency pressures. These were intense before the pandemic struck, as discussed in McKinsey's recent state-of-the-industry reports on P&C[1] and on life.[2] Legacy IT systems and, in some cases, lagging digital capabilities are growing impediments, as the COVID-19 environment pushes many more customers toward digital-first relationships. Insurers, reinsurers, and brokers that made bold moves into digital years ago are now harvesting the benefits of their investments. Others need to catch up in a hurry.

Given the profound uncertainties and their varying impact across business lines, insurers must commit strongly to risk-oriented, structured decision-making approaches. We believe it is time for chief risk officers (CROs) to step up to this challenge. With their help, the industry can reinvent itself to stay relevant to customers and attractive to investors.

The CRO and the evolution of the insurance industry

CROs for leading insurers are playing a critical role in the present risky and uncertain environment. They have risk oversight of activities conducted by the first line (business and corporate functions) and assure the chief executives and boards that companies are achieving a proper risk-management balance. In approaching heightened risk levels, CROs aim to limit the downside danger but also enable the business to make the necessary risk–reward trade-offs to capture the upside. It is a delicate balance.

For a long time—and especially as a consequence of the financial crisis of 2008–09—the CRO role in financial services was regarded as a necessary response to regulatory pressure, to provide required controls and guardrails. Today, the importance of the CRO role has outgrown this conception, and that is a good thing. Many CROs are working with CEOs, executive teams, and boards, stepping forward in this crisis and taking the opportunity to shape the future of the organizations they serve. Over the past few months, we have been listening to leaders of insurers of all sizes around the globe—CEOs, board members, CFOs, HR heads, as well as CROs. One insight that has emerged is that the CRO role as risk manager has continued to evolve. CROs are engaged in the most difficult decisions, providing top management with perspectives and guidance on strategic business risks—when to take them and for which expected financial, organizational health, and reputational rewards.

Unsurprisingly, therefore, leading insurers are investing more in their risk-function capabilities. At a recent CRO roundtable with 25 leading North American insurers, 95 percent of the participants indicated that demand for the services of the risk

---

[1] Sylvain Johansson, Andy Luo, Erwann Michel-Kerjan, and Leda Zaharieva, "State of property & casualty insurance 2020: The reinvention imperative," April 2020, McKinsey.com.
[2] "Life insurance and annuities state of the industry 2018: The growth imperative," October 2018, McKinsey.com.

function will increase next year. At this critical juncture, CROs should join top management to set and implement a strategy for capturing value in the next three to five years. A new CRO role is evolving:

— from using static, backward-looking risk-measurement tools to developing state-of-the art capabilities, such as scenario planning, dynamic stress testing, and advanced analytics
— from focusing only on financial risk to taking a more holistic view of the risk landscape, including nonfinancial risk: the new focus includes cyberrisk, technology risk, fraud risk, model risk, people risk, and compliance risk, but also wider external risks, including climate risk and geopolitical risk
— from performing a limited-control function to counseling the CEO and board in developing and executing a sustainable growth strategy supported by a balanced risk appetite

The CRO's contribution to a sustainable growth strategy

This is an important moment for chief risk officers. Most insurance companies are rethinking their strategies and need the knowledge and skills of CROs to navigate the perils of unprecedented times. To support a sustainable growth strategy under stressed conditions, CROs can start by maximizing the risk organization's existing capabilities. New capabilities are also needed as CROs help their companies embrace a holistic view of risk, including financial and nonfinancial risks. The following actions are essential and consistent with the new CRO leadership paradigm.

Managing risk through COVID-19 uncertainties
It will be necessary to develop high-frequency stress tests and business-plan forecasts and to review investment strategies.

1. Develop high-frequency stress tests and business-plan forecasts. To reveal vulnerabilities

and develop strategic implications, CROs should develop advanced stress-testing for profit and loss (P&L) and the balance sheet (for example, investment portfolios). The program should be scenario-based and refined through iteration. Carriers around the world, from employee-benefit companies to global multiline insurers, have developed analytical tools to rebase revenue expectations using detailed economic data. Some risk leaders are gaining new insights into market dynamics in metropolitan statistical areas by combining customer projections with epidemiological and economic scenarios. This can help improve the accuracy of projections of customer default or renewal rates: projections can become more precise with stronger links between risk identification, economic scenarios, and overall company strategy.

2. Review the investment strategy. Pressure on industry performance is coming from several sources, including equity-market volatility, the low-interest-rate environment, and sometimes the repricing of assets associated with climate risk. The squeeze is felt on insurers' balance sheets, product profitability in life insurance, and investment-management fees for savings products. Given these pressures, CROs will need to ensure that the investment strategy is reviewed and realigned according to the results based on economic scenarios and resulting risk capacity and risk appetite.

Addressing the nonfinancial-risk profile
Here are measures to strengthen cyberrisk practices, address fraud and other operational risks, and adapt and remediate models.

3. Strengthen cyberrisk practices. The new working environment has increased network exposures to cyberrisk. As employees use personal devices for work, for example, they can become more vulnerable to phishing. Traffic volumes

are rising sharply on virtual private networks as employees work from home, straining IT systems and personnel; sensitive data and systems must be protected against access through insecure networks or devices. CROs must take account of these new strains and vulnerabilities, and strengthen cybersecurity and cyber practices across the organization. Many insurance companies have completed comprehensive assessments of their systems and information assets—for example, the likelihood that any component will be compromised. CROs must prioritize and reprioritize assets as needed, protecting critical assets and closing critical control gaps as they appear.

4. Pay more attention to fraud. Fraud and financial crime[3] seem to be on the rise as a result of the new remote-working environment and the economic downturn, a situation recalling the spike in insurance fraud during the financial crisis of 2008–09. As CROs strengthen essential controls and the technology infrastructure, they should also push to improve analytics capabilities for fraud. The necessary moves could include building an identification engine capable of ingesting vast amounts of claims data, accurately sizing and analyzing drivers of current losses, and quickly identifying high-risk claim reimbursement.

5. Address other operational risks. Rising levels of digital interaction and remote work have also changed companies' overall operational risk profiles, which CROs must monitor and assess accurately. They can then build tools to mitigate these and other nonfinancial risks and quickly address emerging concerns. In a recent McKinsey survey of North American carriers, participants discussed their latest approaches to nonfinancial risk. One large global life insurer, for instance, launched an ambitious review of its nonfinancial-risk metrics and upgraded them in key businesses, covering the entire nonfinancial-risk taxonomy in great detail. Before the pandemic, the company had begun to shift its reportage from lagging to

leading indicators to help executives gain a more accurate view of risks and make better-informed decisions. That gives them a significant advantage during the pandemic crisis.

6. Adapt and remediate models. The CRO should lead a full review of critical models used across the organization since they could have been compromised in this changed environment. The assessment should include the rapid triage and remediation of models most affected by the pandemic. The associated economic downturn has triggered significant step changes that are often not accounted for in the original assumptions made several years ago, when these models were designed. The persistent low-interest-rate environment—and potentially negative-interest-rate environment—must also be factored in. The CRO should manage remediation on a risk-based timeline and ask the business to develop new models as needed.

Building the insurance organization of the future
CROs should partner with senior management to revisit the risk appetite and strategy, transform risk culture, build reputational resilience, and improve insights about systemic risks.

7. Partner with senior management to revisit the risk appetite and strategy. By becoming thought partners with top management, CROs can help steer the organization, identifying and selectively committing to strategic opportunities. They can also engage in dialogue with regulatory agencies to better anticipate the regulatory landscape. CROs have a key role to play in shaping the risk appetite. The CRO should work closely with the CEO, the CFO, and the heads of businesses to help cascade it through the whole organization, calibrate it as part of the new sustainable growth strategy.

8. Transform the risk conduct and culture framework. In the current environment, companies have to make decisions quickly—too quickly,

---

[3] Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, "Transforming approaches to AML and financial crime," September 2019, McKinsey.com.

sometimes, for existing governance and guardrails. An appropriate framework for risk conduct and culture creates a safe environment for speaking up about dangers, fosters adherence to company values, and therefore helps risk leaders make sustainable decisions quickly. As CROs work with top management to develop the future organization, they should partner with HR heads to transform the risk culture.[4] Many insurers have already begun to assess current risk culture and to identify opportunities for improvement by making employees aware of present and emerging risks and giving them the skills to protect both policyholders and the organization. Risk culture can be measured and actions taken to enhance it where improvements are most needed.

9. Build reputational resilience. The pandemic is creating unprecedented challenges to organizational culture. In the work-from-home model, maintaining that culture and transmitting it to new hires can be more difficult. Furthermore, as companies address their customers' changing needs, they must take into account the heightened public scrutiny and societal impact of the ongoing crisis. The CRO must therefore ensure that robust governance is in place, and work to strengthen risk culture and organizational resilience.

10. Significantly improve the company's insights about systemic risks. The pandemic is a reminder that low-probability, high-consequence events do indeed happen. Pandemic scenarios were heretofore mostly considered as extreme cases in advanced modeling exercises. That no longer works. With the right mandate from the rest of the organization, the central risk function could become a center of excellence to protect insurers by developing and defining better insights on systemic risk. The center of excellence could also identify issues—climate change and geopolitical risks, for example—that call for innovations to keep insurers relevant in a fast-changing risk landscape.

More sophisticated stress testing to discover business vulnerabilities

For many financial institutions, including insurers, annual investment and product planning was completed before the economic impact of the COVID-19 pandemic was universally apparent. In performing stress tests on the impact of market stress on solvency, most insurers used short-term, next-budget-cycle timelines. Now, deep into the pandemic, insurers understand that the economic recovery path is uncertain and performance may change widely during the next two- or three-year period, and even beyond. The changing probabilities concerning the duration of the work-from-home model and restrictions on travel and retail activity, for example, make it clear that more than short-term planning is required. In this context, companies must go beyond their normal stress-testing regimens.

To understand how rapidly evolving economic conditions will affect their portfolios, leading insurers are using stress-testing tools accompanied by continued close monitoring. They are looking beyond regulatory compliance and building the data and capabilities needed to test scenarios rapidly and to support responsive decision making according to the changing outcomes. New analytics skills and tools are needed, which for most insurers would complement existing capabilities in scenario-based assessments of assets and liabilities. They can be developed using existing resources and capabilities present in the risk organization, in a coordinated effort by the CEO, CFO, CRO, and the heads of businesses.

Insurers need to think through scenarios with varying timelines and sequences of events and how they intersect with different types of stress testing—for liquidity and capital, business strategy, and climate and catastrophic events. This holistic assessment will give CROs a wider view of the uncertainties and therefore support effective risk management. Exhibit 2 shows how more

---

[4] Richard Higgins, Grace Liou, Susanne Maurenbrecher, Thomas Poppensieker, and Olivia White, "Strenghtening institutional risk and integrity culture," November 2020, McKinsey.com.

sophisticated stress tests can account for many factors affecting P&Ls over longer time horizons.
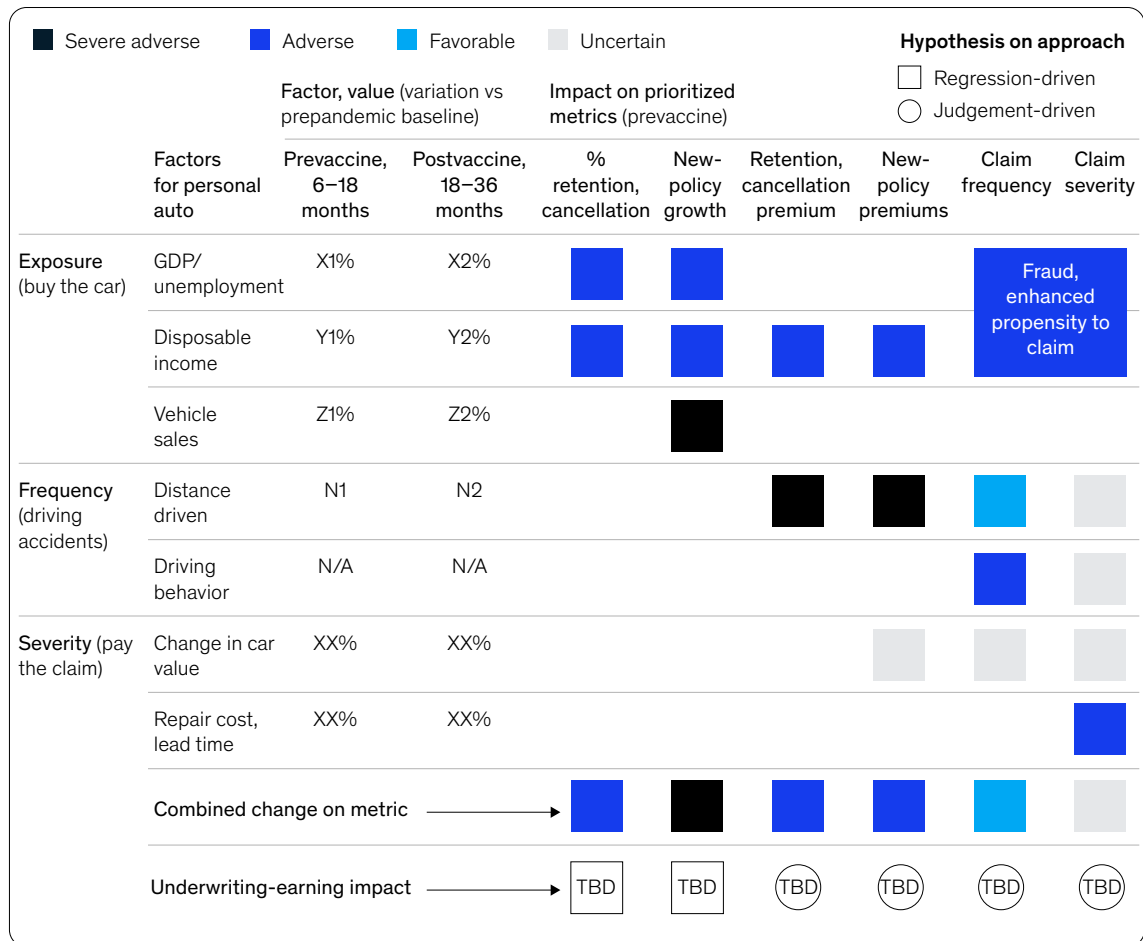
The new orientation also requires a shift in the stress-test horizon from one year to a three- or four-year period. The objective is rapid design and testing of a wide range of scenarios exploring different company vulnerabilities. The method involves the development of more sophisticated econometric models—statistical analysis of economic data—using detailed, location-specific analytics, since the dynamics of economies will probably differ widely from one city to another. The models should use relevant business-sensitivity metrics (such as policy renewals or new sales) to estimate the impact of different scenarios on business performance and to act on those estimates. Insurers can use these exercises to reallocate capital quickly across the product lines and markets where it can be put to best use.

Exhibit 2

Stress testing links scenarios to the key profit-and-loss factors of underwriting income.

Sanitized auto-insurance dashboard example, impact of factors on P&L metrics

Legend: ■ Severe adverse ■ Adverse ■ Favorable ☐ Uncertain

Hypothesis on approach: ☐ Regression-driven ○ Judgement-driven

Factors for personal auto	Factor, value (variation vs prepandemic baseline)		Impact on prioritized metrics (prevaccine)					
	Prevaccine, 6–18 months	Postvaccine, 18–36 months	% retention, cancellation	New-policy growth	Retention, cancellation premium	New-policy premiums	Claim frequency	Claim severity
Exposure (buy the car)								
GDP/unemployment	X1%	X2%	■ (Adverse)	■ (Adverse)			Fraud, enhanced propensity to claim (Adverse)	
Disposable income	Y1%	Y2%	■ (Adverse)	■ (Adverse)	■ (Adverse)	■ (Adverse)		
Vehicle sales	Z1%	Z2%		■ (Severe adverse)				
Frequency (driving accidents)								
Distance driven	N1	N2			■ (Severe adverse)	■ (Severe adverse)	■ (Favorable)	☐ (Uncertain)
Driving behavior	N/A	N/A					■ (Adverse)	☐ (Uncertain)
Severity (pay the claim)								
Change in car value	XX%	XX%				☐ (Uncertain)	☐ (Uncertain)	☐ (Uncertain)
Repair cost, lead time	XX%	XX%						■ (Adverse)
Combined change on metric ⟶			■ (Adverse)	■ (Severe adverse)	■ (Adverse)	■ (Adverse)	■ (Favorable)	☐ (Uncertain)
Underwriting-earning impact ⟶			TBD (□)	TBD (□)	TBD (○)	TBD (○)	TBD (○)	TBD (○)

Many of these capabilities require significant business expertise and may now lie in the realm of business planning and strategy. However, risk teams have the unique analytical and data capabilities to support such modeling. These broader stress tests will also help CROs develop a view of potential emerging business risks and set the company's strategic direction.

The CRO role in increasing efficiency and effectiveness

Operational efficiency and effectiveness have always been vital in insurance, and the pandemic has made them more important than ever. CROs can lead or contribute to efforts to address the challenges—for example, by shifting governance or strengthening the most critical controls. Partnering with the first line, CROs can work to minimize the burden of controls, without compromising the effectiveness of risk management. On a deeper level, and with CRO involvement, insurers should return to developing process-automation and artificial-intelligence programs. The CRO can help speed up these advances and free colleagues to focus more keenly on the risks requiring experience and judgment.

———————

The insurance industry is undergoing significant change to remain relevant in a changing risk environment that is now evolving even faster as result of the pandemic. We believe that the gap between companies that embrace and act upon these changes, make bold moves, and capture the resulting value and those that do not will continue to widen. Experience suggests that if companies adapt quickly to the crisis and emerge stronger in the first year, they will continue to lead for the next five. The pandemic has certainly elevated the risk function's strategic role. CROs now have a unique opportunity to seize the moment.

Extraordinary risks

The disaster you could have stopped: Preparing for extraordinary risks

Ignoring high-consequence, low-likelihood risks can be damaging to an organization, but preparing for everything is impossibly costly. Here is how leaders can make the right investments.

by Fritz Nauck, Ophelia Usher, and Leigh Weiss
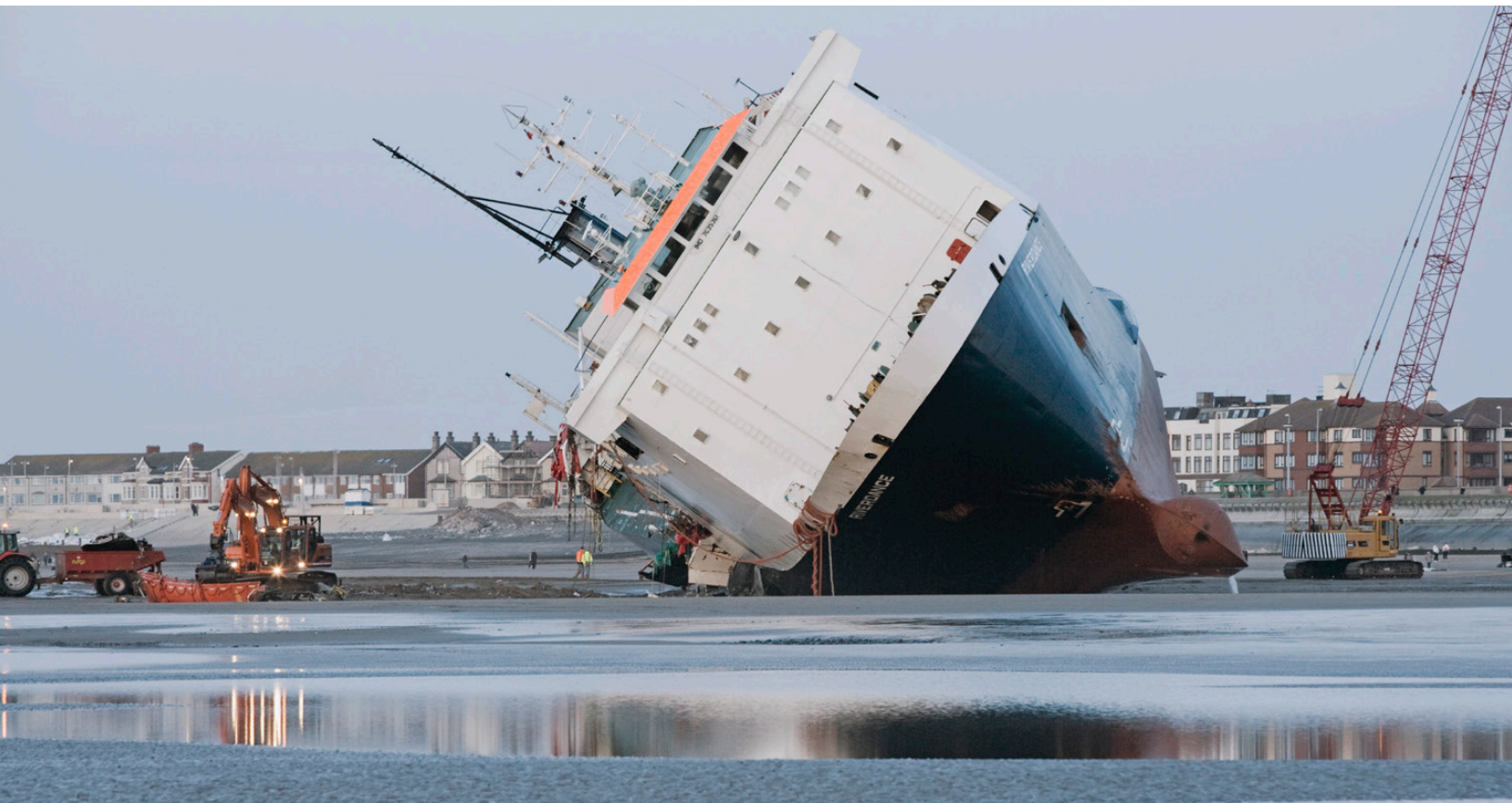
The COVID-19 crisis is dramatically highlighting the potential impact of high-consequence, low-likelihood risks. Low but never zero: that is the probability of risks such as a viral epidemic ballooning into a pandemic that costs millions of lives and shuts down economies across the globe. The chances of an extraordinary regional catastrophe, whether naturally occurring or human-caused, are similar, as are the disastrous effects. A severe earthquake, a massive oil spill, or a nuclear accident can result in heavy loss of life, ecological damage, and financial loss for countries and companies.

The relative improbability of such events well illustrates the decision makers' dilemma: which of them should their organizations plan for? The danger of a pandemic was not unknown. Health organizations and policy makers discussed the danger on the global stage. Many organizations accounted for it in their enterprise-risk-management (ERM) frameworks as a high-consequence, low-likelihood event. Some organizations, especially in the healthcare and travel sectors, even had firsthand experience with the SARS pandemic in 2003. Nonetheless, companies were by and large unprepared for COVID-19. More than 50 billion-dollar companies have filed for bankruptcy in 2020 in the United States alone. As Exhibit 1 shows, furthermore, the pandemic's adverse economic effects have varied widely by industry sector.

Some high-consequence, low-likelihood risks have to do with business strategy, such as those posed by the digital disruption; operational risks are another category and include serious quality-control failures

Exhibit 1

The impact of the COVID-19 pandemic in the United States varies widely by industry sector.

Year-over-year change in real GDP for selected industries, 2Q 2019 to 2Q 2020,[1] %
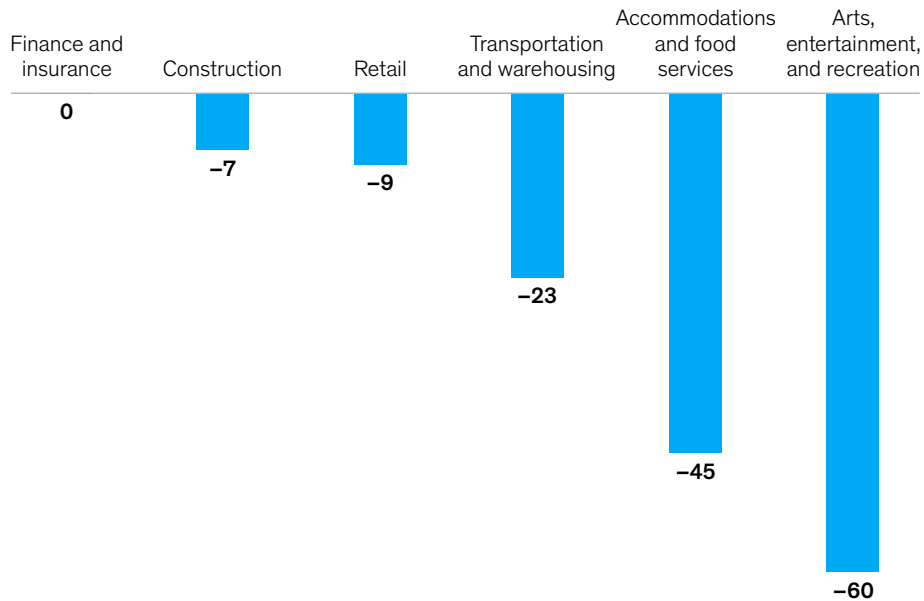
Note: As of October 2, 2019.
[1] Indexed to 4Q 2019.
Source: Bureau of Economic Analysis

in manufacturing. Missed opportunities are another equal source of extraordinary risk. Opportunities to adopt disruptive innovation can bring companies to crucial moments of truth, when movers gain significant market advantage over hesitant peers. Amazon, for example, moved to help third parties build e-commerce sites, leading to Amazon Web Services (AWS). Now, through AWS, Amazon has around 30 percent of the cloud-computing market.[1] Our work on resilient corporations demonstrated that those able to do more than just hunker down in an economic crisis—retaining the wherewithal to invest in new opportunities—will emerge from it in a strengthened position.

Some organizations have even built business models around taking advantage of low-likelihood opportunities (such as those in pharmaceutical pipelines). The models allow for fast movement when a high-consequence risk or opportunity occurs. Missing a high-consequence opportunity can lead to ultimate demise just as ignoring a risk can.

A recent article in the *McKinsey Quarterly* described the decisions by boards or management teams to ignore or act on these high-consequence, low-likelihood risks as "big bets." That characterization is based on the broad scope of a decision and the size of its impact.[2] When it comes to extraordinary risks, the decisions are also governed by the unfamiliarity and infrequency of these risks. These consequential decisions are not highly visible parts of the CEO's public agenda, unlike more familiar big bets such as mergers and acquisitions. For example, the decision by Nokia's mobile-phone division to develop a response to potential supply-chain disruptions was not even discussed by investors. This decision allowed the telecommunications company to act fast to find alternative chips suppliers when a fire disrupted the normal supply. The move led to Nokia expanding its share of the global market and boosting profits significantly.[3] The big bet in supply-chain resiliency doubly paid off in this high-consequence,

low-likelihood event, as potential losses were averted and a large opportunity was captured.

Big risks that matter

The number of potential high-consequence, low-likelihood risks is far too great for corporate decision makers to plan for all of them. Indeed, the abundance of possibilities is one reason why some companies don't plan for any of them. The first strategic requirement that is often missing when addressing these risks, therefore, is the identification of the risks that matter. This action, known as risk ID, is an important part of robust ERM. It means differentiating risks that could hurt the business from risks that could damage or destroy the company.

Some organizations have concluded that such existential risks are unknowable. This is an error, in our view. By far, most existential crises that companies have faced in recent years were identified in advance by experts—from oil spills to chemical disasters to nuclear accidents.

The threats behind these high-profile incidents were known and recognized in advance by industry and government specialists. They were "predictable surprises," as Michael Watkins and Max Bazerman described in an eponymous article in the *Harvard Business Review.*[4] Predictable surprises meet three criteria: first, they are the result of risks decision makers know are possible, even if unlikely—such as a 500-year flood. Second, leaders feel confident that if the risk materializes, the event will have a big impact on the whole organization. Third, predictable surprises require organizations to respond.

Sometimes, but not always, these risks are identified in ERM frameworks, where they are categorized as high consequence, low likelihood. The predictable surprises found here can include epidemics, pandemics, cyberattacks, hurricanes,

[1] Ron Miller, "How AWS came to be," Tech Crunch, July 2, 2016, techcrunch.com.
[2] Aaron De Smet, Gregor Jost, and Leigh Weiss, "Three keys to faster, better decisions," *McKinsey Quarterly*, May 2019, McKinsey.com.
[3] Amit S. Mukherjee, "The fire that changed an industry," InformIT, October 1, 2008, informit.com.
[4] Michael Watkins and Max Bazerman, "Predictable surprises: The disasters you should have seen coming," *Harvard Business Review*, April 2003, hbr.org.

floods, financial fraud, economic recessions, oil spills, and other catastrophes, whether natural or human-caused. Decision makers should prioritize these potential threats, making big bets on those that would precipitate an existential crisis for their organization.

Understanding the potential impact of such events is the first step for decision makers in reducing the chance that a particular event results in an existential crisis. The likelihood does not matter for these risks—they are all unlikely, according to traditional ERM programs. Once scored by ERM, they all land in the same low-likelihood corner. However, the impact on the organization *does* matter. Not all the risks are equal: some would create an existential crisis while others would not. Thus decision makers need a way to distinguish among these high-consequence, low-likelihood risks.

Identifying the most important risks

To identify and define the most important risks, we recommend using a two-by-two risk grid (Exhibit 2). In this plan, the potential impact of an event on the whole company is situated along the vertical axis and the decision makers' level of certainty about the impact is situated on the horizontal axis. High placement on the vertical axis means that the company's existence would be threatened if this risk occurred—or the company would miss a massive opportunity. Low vertical-axis placement means that the impact or opportunity would be limited or isolated. The vertical axis allows senior decision makers to distinguish risks that require board- and CEO-level attention from those that can be managed at a lower level. These risks will vary significantly by company and industry sector. For example, the impact of COVID-19 is varied according to a company's ability to conduct operations and serve customers with employees working remotely.

A risk placed to the right on the horizontal axis means that decision makers are relatively certain of its scope and intensity; leftward placement signals doubt about the risk's reach and impact. Using the horizontal axis, decision makers recognize the differences between familiar risks with known impact and risks that they are still investigating. The placement of low-certainty risks will shift as decision makers learn more about the potential risk.

Exhibit 2

Organizations must plan for predictable surprises—events that would pose an existential crisis.

High-consequence, low-likelihood risks can be plotted according to scope and certainty of impact
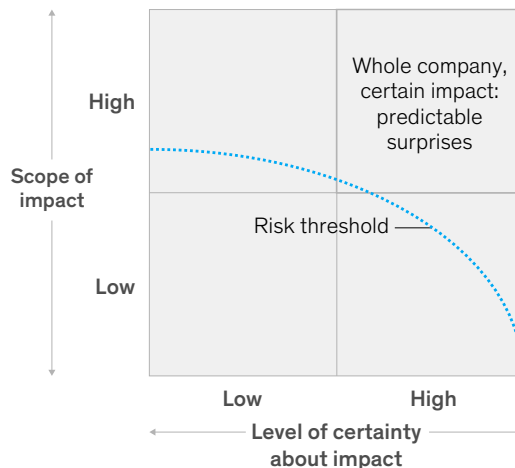
Potential risks are ranked in relation to each other, rather than on an absolute scale. This approach allows decision makers to separate into distinguishing categories risks that are traditionally grouped together in ERM frameworks. The technique could be used by an insurer, for example, to create differentiated products by applying deeper segmentation to populations formerly categorized as high risk.

Risks placed in the upper-right corner are the high-consequence, low-likelihood risks that everyone agrees would pose an existential threat to the company. These can then be addressed with the big bets and they might move lower down on the vertical axis as a result. Big bets to address these types of risks can take many forms—financial, operational, or strategic. Energy providers, for example, sometimes divide their organizations into several legal entities so that a catastrophic loss in one physical location would not result in a collapse of the entire enterprise.

Despite big-bet actions, the potential impact of certain risks may not diminish. As long as a process is in place for quickly identifying and addressing an emerging event, the company will survive and may also thrive (as Nokia did). Decision makers can also move risks up or down on the vertical axis as they learn more about potential impact. The same risk could have widely different impact on different companies (see sidebar, "Different companies, same risk, different impact).

Risks and the core of the organization

Decision makers locate potential risks, such as a pandemic, on their own grid after defining their core business and identity and understanding what impact a risk would have on this core. The core of the company could include products and services, the loyalty of a customer segment, public perception, brand identity, and legal requirements that must be met. For example, technical failure of a particular part can adversely affect the reputation of a manufacturer's entire product line; high-profile fraud

can damage a financial institution by undermining customer confidence. Reliable service provision could be at the core of a company, especially where customers have a switching option. Decision makers identify core elements by the essential role they play; without them, the business would disappear.

Once the core is established, decision makers can identify the high-consequence, low-likelihood risks that would adversely affect the core, locating the risks along the vertical axis of the grid. Risks that would not affect an organization's core are less likely to create an existential crisis. By focusing on the core, decision makers are making their organization's strategy crystal clear. Those organizations with clear strategies are nearly three times more likely than others to lead in their sector. Those that make good decisions faster, that is, are more likely to outperform industry peers.

In one category of existential risk are catastrophic operational failures, such as those caused by natural disasters, accidents, negligence, and cyberattacks. Reputational risk events can also set off existential crises; these may be the result of operational failures, cyberattacks, data breaches, or fraud and other forms of financial malfeasance. Decision makers can look along their ERM frameworks for the most common risk segments: health and safety, reputation, operations, strategy, compliance, and financial.

It is also important to consider other risk segmentations to avoid missing critical risks—*internal risks* arising from the business model, for example, versus *external risks*, such as those potentially arising from global economic conditions. Other useful risk pairs to consider are adversarial risks such as an activist investor or cyber- or terrorist attacks, versus nonadversarial risks such as natural or human-caused disasters and accidents. High-consequence, low-likelihood risks that could cause existential damage might be found in any of these categories. The impact will of course depend on the company's established core and many other variables.

Different companies, same risk, different impact

The exhibit demonstrates how pairs of companies with much in common and some differences would assess the same risk on the risk grid.

The first scenario shows two electronics companies with the same value proposition and different operating models. They make the exact same product for the same customers. The main difference between them is their supply chain. Electronics company A has a resilient supply chain with several sources of raw materials and several manufacturing sites. Electronics company B has a leaner supply-chain model. If the two companies are assessing the risk of a pandemic, electronics company B is at greater risk of a whole-company disaster, and the greater risk is shown in the risk grid.

Scenario two shows two retail companies with different business value propositions. One sells traditional men's and women's fashion items that are stable from year to year. The other sells trendy fashion items that have a life cycle of eight weeks, after which they lose their customer appeal. Imagine these two companies are assessing the risk of a labor strike in the major US port they share where their items arrive from Asia. If the clothing items of trendy fashion company C are stuck in a port for months, the items become virtually worthless. Customers are not interested in last quarter's fashions. The traditional

Exhibit

The same risk will have a different impact on different companies, depending on culture, supply chain, financials, and other characteristics.

Crisis scenarios for pairs of companies in three sectors

■ Weak attribute ■ Stable attribute ■ Strong attribute

	Scenario 1 Same business value proposition, different operating model		Scenario 2 Different business value proposition		Scenario 3 Same business value proposition, different organizational culture	
	Electronics company A	Electronics company B	Trendy fashion company C	Traditional fashion company D	Automaker E	Automaker F
Customer loyalty	Strong	Strong	Strong	Stable	Strong	Stable
Brand identity	Stable	Strong	Strong	Strong	Strong	Strong
Supply-chain resilience	Strong	Weak	Strong	Strong	Stable	Strong
Psychological safety[1]	Strong	Stable	Strong	Stable	Weak	Strong
Inventory durability	Stable	Stable	Weak	Strong	Weak	Weak
Financial stability	Strong	Strong	Stable	Stable	Strong	Stable
Certainty of impact	High	High	Medium	Medium	Medium	Medium
Impact on whole company	Medium	High	High	Medium	High	Medium

[1] The freedom to raise mistakes and problems without fear of repercussions.

fashion company's items can still be sold because their styles are more enduring. The risk assessment varies, as shown on the corresponding risk grids.

Finally, the third scenario shows two auto manufacturers with similar business value propositions and different organizational cultures. Automaker F has a culture of empowered employees who are given freedom to take risks and where failure is seen as an opportunity to learn and improve. Their relatively flat organizational structure and culture of personal ownership passes bad news up the chain of command when necessary. In contrast, automaker E has a hierarchical structure with a risk-averse culture of finger-pointing and blaming others. When mistakes are noticed, they are usually papered over, because no one wants to be the person to share bad news. Imagine these two companies are assessing the potential of a major quality-control problem. Both companies are fairly certain that such a risk exists. Automaker E is much more concerned about the impact of that risk on the company because it is much less likely to be reported if it is discovered.

Organizations can sometimes survive existential crises, though with diminished value. But crises and missed opportunities can also cause an entire organization to fail. It is therefore important for decision makers to consider all types of high-consequence, low-likelihood risks. By measuring the impact on the core, they can differentiate among them, illuminating the particular issues that are of highest importance to the organization.

Conducting a 'premortem' for risk events

The premortem exercise is a technique decision makers can use to identify which predictable surprises would have serious consequences on their organization. It involves a thought exercise in which the core value proposition is assumed to have been damaged or destroyed. Decision makers then consider all the possibilities that could have led to this, with help from risks experts who have been warning about the potential for such events. Missed opportunities should also be considered. A diversity of perspectives and the quality of debate are essential conditions for making high-quality, big-bet decisions quickly. To obtain perspectives of sufficient diversity, especially for external risks, organizations sometimes need to bring in experts. For example, an insurance company might bring in hydrologists and climate-change scientists to consider how their exposure to flood risk might be evolving. Once these "whole-company risks" have been identified, decision makers can plot them on their risk grid based on the size and certainty of their impact on the company's core value.

Avoiding bias in your risk grid

When identifying the risks of greatest consequence, decision makers need to avoid optimism bias—a view that tends to see more positive outcomes than the evidence warrants. Confirmation and anchoring bias also reduce predicted impact—through assumptions that future threats will recapitulate those of the past.

Biases can be partly neutralized by a healthy organizational culture in which people are rewarded for speaking up, sharing dissenting ideas, and listening to others' voices. For such a culture to thrive, people must feel completely secure in sharing their views. Without that personal security, important risks might go undiscovered. Whistleblowers, furthermore, must be protected and their concerns investigated—especially when the risks in question are those that could cause physical harm—such as catastrophic accidents due to product-safety failures.

Impact measurement

The goal is to create a risk grid where the predictable surprises that could destroy the organization are measured according to impact. Their probability is not in question here, since all of these risks are considered low likelihood.

However, an organization's confidence in its impact assessments does matter. Once the risks are mapped on the vertical axis (severity of impact), decision makers must continue to probe them.

On the horizontal axis (certainty of impact), risks positioned to the left (low certainty) could shift position as more about them is learned. For those risks situated farther to the right on this axis, their higher certainty of impact signals to the board and the CEO that mitigating these risks will require investment (big bets).

Taking action

Starting with the high-consequence, low-likelihood risks of greatest impact—those in the upper-right hand corner of the grid—the organization must decide on what actions would reduce their potential impact to an acceptable level. What is acceptable will vary by board and management team, based on many factors, including inherent risk within their industry and availability of resources. Decision makers recognize that many of these risks—earthquakes, pandemics, recessions—are outside the organization's control. With such risks, the objective is to reduce—below the existential threshold—their potential impact on the organization.

To identify and decide on the most effective actions, decision makers can assemble external and internal experts and cross-functional teams. A diverse perspective and sharp, high-level discussion are needed for this task. Lists of potential actions can be generated and pared down as the teams discuss them. In one approach to this step, participants create lists of choice actions that if taken today could reduce risk down the road. Then they fast-forward into six-month or one-year scenarios and identify a small decision that could have made a big difference in protecting the core value of the organization. Alternatively, experts develop potential actions, and a "red team" pressure-tests

them; in another approach, leaders are chosen and assigned to explore these questions and monitor the organization for ideas. Whatever method an organization chooses, the outcome should be a range of potentially effective actions for decision makers to consider.

From the lists, leaders should identify actions that could reduce the impact of several risks at once. Those that would reduce harm significantly in the here and now can be taken as no-regrets moves; others can be designated as trigger-based decisions, to be taken when certain conditions occur.

No-regrets moves might include the creation of a more resilient supply chain by allowing single-source suppliers as an exception only. The introduction of multiple sources for a majority of items promotes resiliency while helping companies manage working-capital costs. This example aligns with a broader suite of resiliency solutions, such as adequate capitalization for rainy days, strong stakeholder relationships, a culture of people speaking up, and a crisis-response plan. Creating more resiliency could be a big-bet option that decision makers might consider because it strengthens an organization's ability to withstand risk events.

Decision makers might also think about developing leading indicators for predictable surprises. This no-regrets move gives decision makers more time to respond to a threat, reducing its adverse impact. Leading indicators of financial fraud, for example, might be overly smooth profits or a rise in the use of nondisclosure agreements (NDAs). Other leading indicators can help detect significant arising opportunities.

Some actions are taken once the likelihood of a particular risk event reaches a certain threshold or trigger. A weather forecast, for example, with a reasonable amount of certainty that a company's operations are in the path of an oncoming hurricane

would trigger necessary countermeasures. Decision makers should develop the appropriate actions while ensuring that the triggers they choose provide enough of a window for the actions to be effective. The objective is to protect the company's core value proposition. An example of an effective trigger and response would be a storm warning that sets in motion actions to stop production on an offshore rig to prevent an oil spill. Obviously, trigger-based decision making requires a monitoring process that alerts the organization when a trigger has occurred.

Protecting against extraordinarily rare events may seem counterintuitive. The risks are many and resources are finite. By defining the core value

proposition, however, leaders can identify and mitigate the risks that would threaten the whole company.

High-consequence, low-likelihood events can fatally damage an organization. The investments organizations make to protect their value propositions—and not miss significant opportunities—can mean the difference between extinction and survival. More than that, however, these investments (big bets) can improve an organization's overall resiliency.

Fritz Nauck is a senior partner in McKinsey's Charlotte office, **Ophelia Usher** is an expert in the Stamford office, and **Leigh Weiss** is a senior expert in the Boston office.

How the voluntary carbon market can help address climate change

The voluntary carbon market is gaining momentum and plays an increasingly important role in limiting global warming. Here's how.

This article was a collaborative effort by Christopher Blaufelder, Joshua Katz, Cindy Levy, Dickon Pinner, and Jop Weterings.

As business leaders set increasingly ambitious commitments to reduce global greenhouse-gas (GHG) emissions, a market is developing that can help to achieve them by supplementing companies' efforts to reduce their own emissions. This is the rapidly growing market for voluntary carbon credits.

Carbon credits (often referred to as "offsets") have an important dual role to play in the battle against climate change. They enable companies to support decarbonization beyond their own carbon footprint, thus accelerating the broader transition to a lower-carbon future. They also help finance projects for removal of carbon dioxide from the atmosphere—delivering negative emissions, which will be needed to neutralize residual emissions that will persist even under the most optimistic scenarios for decarbonization. However, while the voluntary carbon credit market is currently experiencing significant momentum, it is still relatively small. The recently launched report by the Taskforce on Scaling Voluntary Carbon Markets aims to create a blueprint for solutions that could help overcome obstacles to its further growth. (For more about the taskforce, which McKinsey supports as a knowledge partner, please read our article "Scaling voluntary carbon markets to help meet climate goals."[1]) This article will explain how carbon credits work and how they can help in the global effort to address climate change.

The dual role of voluntary carbon credits in addressing climate change

A carbon credit is a certificate representing one metric ton of carbon dioxide equivalent that is either prevented from being emitted into the atmosphere (emissions avoidance/reduction) or removed from the atmosphere as the result of a carbon-reduction project. For a carbon-reduction project to generate carbon credits, it needs to demonstrate that the achieved emission reductions or carbon dioxide removals are real, measurable, permanent, additional, independently verified, and unique (see sidebar "Criteria for carbon credits"). If a project meets these criteria—as specified by independent

standards such as Gold Standard and Verified Carbon Standard (VCS)—credits can be issued. The impact of a carbon credit can only be claimed—that is, counted toward a climate commitment—once the credit has been retired (canceled in a registry), after which it can no longer be sold. A carbon credit is considered a "voluntary carbon credit" when it is bought and retired on a voluntary basis rather than as part of a process of compliance with legal obligations.

The proceeds from the sale of voluntary carbon credits enable the development of carbon-reduction projects across a wide array of project types. These include, among others, renewable energy; avoiding emissions from fossil-fuel-based alternatives; natural climate solutions, such as reforestation, avoided deforestation, or agroforestry; energy efficiency; and resource recovery, such as avoiding methane emissions from landfills or wastewater facilities.

While most of the projects types that include renewable energy, avoided deforestation, and resource recovery focus on *avoiding* carbon emissions, others, such as reforestation, focus on *removing* carbon dioxide from the atmosphere. This is a meaningful difference, illustrating the dual role voluntary carbon credits can play in addressing climate change:

— *In the short term,* voluntary carbon credits from projects focused on emissions avoidance/reduction can help accelerate the transition to a decarbonized global economy, for example by driving investment into renewable energy, energy efficiency, and natural capital. Avoiding emissions is typically the most cost-efficient way to address atmospheric GHG concentrations.

— *In the medium to long term,* voluntary carbon credits could play an important role in scaling up carbon dioxide removals (or negative emissions) needed to neutralize residual emissions[2] that cannot be further reduced.

---

[1]Christopher Blaufelder, Cindy Levy, Peter Mannion, Dickon Pinner, and Jop Weterings, "Scaling voluntary carbons markets to help meet climate goals," November 2020, McKinsey.com.
[2]Emissions that can only be eliminated at prohibitive cost or that cannot be eliminated with existing technology.

Criteria for carbon credits

Carbon credits should represent emission reductions or carbon dioxide removals that are:

— real and measurable—realized and not projected or planned, and quantified through a recognized methodology, using conservative assumptions

— permanent—not reversed; relating to projects with a reversibility risk such as forestry projects, which could suffer from fire, logging, or disease; here, comprehensive risk mitigation and a mechanism to compensate for any reversals need to be in place

— additional—would not have been realized if the project had not been carried out, and the project itself would not have been undertaken without the proceeds from the sale of carbon credits

— independently verified—verified by an accredited, independent third party

— unique and traceable—transparently tracked in a public registry and not double-counted

Additionally, it is important that appropriate safeguards are in place to ensure projects comprehensively address and mitigate all potential environmental and social risks.

In a recent analysis, we found that at least 5 gigatons of negative emissions will be needed annually to reach net-zero emissions by 2050. These could be realized through a combination of natural climate solutions such as reforestation (for example, sequestering carbon in trees) and nascent technology-based carbon capture, use, and storage solutions such as direct air capture with carbon storage (DACCS), and bioenergy with carbon capture and storage (BECCS). Voluntary carbon credits can help finance the scale-up of these solutions.

The role of voluntary carbon credits in corporate climate commitments

A credible corporate climate commitment begins with setting an emissions reduction target that covers both a company's direct and indirect GHG emissions: if a company does not already have an emissions baseline from which to set a target, creating one is a necessary first step. Aligning such a target's ambition level with the latest climate science is widely seen as best practice. In other words, the target needs to be in line with the level of decarbonization required to limit global warming to well below 2 degrees Celsius above preindustrial levels at a minimum—and ideally be in line with a 1.5-degree pathway, which scientists estimate would reduce the odds of initiating the most dangerous and irreversible effects of climate change. For setting such a target, the Science Based Targets initiative has developed methodologies, which have been already adopted by more than 1,000 companies, including many leading multinationals. To achieve the required emissions reductions, companies can pull levers such as improving energy efficiency, transitioning to renewable energy, and addressing value-chain emissions.

As a next step, a company may commit to a target that involves the use of voluntary carbon credits—either to compensate for emissions that it has not been able to eliminate yet or to neutralize residual emissions that cannot be further reduced due to prohibitive costs or technological limitations. These types of targets come with

various designations (for example, carbon neutral, climate neutral, net-zero, carbon negative, climate positive) but they all typically involve a company supplementing reductions achieved within its own carbon footprint by financing reductions elsewhere through the purchase and retirement of voluntary carbon credits (see sidebar "Types of carbon targets"). By offsetting its remaining emissions in this way, a company can claim it is mitigating its residual impact on the climate. Some, such as Microsoft, have gone further by setting aspirations to make a net-positive impact on the climate.

Strong momentum, mainly driven by new corporate commitments and point-of-sale offerings

Following three years of robust growth, the voluntary carbon market[3] reached a record high in 2019, both in issuances and retirements (exhibit). Issuances were 138 million tons of carbon dioxide equivalent—almost double the 2018 volume— and retirements 70 million, a 33 percent increase compared with 2018. This growth has been driven by a combination of new corporate climate commitments, such as those to carbon neutrality and net zero, as well as so-called point of sale offerings of voluntary carbon credits, such as Shell's carbon-neutral fuel, which is a bundled retail offering of gasoline and voluntary carbon credits and airline-passenger offsetting programs, which enable passengers to offset the emissions of their flights through the airline's website.

Based on year-to-date volumes and an extrapolation in line with historical seasonality patterns, we expect the market to set another

---

[3] We estimated the voluntary carbon market size based on five standards: VCS, Gold Standard, Climate Action Reserve, American Carbon Registry, and Plan Vivo. We excluded ARB-eligible credits and Gold Standard–labeled Certified Emission Reductions (CERs) used for meeting compliance targets.

Types of carbon targets

In the context of corporate target setting, "carbon neutral" refers to offsetting all unabated greenhouse-gas emissions through the application of carbon credits to a given part of an organization's footprint (for example, company-level, activity-level, product-level), usually on an annual basis. The term carbon neutral is typically used to cover other greenhouse gases as well; relevant standards, such as PAS2060, clearly specify carbon neutral's scope as including carbon dioxide equivalent (CO_2e) emissions, beyond just carbon dioxide.

"Climate neutral" is often used interchangeably with carbon neutral, but it places more of an emphasis on covering greenhouse gases beyond carbon dioxide. In addition, it can include climate impacts other than greenhouse-gas emissions, for example, radiative forcing from aircraft contrails.

While the exact definition of "net zero" is still being debated, it is considered a forward-looking commitment requiring companies to reduce their emissions and balance remaining (residual) emissions by a given target year. There is an emerging view among stakeholders, including nongovernmental organizations and corporate climate leaders, that a credible net-zero target requires reducing emissions in line with the latest climate science and neutralizing residual emissions (at net zero) using carbon dioxide removals (not carbon credits from emissions avoidance/reduction projects).

Finally, both "carbon negative" and "climate positive," which are used interchangeably, have not yet been clearly defined, but they imply going beyond the targets described above to make a net-positive impact on our climate.

The voluntary carbon market has grown significantly in recent years.

Voluntary carbon market, millions of metric tons of carbon dioxide equivalent ■ Issuances ■ Retirements
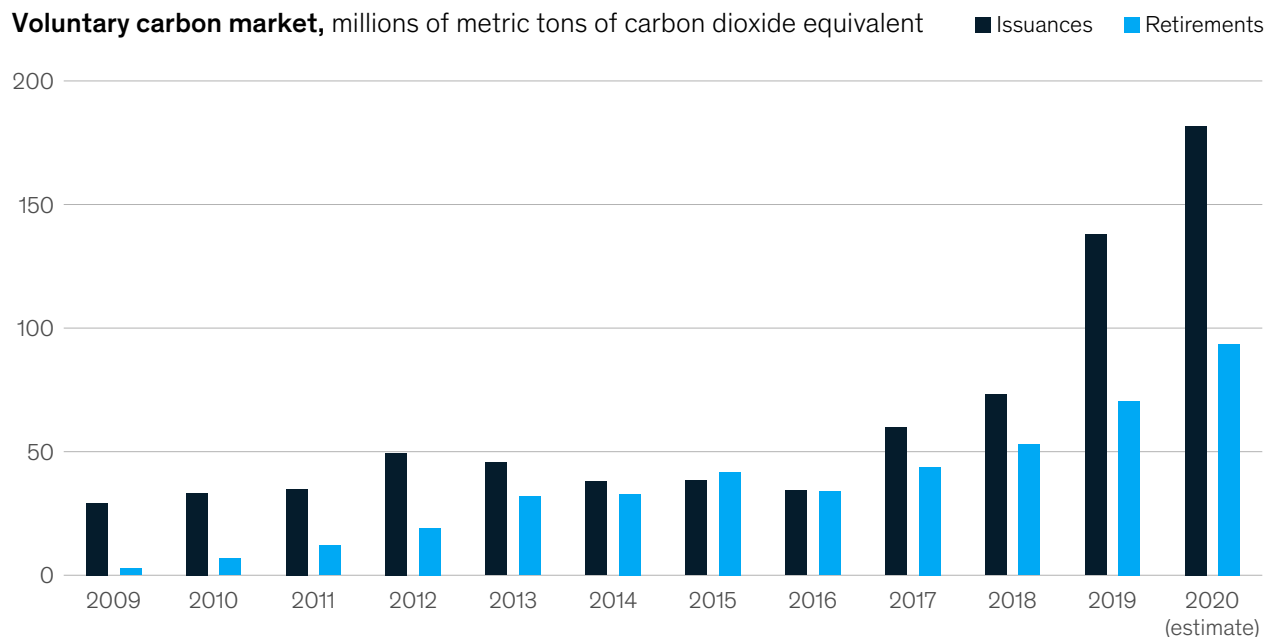
Note: We estimated the voluntary carbon market size based on 5 standards: Verified Carbon Standard (VCS), Gold Standard (GS), Climate Action Reserve (CAR), American Carbon Registry (ACR), and Plan Vivo. We excluded ARB-eligible credits and Gold Standard–labeled CERs used for meeting compliance targets. Data were retrieved from aforementioned registries on December 2, 2020, for YTD volumes up until the end of November (ie, 150 million tCO_2e of issuances and 81 million tCO_2e of retirements). We projected volumes for full-year 2020, based on extrapolation in line with historical seasonality (past 5 years), and did not adjust for any COVID-19 related impacts on seasonality patterns.
Source: ACR; CAR; GS; Plan Vivo; VCS

record this year, with issuances and retirements both growing by approximately one-third compared with 2019. After years of declining prices (from an average price of around $7 per ton in 2008 to around $3 per ton in 2019[4]) due to supply outpacing demand, we expect average prices to go up in the near to medium term, mainly due to strong demand growth especially for higher-cost project types such as reforestation and carbon dioxide removal projects more generally (see sidebar "Issuances and retirements"). While still relatively small, the voluntary carbon market is experiencing significant momentum and its impact (and future potential) is getting more and more attention.

Natural climate solutions (NCS), a category including project types such as reforestation, avoided deforestation, improved forest management, and agroforestry, have grown faster than any other project category and contributed significantly to the voluntary carbon market's growth trajectory. From 2016 to 2019, issuances within this category more than doubled every year, on average—and in 2019, NCS accounted for 53 percent of total issuances. Meanwhile, retirements in this category have also rapidly grown (close to 50 percent per year, on average). We believe this trend could be the result of increased awareness of NCS's potential (they can deliver one-third of the emissions reductions

[4]According to the Ecosystem Marketplace.

Issuances and retirements

To analyze the voluntary carbon market, we focus on two metrics: issuances and retirements, which together give a good idea of market dynamics. Issuance volume is a proxy for supply, as it represents voluntary carbon credits issued by a standard (for example, Gold Standard, VCS) upon the successful verification of emission reductions or carbon dioxide removals realized by a certified carbon-reduction project. Retirement volume is a proxy for demand, as it represents voluntary carbon credits bought and canceled in a registry, preventing the onward sale of the certificates. Only upon retirement can the buyer in whose name the credit was retired claim its impact (that is, count the credit toward a climate commitment).

needed to align with the Paris Agreement between now and 2030[5]), a growing focus on carbon dioxide removal (of which NCS is the most cost-effective and technologically proven method), and buyers' preference for co-benefits beyond climate-change mitigation, such as biodiversity and impact on local communities.

What's next: Challenges and opportunities

To accelerate the voluntary carbon market's growth trajectory and realize its full potential, it will be important to address some significant challenges. These include the need to strengthen impact and quality assurance, to align stakeholders on the criteria for credible use of voluntary carbon credits as part of an overall climate strategy, build new market infrastructure, and reduce regulatory uncertainty. We believe that implementing innovative solutions to these challenges could unlock further growth. The recently launched Taskforce on Scaling Voluntary Carbon Markets aims to create a blueprint for these solutions.

Strengthening impact and quality assurance

While reputable standards such as Gold Standard and VCS certify projects' adherence to the requirements of their respective methodologies, buyers typically have limited transparency on the progress of the carbon-reduction projects in their portfolio. Stakeholders also regularly raise questions about certain types of projects, such as those related to additionality in large-scale renewable-energy projects; biodiversity in the context of afforestation projects planting non-native species and/or monocultures; leakage and insufficient local-community engagement in the case of avoided deforestation; or permanence of natural climate solutions more broadly (see sidebar "Additionality, leakage, and permanence defined").

While reputable standards have implemented safeguards to address these issues, the combination of insufficient transparency and continued stakeholder skepticism has led buyers to demand a further strengthening of impact and quality assurance. As a result, we expect innovation in measurement, reporting, and verification practices to accelerate over the coming years.

Aligning stakeholders on credible use of voluntary carbon credits

There is currently no consensus among stakeholders on what it takes to use voluntary carbon credits credibly as part of an overall climate strategy. Therefore, companies may have different interpretations of the role voluntary carbon credits could play in their journeys toward net-zero. Key points of discussion include the extent to which

---

[5] Bronson Griscom et al., "Natural climate solutions," *Proceedings of the National Academy of Sciences*, October 2017, Volume 114, Number 44, pp. 11645–50, pnas.org.

Additionality, leakage, and permanence defined

A carbon-reduction project is considered "additional" when its impact (emission reductions and/or removals) would not have been realized if the project had not been carried out, and that the project itself would not have been undertaken without the proceeds from the sale of carbon credits. As technology costs continue to fall, a growing number of renewable-energy projects no longer need the proceeds from the sale of carbon credits to be viable—a key reason why the criterion of additionality is particularly relevant in the context of renewable energy projects. In response, standard bodies have started to phase out large-scale renewable-energy projects. For example, VCS no longer certifies new, grid-connected renewable-energy projects unless they're located in the least-developed countries.

Leakage occurs when a carbon-reduction project displaces emission-causing activities and produces higher emissions outside the project boundary. For example, protecting a certain forest area may cause loggers to go elsewhere. Leakage risk can be mitigated by strengthening project design as well as conservatively quantifying emission reductions and removals, making appropriate adjustments for estimated leakage.

Carbon-reduction projects should realize permanent emission reductions and/or removals. Where projects have a reversibility risk—such as forestry projects, which could suffer from fire, logging, or disease—comprehensive risk mitigation and a mechanism to compensate for any reversals needs to be in place. It is common practice for standard bodies to include buffer provisions (requiring all projects with reversibility risk to set aside a certain percentage of credits in a buffer or insurance pool). In the unfortunate event of a reversal of emission reductions and/or removals (for example, due to fire or disease), credits from the buffer would be used to cover the losses.

a company can rely on voluntary carbon credits versus reducing its own footprint; the type of credits (for example, emissions avoidance/reduction versus carbon dioxide removal) to use, and how their role may evolve over time. There is a clear distinction between the role of voluntary carbon credits today and that which they will play when a company has all but fully decarbonized its footprint and needs only to neutralize its residual emissions.

Building new market infrastructure

Today, voluntary carbon credits are mainly traded over the counter, resulting in limited transparency on market data (for example, transaction volumes, price levels) and a paucity of reference data, which was a key barrier to market growth in the past. Standardized, tradable products and contracts could help increase liquidity and scale transactions, provided that the quality of credits traded and integrity of market participants are ensured.

Reducing regulatory uncertainty

The negotiations over the Paris Agreement's Article 6, which introduces a new international carbon market/mechanism, are ongoing. As a result, the implications of Article 6 for the voluntary carbon market are still unclear. Should voluntary purchases of carbon credits by private-sector actors help countries achieve their post-2020 climate pledges (which are referred to as nationally determined contributions), or should they be incremental to such targets? Will governments continue to allow projects to issue voluntary carbon credits? When is double-counting an issue, and how can that be avoided?

Reducing regulatory uncertainty may encourage more buyers to make long-term commitments, and developers to make large-scale investments.

———————

Voluntary carbon credits could play a critical role in helping the world attain a 1.5-degree pathway. They can both accelerate the transition to a lower-carbon future by enabling companies to support decarbonization beyond their own carbon footprint and help neutralize residual emissions by financing carbon dioxide–removal projects. To realize this potential, significant practical effort is required to address current challenges and scale up the voluntary carbon market. Achieving that will create significant benefits not just in the battle against climate change but also in preserving nature and the untold benefits it provides to humanity.

Christopher Blaufelder is a partner in McKinsey's Zurich office; **Joshua Katz** is a partner in the Stamford office; **Cindy Levy** is a senior partner in the London office; **Dickon Pinner** is a senior partner in the San Francisco office; and **Jop Weterings** is director of environmental sustainability, based in the Amsterdam office.

Derisking

Derisking AI by design: How to build risk management into AI development

The compliance and reputational risks of artificial intelligence pose a challenge to traditional risk-management functions. Derisking by design can help.

by Juan Aristi Baquero, Roger Burkhardt, Arvind Govindarajan, and Thomas Wallace

Artificial intelligence (AI) is poised to redefine how businesses work. Already it is unleashing the power of data across a range of crucial functions, such as customer service, marketing, training, pricing, security, and operations. To remain competitive, firms in nearly every industry will need to adopt AI and the agile development approaches that enable building it efficiently to keep pace with existing peers and digitally native market entrants. But they must do so while managing the new and varied risks posed by AI and its rapid development.

The reports of AI models gone awry due to the COVID-19 crisis have only served as a reminder that using AI can create significant risks. The reliance of these models on historical data, which the pandemic rendered near useless in some cases by driving sweeping changes in human behaviors, make them far from perfect.

In a previous article, we described the challenges posed by new uses of data and innovative applications of AI. Since then, we've seen rapid change in formal regulation and societal expectations around the use of AI and the personal data that are AI's essential raw material. This is creating compliance pressures and reputational risk for companies in industries that have not typically experienced such challenges. Even within regulated industries, the pace of change is unprecedented.

In this complex and fast-moving environment, traditional approaches to risk management may not be the answer (see sidebar "Why traditional model risk management is insufficient"). Risk management cannot be an afterthought or addressed only by model-validation functions such as those that currently exist in financial services. Companies need to build risk management directly into their

Why traditional model risk management is insufficient

Model risk management (MRM) in regulated industries such as banking is currently performed by dedicated and independent teams reporting to the chief risk officer. While these firms have developed a robust MRM approach to improve the governance and control of their critical models determining capital requirements and lending decisions, this approach is usually not ideal for firms with different requirements or in less heavily regulated industries, for the following reasons:

— MRM is typically based on a point-in-time model assessment (for example, once every one to five years), which assumes that the models are largely static between reviews. AI models learn from data, and their logic changes when they are retrained to learn from new data. For instance, a fraud model is retrained weekly in order to adapt to new scams.

— Traditional MRM workflows are often sequential and require six to 12 weeks of review time after the model development is complete, which delays deployment. These workflows are not easily adapted to the agile and iterative development cycles frequently used in AI model development.

— MRM is often focused more on traditional risk types (primarily financial risks, such as capital adequacy and credit risk) and may not fully cover the new and more diverse risks arising from widespread use of AI such as reputational risk, consumer and conduct risk, and employee risk.

— Some applications and use cases, such as chatbots, natural-language processing, and HR analytics, can qualify as "models" under regulatory definitions used in banking. But these

applications are very different from the traditional model types (for example, capital models, stress-testing models, and credit-risk models), and traditional MRM approaches are not easily applied.

— AI and machine-learning algorithms are often embedded in larger AI application systems, such as software-as-a-service (SaaS) offerings from vendors, in ways that are significantly more complex and more opaque than traditional models. This greatly complicates coordination between those who review the model and those who assess the application and platform (IT risk) or the vendor (third-party risk).

AI initiatives, so that oversight is constant and concurrent with internal development and external provisioning of AI across the enterprise. We call this approach "derisking AI by design."

Why managing AI risks presents new challenges

While all companies deal with many kinds of risks, managing risks associated with AI can be particularly challenging, due to a confluence of three factors.

AI poses unfamiliar risks and creates new responsibilities

Over the past two years, AI has increasingly affected a wide range of risk types, including model, compliance, operational, legal, reputational, and regulatory risks. Many of these risks are new and unfamiliar in industries without a history of widespread analytics use and established model management. And even in industries that have a history of managing these risks, AI makes the risks manifest in new and challenging ways. For example, banks have long worried about bias among individual employees when providing consumer advice. But when employees are delivering advice based on AI recommendations, the risk is not that one piece of individual advice is biased but that, if the AI recommendations are biased, the institution is actually systematizing bias into the decision-making process. How the organization controls bias is very different in these two cases.

These additional risks also stand to tax risk-management teams that are already being stretched thin. For example, as companies grow more concerned about reputational risk, leaders are asking risk-management teams to govern a broader range of models and tools, supporting anything from marketing and internal business decisions to customer service. In industries with less defined risk governance, leaders will have to grapple with figuring out who should be responsible for identifying and managing AI risks.

AI is difficult to track across the enterprise

As AI has become more critical to driving performance and as user-friendly machine-learning software has become increasingly viable, AI use is becoming widespread and, in many institutions, decentralized across the enterprise, making it difficult for risk managers to track. Also, AI solutions are increasingly embedded in vendor-provided software, hardware, and software-enabled services deployed by individual business units, potentially introducing new, unchecked risks. A global product-sales organization, for example, might choose to take advantage of a new AI feature offered in a monthly update to their vendor-provided customer-relationship-management (CRM) package without realizing that it raises new and diverse data-privacy and compliance risks in several of their geographies.

Compounding the challenge is the fact that AI risks cut across traditional control areas—model, legal, data privacy, compliance, and reputational—that are often siloed and not well coordinated.

AI risk management involves many design choices for firms without an established risk-management function

Building capabilities in AI risk management from the ground up has its advantages but also poses challenges. Without a legacy structure to build upon, companies must make numerous design choices without a lot of internal expertise, while trying to build the capability rapidly. What level of MRM investment is appropriate, given the AI risk assessments across the portfolio of AI applications? Should reputational risk management for a global organization be governed at headquarters or on a national basis? How should we combine AI risk management with the management of other risks, such as data privacy, cybersecurity, and data ethics? These are just a few of the many choices that organizations must make.

Baking risk management into AI development

To tackle these challenges without constraining AI innovation and disrupting the agile ways of working that enable it, we believe companies need to adopt a new approach to risk management: derisking AI by design.

Risk management by design allows developers and their business stakeholders to build AI models that are consistent with the company's values and risk

appetite. Tools such as model interpretability, bias detection, and performance monitoring are built in so that oversight is constant and concurrent with AI development activities and consistent across the enterprise. In this approach, standards, testing, and controls are embedded into various stages of the analytics model's life cycle, from development to deployment and use (Exhibit 1).

Typically, controls to manage analytics risk are applied after development is complete. For example, in financial services, model review and validation often begin when the model is ready for implementation. In a best-case scenario, the control function finds no problems, and the deployment is delayed only as long as the time to perform those checks. But in a worst-case scenario, the checks turn up problems that require another full development cycle to resolve. This obviously hurts efficiency and puts the company at a disadvantage relative to nimbler firms (see sidebar "Learning the value of derisking by design the hard way").

Similar issues can occur when organizations source AI solutions from vendors. It is critical for control teams to engage with business teams and vendors early in the solution-ideation process, so they understand the potential risks and the controls to

mitigate them. Once the solution is in production, it is also important for organizations to understand when updates to the solution are being pushed through the platform and to have automated processes in place for identifying and monitoring changes to the models.

It's possible to reduce costly delays by embedding risk identification and assessment, together with associated control requirements, directly into the development and procurement cycles. This approach also speeds up preimplementation checks, since the majority of risks have already been accounted for and mitigated. In practice, creating a detailed control framework that sufficiently covers all these different risks is a granular exercise. For example, enhancing our own internal model-validation framework to accommodate AI-related risks results in a matrix of 35 individual control elements covering eight separate dimensions of model governance.

Embedding appropriate controls directly into the development and provisioning routines of business and data-science teams is especially helpful in industries without well-established analytics development teams and risk managers who conduct independent reviews of analytics or manage

Learning the value of derisking by design the hard way

A large food manufacturer developed an analytics solution to forecast demand for each of its products across geographies in order to optimize manufacturing, logistics, and the overall supply chain. The new model showed higher accuracy compared with the company's existing expert-based approach.

But before the model was deployed, the manufacturer initiated an independent third-

party review of the model, which uncovered several problems with the model, including a critical data leakage. The model had accidentally included a feature that captured the actual demand. Once the feature was removed, the model accuracy dropped below the existing expert-based approach.

This revelation led to a complete redesign of the model architecture and the realization

that the company needed to undertake a broader initiative to embed risk management into model development to prevent this and other issues from recurring. The manufacturer began the effort by creating new roles within the group to perform model review, defining roles and responsibilities for model checks throughout the modeling pipeline, and implementing standards for development and documentation of analytics.

Exhibit 1

Risk management by design embeds controls across the algorithmic model's life cycle.
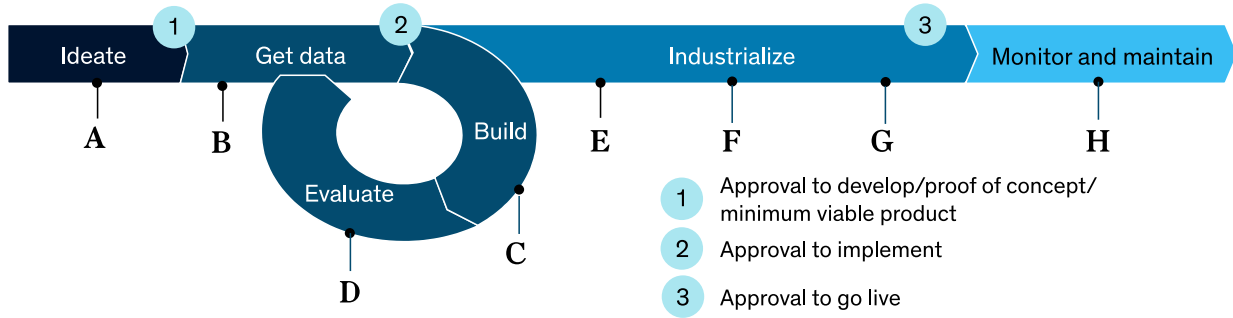
A Designing the solution

Controls examples: scoping review, evaluation metrics, assessment of environment including available data

B Obtaining reliable data required to build and train model

Controls examples: data-pipeline testing, data-sourcing analysis, statistical-data checks, process and data-usage fairness, automated documentation generation

C Building a model that achieves good performance in solving the problem specified during ideation

Controls examples: model-robustness review, business-context metrics testing, data-leakage controls, label-quality assessment, data availability in production

D Evaluating performance of model and engaging business regularly to ensure business fit

Controls examples: standardized performance testing, feature-set review, rule-based threshold setting, model-output review by subject-matter expert, business requirements, business restrictions, risk assessment, automated document generation, predictive-outcome fairness

E Moving model to production environment

Controls examples: nonfunctional-requirements checklist, data-source revalidation, full data-pipeline test, operational-performance thresholds, external-interface warnings

F Deploying model where it starts being used by the business

Controls examples: colleague responsibility assignment and training, escalation mechanisms, workflow management, audit-trail generation

G Inventory management of all models

Controls examples: search tool, automated inventory statistical assessment and risk overview by department

H Live monitoring in production

Controls examples: degradation flagging, retraining scheduler, periodic testing such as Bayesian hypothesis testing, automated logging, and audit-trail generation

Review and approval for continued use

Controls example: verification that algorithm continues to work as intended and its use continues to be appropriate in current environment

associated risk. They can move toward a safe and agile approach to analytics much faster than if they had to create a stand-alone control function for review and validation for models and analytics solutions (see sidebar "An energy company takes steps toward derisking by design").

As an example, one of the most relevant risks of AI and machine learning is bias in data and analytics methodologies that might lead to unfair decisions for consumers or employees. To mitigate this category of risk, leading firms are embedding several types of

controls into their analytics-development processes (Exhibit 2):

— *Ideation.* They first work to understand the business use case and its regulatory and reputational context. An AI-driven decision engine for consumer credit, for example, poses a much higher bias risk than an AI-driven chatbot that provides information to the same customers. An early understanding of the risks of the use case will help define the appropriate requirements around the data and

methodologies. All the stakeholders ask, "What could go wrong?" and use their answers to create appropriate controls at the design phase.

— *Data sourcing*. An early risk assessment helps define which data sets are "off-limits" (for example, because of personal-privacy considerations) and which bias tests are required. In many instances, the data sets that capture past behaviors from employees and customers will incorporate biases. These biases can become systemic if they are incorporated into the algorithm of an automated process.

— *Model development*. The transparency and interpretability of analytical methods strongly influence bias risk. Leading firms decide which methodologies are appropriate for each use case (for example, some black-box methods will not be allowed in high-risk use cases) and what post hoc explainability techniques can increase the transparency of model decisions.

— *Monitoring and maintenance*. Leading firms define the performance-monitoring requirements, including types of tests and frequency. These requirements will depend on the risk of the use case, the frequency with which the model is used, and the frequency with which the model is updated or recalibrated. As more dynamic models become available (for example, reinforced learning, self-learning), leading firms use technology platforms that can specify and execute monitoring tests automatically.

Putting risk managers in a position to succeed—and providing a supporting cast

To deploy AI at scale, companies need to tap an array of external and unstructured data sources, connect to a range of new third-party applications, decentralize the development analytics (although common tooling, standards, and other centralized capabilities help speed the development process), and work in agile teams that rapidly develop and update analytics in production.

These requirements make large-scale and rapid deployment incredibly difficult for traditional risk managers to support. To adjust, they will need to integrate their review and approvals into agile or

An energy company takes steps toward derisking by design

Companies in industries that have been running analytical models for decades under the scrutiny of regulators, such as financial services, often have a foundation for moving to a derisk-by-design model.

Organizations in industries that have adopted analytics more recently and are less regulated (at least in the area of model outputs) will need to build their capabilities nearly from scratch.

One large North American energy company initiated a multiyear analytics transformation in order to improve the efficiency of current assets—for example,

to produce higher-quality coal. The company set up an analytics center of excellence (COE), which discovered that thousands of analytics use cases had been developed and deployed across the organization without any clear oversight, creating risks for human health and safety, financial performance, and company reputation.

In response, the COE appointed a model manager to oversee the model-governance rollout across the organization. The manager's team identified six key priorities: implementing a process to identify models as they are developed; creating

a centralized inventory for all analytics use cases and related information (such as developer and owners); establishing a tiering system to identify the most material models; creating standards for model development and documentation; defining and implementing requirements for model review and monitoring for all models; and defining model-governance processes, roles,and responsibilities for all stakeholders across the modeling pipeline. These changes helped the organization take a giant step toward embedding risk management into the end-to-end process of model development.

Exhibit 2

Bias is one important risk that can be mitigated by embedding controls into the model-development process.

Illustrative example

● Guidance and checklists   ● Analytical methods and data tools

Ideation	Data sourcing	Model development	Industrialization, monitoring, and maintenance
Determine the **level of bias risk,** given model use and context.	Detect and mitigate bias risk in data.	Find and reduce bias through modeling.	Continuously monitor and manage bias risk in production.

Ideation

● Bias and explainability risk assessment

How can we **set up a team to reduce or mitigate** risk of bias?

● Guidance on convening a diverse team

What **legal and reputational constraints should we take into account?**

● Scoping and regulatory guidance

How will we **measure bias** for this use case in this usage context?

● Creation of bias risk metrics

What is the **level of our analytics capabilities?**

● Capability context assessment

Data sourcing

● Bias-detection techniques

● Fair-representation techniques

● Evaluation of risk from the choice of data sets and collection methods

● Mitigation of risk in feature selection and engineering

● Documentation with data sheets for data sets

Model development

● Explainable AI techniques to explain root cause

● Counterfactual analysis

● Review of underlying hypotheses

● Fairness-aware algorithms

● Remediation with post-processing techniques on output

● Documentation with model cards

Industrialization, monitoring, and maintenance

● Context monitoring
- Regulatory changes
- Legal changes
- Company-policy changes
- Usage appropriateness

● Model monitoring
- Data drift
- Model metrics
- Bias metrics in outcomes

● Model maintenance
- Database of metrics and trend tracking
- Updates of documentation

● Execute development checks and controls to manage the risk of bias

● Monitor model for bias metrics

sprint-based development approaches, relying more on developer testing and input from analytics teams, so they can focus on review rather than taking responsibility for the majority of testing and quality control. Additionally, they will need to reduce one-off "static" exercises and build in the capability to monitor AI on a dynamic, ongoing basis and support iterative development processes.

But monitoring AI risk cannot fall solely on risk managers. Different teams affected by analytics risk need to coordinate oversight to ensure end-to-end coverage without overlap, support agile ways of working, and reduce the time from analytics concept to value (Exhibit 3).

AI risk management requires that each team expand its skills and capabilities, so that skill sets

in different functions overlap more than they do in historical siloed approaches. Someone with a core skill—in this case, risk management, compliance, vendor risk—needs enough analytics know-how to engage with the data scientists. Similarly, data scientists need to understand the risks in analytics, so they are aware of these risks as they do their work.

In practice, analytics teams need to manage model risk and understand the impact of these models on business results, even as the teams adapt to an influx of talent from less traditional modeling backgrounds, who may not have a grounding in existing model-management techniques. Meanwhile, risk managers need to build expertise—through either training or hiring—in data concepts, methodologies, and AI and machine-learning risks, to ensure they can coordinate and interact with analytics teams (Exhibit 4).

This integration and coordination between analytics teams and risk managers across the model life cycle requires a shared technology platform that includes the following elements:

— an agreed-upon documentation standard that satisfies the needs of all stakeholders (including developers, risk, compliance, and validation)

— a single workflow tool to coordinate and document the entire life cycle from initial concept through iterative development stages, releases into production, and ultimately model retirement

— access to the same data, development environment, and technology stack to streamline testing and review

— tools to support automated and frequent (even real-time) AI model monitoring, including, most critically, when in production

— a consistent and comprehensive set of explainability tools to interpret the behavior of all AI technologies, especially for technologies that are inherently opaque

Exhibit 3

The responsibilities for enabling safe and ethical innovation with artificial intelligence span multiple parts of the organization.

Business		
Front line Confirm soundness of predictive drivers, modeling approach, and results based on business experience	**Operations** Validate insights against business experience; ensure appropriate use-case calibration (eg, clarity on modeling objectives)	**Business-unit control** Ensure tests required by second-line-of-defense functions are performed, including ongoing monitoring and testing of models in use

Analytics	Data	Technology
Data scientists, developers Develop best-in-class models in line with second-line-of-defense standards; provide transparency into model behavior (ie, explainability)	**Data engineers/strategists** Maintain data quality; ensure applicability of new features (ie, feature engineering) to modeling objectives	**IT (software and hardware)** Mitigate implementation risks by ensuring adequacy of production environment (eg, scalability, preventing data leakage)

Risk and control functions		
Model risk management Develop standards providing guard-rails on AI/ML[1] model development; assess AI/ML model risk	**Compliance and legal** Provide guidance on compliance risks (eg, prevent bias arising from use of certain restricted customer characteristics)	**Cloud risk, vendor risk, etc** Provide guidance on mitigating key nonfinancial risks (eg, reputational damage, third-party) linked to AI/ML models

[1] Artificial intelligence/machine learning.

Getting started

The practical challenges of altering an organization's ingrained policies and procedures are often formidable. But whether or not an established risk function already exists, leaders can take these basic steps to begin putting into practice derisking AI by design:

— *Articulate the company's ethical principles and vision.* Senior executives should create a top-down view of how the company will use data, analytics, and AI. This should include a clear statement of the value these tools bring to the organization, recognition of the associated risks, and clear guidelines and boundaries that can form the basis for more detailed risk-management requirements further down in the organization (see sidebar "Building risk management into AI design requires a coordinated approach").

— *Create the conceptual design.* Build on the overarching principles to establish the basic framework for AI risk management. Ensure this covers the full model-development life cycle

outlined earlier: ideation, data sourcing, model building and evaluation, industrialization, and monitoring. Controls should be in place at each stage of the life cycle, so engage early with analytics teams to ensure that the design can be integrated into their existing development approach.

— *Establish governance and key roles.* Identify key people in analytics teams and related risk-management roles, clarify their roles within the risk-management framework, and define their mandate and responsibilities in relation to AI controls. Provide risk managers with training and guidance that ensure they develop knowledge beyond their previous experience with traditional analytics, so they are equipped to ask new questions about what could go wrong with today's advanced AI models.

— *Adopt an agile engagement model.* Bring together analytics teams and risk managers to understand their mutual responsibilities and working practices, allowing them to solve

Exhibit 4

Both analytics and risk professionals will need to complement their traditional skill sets with sufficient knowledge of the others' function.

	Data and analytics professionals	Risk and control officers
Core competencies	• Math, statistics, machine learning, deep learning • Building algorithmic models • Collecting, cleansing, structuring data • Creating data visualizations and dashboards • Explaining model drivers	• Knowledge of applicable regulations • Identification and analysis of risks • Credible and independent review of business activities
New complementary skills	• Awareness of analytics risks, including bias, fairness, and instability • Understanding of where risks can arise in analytics-development life cycle • Ability to use risk-management tools as part of analytics-development process (eg, explainability and bias testing, model-performance-monitoring dashboards) • Understanding of risk-control team's role and responsibilities and ability to engage with them effectively	• General understanding of analytics techniques and their implications, including performance vs interpretability trade-offs • Awareness of best practices in testing for bias, fairness, and stability and ability to understand results from risk-management tools such as explainability reports • Understanding of data/feature-selection practices and their effect on risks (eg, bias) • Understanding of analytics teams' roles and responsibilities and ability to engage with data and analytics professionals

Building risk management into AI design requires a coordinated approach

While AI applications can be developed in a decentralized fashion across an organization, managing AI risk should be coordinated more centrally in order to be effective. A major North American bank learned this lesson when it set out to create a new set of AI risk-management capabilities to complement its existing risk frameworks. Intitially, multiple groups began their own AI risk-management efforts. This fragmentation created a host of challenges around key risk processes, including tracking and assessing the risks of AI embedded in vendor technologies, triaging and risk oversight of AI tools, building controls into AI model development involving multiple analytics groups, and operationalizing ethical principles on data and AI approved by the board. As a result, the bank struggled to demonstrate that all AI risks were managed through the development life cycle.

The bank alleviated these issues by establishing one multidisciplinary team to define a clear target state of AI risk management, build alignment across stakeholders, clarify AI governance requirements, and specify the engagement model and technical requirements conflicts and determine the most efficient way of interacting fluidly during the course of the development life cycle. Integrate reviews and approvals into agile or sprint-based development approaches, and push risk managers to rely on input from analytics teams, so they can focus on reviews rather than taking responsibility for the majority of testing and quality control.

— *Access transparency tools*. Adopt essential tools for gaining explainability and interpretability. Train teams to use these tools to identify the drivers of model results and to understand the outputs they need in order to make use of the results. Analytics teams, risk managers, and partners outside the company should have access to these same tools in order to work together effectively.

— *Develop the right capabilities*. Build an understanding of AI risks throughout the organization. Awareness campaigns and basic training can build institutional knowledge of new model types. Teams with regular review responsibilities (risk, legal, and compliance) will need to become adept "translators," capable of understanding and interpreting analytics use cases and approaches. Critical teams will need to build and hire in-depth technical capabilities to ensure risks are fully understood and appropriately managed.

—————

AI is changing the rules of engagement across industries. The possibilities and promise are exciting, but executive teams are only beginning to grasp the scope of the new risks involved. Existing approaches to model-risk-management functions may not be ready to support deployment of these new techniques at the scale and pace expected by business leaders. Derisking AI by design will give companies the oversight they need to run AI ethically, legally, and profitably.

Juan Aristi Baquero and **Roger Burkhardt** are partners in McKinsey's New York office, **Arvind Govindarajan** is a partner in the Boston office, and **Thomas Wallace** is a partner in the London office.

The next S-curve in model risk management

How banks can drive transformations of the model life cycle in a highly uncertain business landscape.

by Frank Gerhard, Pedro J. Silva, Maribel Tejada, and Thomas Wallace

The economic effects of the COVID-19 pandemic have thrown into stark relief the significant challenges facing banks' financial models. Some models have failed in the crisis, an outcome that has drawn attention to models generally. The causes of the failure include not only COVID-19 effects but also regulatory requirements and models' increasing time to market. Institutions are realizing that even models which have not been significantly affected by these stresses are wanting in other ways.

The present crisis is creating a moment in which banks can rethink the entire model landscape and model life cycle. The next S-curve for model risk management (MRM) includes new model strategies to address new regulation and changing business needs. Models must become more accurate, so banks need to recalibrate them more frequently and develop new models more rapidly. A sustainable operating model is needed, since monitoring, validation, and maintenance activities must support the redevelopment and adjustment of models. The solution will have to be designed to manage models effectively over the long term.

The new strategy will require a top-down approach to model development because the institution has to be able to identify those changes that can be made through overlays and those that need recalibration and redevelopment. Once the model-development wave is complete, model validation, monitoring, and maintenance can be "industrialized"—conducted in a methodical, automated manner, sufficient for managing an increasing number of models. High standards are needed for both model risk management and regulatory requirements.

For the most part, quick solutions become unsustainable in the long run, for several reasons: experience has shown that banks cannot rely on expert judgment alone; many solutions address temporary conditions (such as the effects of government intervention or changes in customer behavior); budgets are strained by the resources needed to monitor, recalibrate, and develop or redevelop the ever-increasing model inventory; and finally, the short time periods in which the work must be done demand a more industrialized and comprehensive approach.

An optimized model landscape

As the economy begins to revive, organizations will likely be under budgetary stress. Differing priorities will compete for fewer resources. Leaders will have to make smart choices to realize model strategies, investing efficiently and sustainably. Banks will likely seek to upgrade their modeling capabilities, rationalize the model landscape, and streamline the processes for developing, monitoring, maintaining, and validating models.

Banks will have to manage trade-offs among expected impact on capital, regulatory provisions, costs to remediate issues, and capacity constraints. The objectives will be best served by avoiding unnecessary complexity. As part of the effort to rationalize the model landscape, better models will be built—those that ensure regulatory compliance but are also more accurate and best serve the business.

Models will also be recalibrated and run more frequently. Some will be replaced by next-generation models, an effort that will require investment in technology and data initiatives to serve the business. The development cycle for new models will be shortened, so that they can be deployed faster. To manage increasing costs, banks will have to ensure that model development, monitoring, and validation are performed efficiently. Banks also must demonstrate to regulators that their model-management frameworks are robust and that the impact of the crisis on models is being capably addressed.

The role of the model-risk-management function

Proactive MRM activities, aligned with both business needs and risk-management objectives, must be in place to prevent overgrowth of the model inventory. To ensure that the inventory is rational and effective, banks need to manage the model landscape as a whole. They also need to ensure that model quality is high. Gaining transparency to direct such efforts can involve deploying model workflow and inventory tools, consistently applied model-risk-rating approaches, and regular monitoring of model performance and use.

The MRM function can support the bank by fully optimizing the portfolio of models. This support goes beyond performing validation work and ensuring consistency across modeling and monitoring practices. Model development is also in need of optimization and consolidation, since development is usually fragmented across different business units.

Hundreds of models now need to be adjusted, developed, and recalibrated. There is a lesson in this—the effective and efficient development of new models must result in models that are easy and inexpensive to maintain in the future. In taking stock of existing models, banks should seek to improve the quality of the best models while decommissioning poor-quality, ineffective, and outdated models.

Sharing responsibility for model management

Model management can no longer be primarily or even mainly the responsibility of the MRM function, a fact that the COVID-19 crisis has underscored. The responsibility must be with the business stakeholders—those who use the models and extensively rely on their outcomes. MRM has to be approached as the collaborative work of all three lines of defense. The second line—the MRM/validation function and the risk function—should enable a clear program for building MRM capabilities among all business stakeholders and model owners. Only through real collaboration can banks ensure that effective controls are designed and models are properly monitored.

As responsibility for MRM is shared, so are its benefits, and certain activities will undergo changes and adaptations.

— *Validation.* The MRM function and risk function will still focus on validation practices, ensuring that models are of good quality and model risk is capably managed. But the business stakeholders and model developers are the ultimate users of models. As such, they must be responsible for ensuring that development

costs are justified, programs are run efficiently, and models are well monitored and maintained. Such active collaboration eliminates work silos, allowing the use of common elements across the model life cycle. This minimizes friction and boosts efficiency.

— *Capability building.* The effort to build the model strategy must be supported by a thorough capability-building program. All model users and owners and the leaders of affected functions and business units need to be trained in the new approach to MRM, so that they all understand their risk-management responsibilities. Given the current environment, defined by new and complex technology and accelerating automation, an aware and responsive workforce is indispensable to strong model governance.

— *Agenda setting.* The MRM function should work closely with the first line to set the agenda, identifying the models that are most important to the business and operations and defining the priority model activities. That requires a forward-looking view into how pandemic-related factors have affected or will affect models. Those that are adversely affected will need recalibration or redevelopment.

— *Active management of the model landscape.* Managing the model landscape will be a joint effort between first- and second-line teams. Model-risk managers will guide the efficient allocation of model-risk appetite by setting definitions for where models should be used, thresholds for materiality and complexity, and precision requirements based on use cases. At the same time, model developers will be given incentives to consolidate similar functions, reduce model count and complexity, and promote modularization and reuse of code.

— *An agile operating model.* The function also needs to determine the best operating approach to manage delays in development and validation plans that were made before the pandemic. This would include a flexible project-management approach, with joint calendars

The big lesson for the new MRM framework is that it must establish standards and standardize processes.

for both development and validation. New organizational structures should be established to ensure cross-functional teams, career- and knowledge-development opportunities, rotation programs, and an effective location strategy. A multidisciplinary team, with representatives from business, development, technology, and validation, can be used to break down siloes and meet the needs of various stakeholders.

— *Ownership.* Most organizations that have been successful in optimizing their model landscape have established clear model ownership and defined roles for those model owners. This ensures that the model-life-cycle process is integrated across the organization, with stakeholders interacting in a coordinated manner. Where model ownership has not been established, strong focus should be given to onboarding programs to ensure the business understands its model risk management responsibilities.

Streamlining and automation
This perfect storm of model-inventory revisions and development presents organizations with a unique opportunity to act strategically. The requirement is clear: institutions need to streamline the entire model life cycle, including ideation, development, implementation, validation, and monitoring. The objectives are to avoid future bottlenecks, support business continuity, and improve institutional performance, while minimizing risk and cost.

Crucially, banks must develop a model strategy for the coming years that meets these demands in a cost-efficient manner.

As model-life-cycle processes are reimagined, the ultimate goal is to bring about strategic change. But flexibility is built into the process, so progressive efficiency gains, such as technical solutions, can be made to capture near-term benefits until more fundamental strategic programs are completed. For automation, processes need to be standardized. This is accomplished through a complete review of process maps, applying lean fundamentals.

MRM should become the agency driving model efficiency. Modeling teams and business stakeholders will need to work alongside risk, including the MRM and model-validation teams. Together they can fully utilize MRM frameworks to manage the increasing number of models efficiently—including newly developed and redeveloped models as well as the monitoring and validation conforming to the increasing level of standardization and automation. The big lesson for the new MRM framework is that it must establish standards and standardize processes. This work is essential for streamlining and automation.

The increasing number of models poses a significant challenge. These models must be validated within budgets but without eroding quality. Banks should therefore ensure a high-quality, independent model review that is also cost-efficient.

Finding efficiencies in the model life cycle

Banks can find efficiency opportunities throughout the model life cycle (exhibit). To do this, they can assess and review their current model process maps, rethinking the processes themselves.

Processes can be redesigned and automated using standard digitization programs, generating efficiencies in a range of areas:

— *Model testing.* Some firms have been able to reduce the time it takes to perform testing during development by as much as 30 percent by applying standard model principles, a standard library of testing codes, automatic testing, and other techniques.

— *Model validation.* Banks have reduced the time it takes to validate and produce the associated report to comply with regulations and ensure business continuity, in some cases by as much as 65 percent. The key drivers of the savings are standardized tiering, automated test selection and testing by model type, and automated population of documents and reports.

Exhibit

Significant savings result from optimizing the model life cycle, especially in validation processes.

Opportunities for automation

- ■ Automating model activities
- ■ Automating documentation
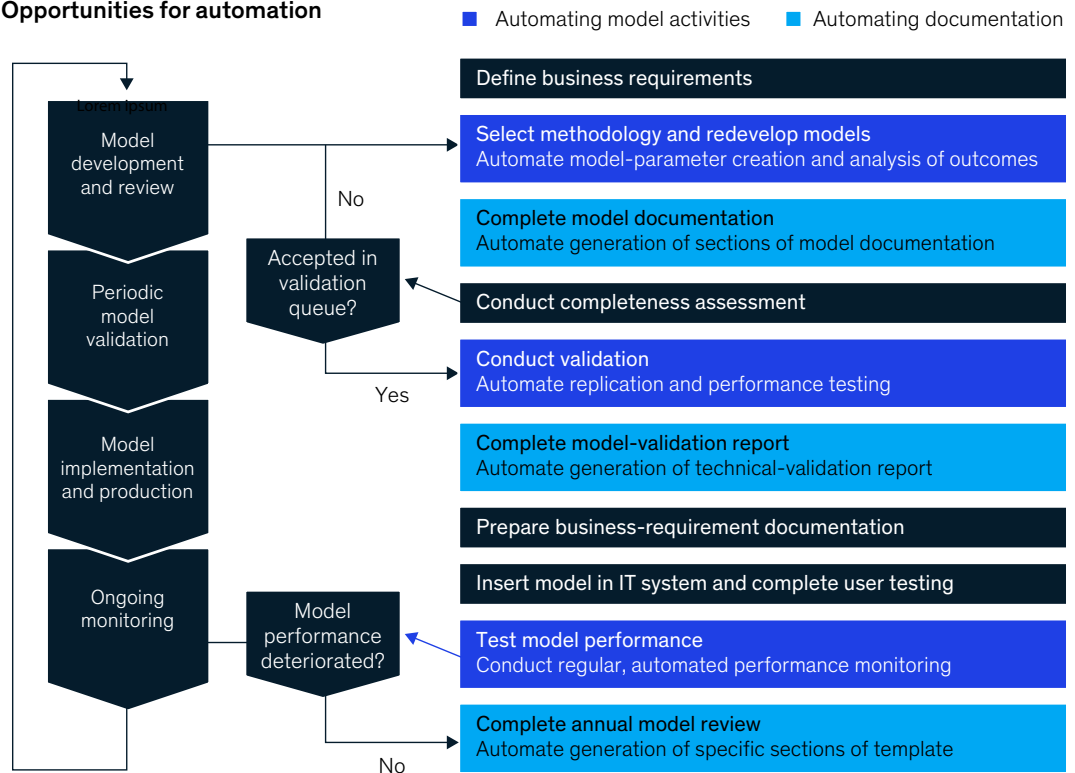
— *Model monitoring.* A predefined monitoring pack built around a library of key performance indicators can reduce the time required to execute ongoing monitoring activities by as much as 35 percent.

— *Data-quality standardization and automation.* Banks can reduce the workload for data-quality testing for models by 20 to 40 percent. For both models in the pipeline and models being monitored, testing can use standard libraries. With machine-learning techniques and automation, banks can scan terabytes of data without human intervention. With only gray areas left to be addressed, the savings in time and effort are significant.

The streamlining and automation of model-related processes—from model development to validation, monitoring, and maintenance—is thus an MRM project integrated across the lines of defense.

Proactive MRM owned by all lines of defense is needed now—not only to meet new regulatory expectations but also to strengthen institutional resiliency in this crisis and the next. It is also needed to maintain and improve model efficiency. A redefined MRM framework will include all stakeholders and cover the entire model life cycle. The model inventory will be reshaped to better support the needs of the business. Standardized processes will provide the foundation for the use of advanced analytical and digital tools and progressive automation.

Banks have to do all this while maintaining high standards for MRM and regulatory compliance. A lot of ground must be covered in the coming months, and given the depth of the present crisis, banks should get started right away.

Frank Gerhard is an associate partner in McKinsey's Stuttgart office; **Pedro J. Silva** is a consultant in the London office, where **Thomas Wallace** is a partner; **Maribel Tejada** is a senior expert in the Paris office.

Applying machine learning in capital markets: Pricing, valuation adjustments, and market risk

By enhancing crisis-challenged financial models with machine-learning techniques such as neural networks, banks can emerge stronger from the present crisis.

This article was a collaborative effort by Juan Aristi Baquero, Akos Gyarmati, Marie-Paule Laurent, Pedro J Silva, and Torsten Wegner, representing views from McKinsey's Risk Practice.
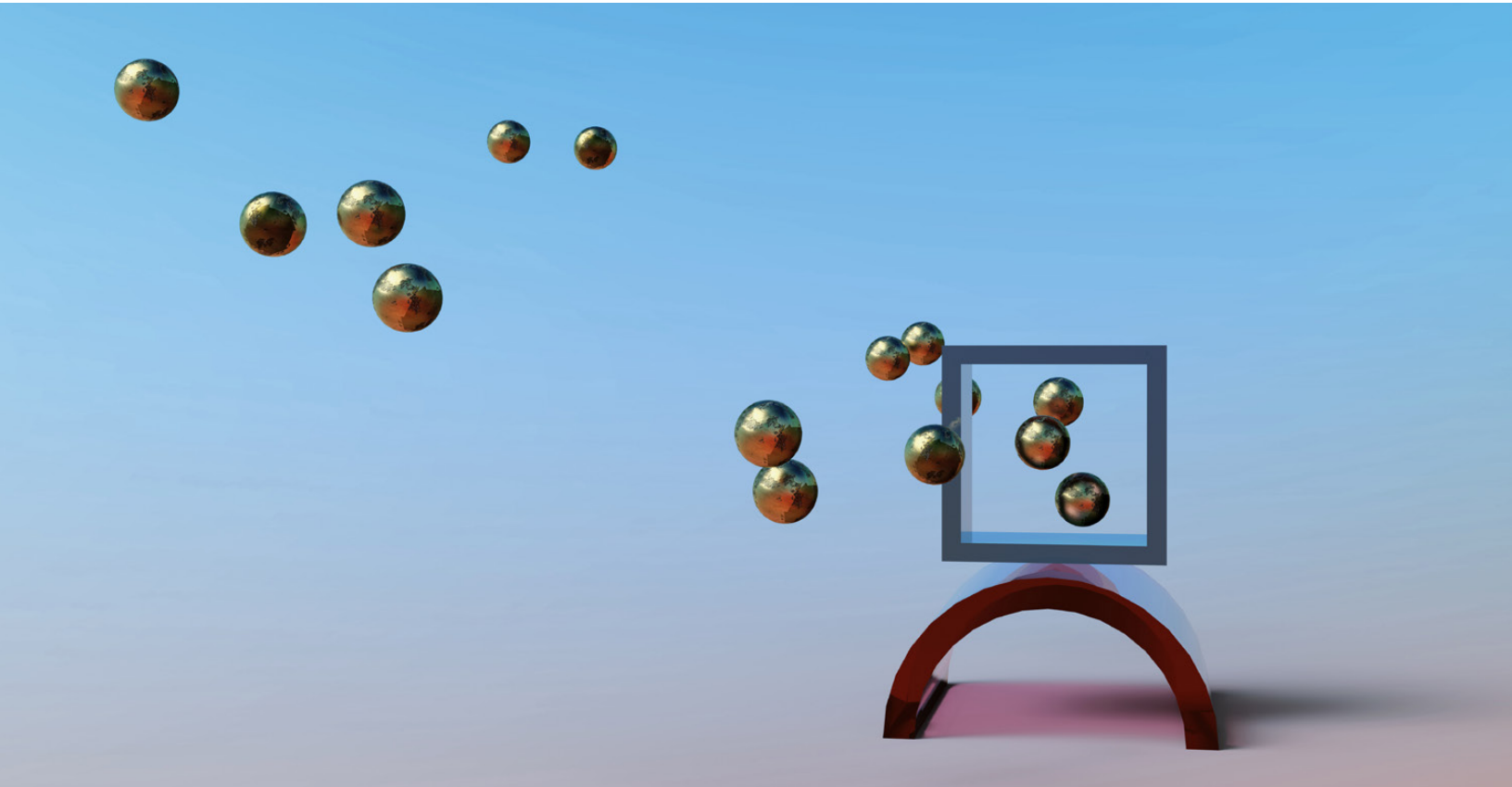
When the COVID-19 outbreak became a global pandemic, the volatility of financial markets hit its highest level in more than a decade, amid pervasive uncertainty over the long-term economic impact. Calm has returned to markets in recent months, but volatility continues to trend above its long-term average. Amid persistent uncertainty, financial institutions are seeking to develop more advanced quantitative capabilities to support faster and more accurate decision making.

As financial markets gyrated in recent months, banks faced particular problems calculating value at risk (VAR) across asset classes. Many institutions experienced elevated levels of VAR back-testing exceptions, leading to higher regulatory-capital multipliers. Increases of as much as 30 percent were reported, prompting regulators to apply exemptions in some cases. There were also challenges with valuation adjustments, as derivatives faced snowballing collateral calls and increasing funding costs. Where credit-value-adjustment (CVA) risks were excluded from market risk models, CVA hedges sat "naked" on the balance sheet, leading to significant uplifts in exposures, and therefore in risk-weighted assets (RWAs). One large US dealer was hit with a loss of $950 million stemming from a valuation adjustment (XVA) in the first quarter of 2020. Elsewhere, rising gap risk in illiquid securities catalyzed painful fair-value losses—as high as $200 million in the case of a major Europe-based bank.

In an unpredictable environment, financial modelers were required to come up with solutions but were often stymied by inadequate models or the need for huge computational power that was not always available. Given the speed of response required, models in some cases were rendered unusable. The inevitable result was an increase in risk exposures and opacity from valuations, sometimes in absolute value and other times relating to the reason for specific model outputs.

An imperative to act

Since forecasting institutions expect the global economy to have contracted by about 5 percent in 2020, banks should aim to optimize their trading books and risk positions. This ambition requires more accurate and timely valuations. With those priorities in mind, more advanced models and

sufficient computational power are imperatives. Indeed, "speed" is of the essence.

In response, some leading institutions have started to incorporate advanced techniques into their quantitative armories. In pricing, an area that has experienced a spike in recent activity, several banks are applying machine learning (ML) to enhance traditional models—for example, by calibrating parameters more efficiently. In particular, banks have used neural networks, a type of ML focused on nonlinear and complex data relationships. Advanced machine-learning techniques can do the following:

— speed up calculations, reducing operational costs and allowing real-time risk management of complex products

— animate more complex models that may currently be unusable in practice, and unlock more accurate valuations

— generate high volumes of synthetic but market-consistent data, helping, for example, to offset the disruptive impact of COVID-19-related market moves

One way to implement neural networks is to apply them to pricing, where they can "learn" how to price vanilla calibration instruments under a given (possibly complex) model, and then act as pricing engines for new model calibration. The approach obviates one of the most significant challenges associated with ML, which is parameter interpretability. In this case, there is no interpretability issue because the network uses the original model's parameters. This means that there is no ML "black box," and the key calibrated parameters can be interpreted in the original model's context.

Neural networks can also support future-exposure modeling for valuation adjustments (Exhibit 1).

The network can be trained on established samples, such as those relating to the evolution of risk factors and corresponding cash flows for the products being modeled. The additional efficiency provided by the network makes for improved accuracy and faster processing (Exhibit 2). That saves banks from using time-consuming nested Monte Carlo approaches and less accurate analytical approximations or "least squares"—style regressions.

There are equally promising applications in real-time portfolio valuation, risk assessment, and margining.

Three steps to deepening ML engagement

Machine learning offers significant enhancement for conventional quantitative approaches, through its ability to interpolate across large data sets and streamline model calibration. Banks would benefit by deepening their ML engagement and testing new use cases. The uncertain macroeconomic environment should act as a catalyzer to this process and trigger banks to act. The emphasis initially should be on discrete applications rather than wholesale transformation. Use cases can later be extended and expanded across the business.

There is no blueprint for model development, and individual businesses must solve for their own pressing needs. However, the experience of early movers suggests that reliable options for establishing a track record encompass three key steps:

1. **Identify quick wins**
    While ML can help to improve numerous calculation processes, it is more useful in some contexts than others. The task for decision makers is to identify potentially winning applications that will help create a positive track record. Likely candidates are models that consume large amounts of time or computing power. ML can both speed the work of these models and lay the groundwork for scaling their application. Among the applications that have begun to attract

Exhibit 1

Neural networks can support future-exposure modeling.

Artificial intelligence	Machine learning	Deep learning and neural networks
Intelligence exhibited by machines, mimicking cognitive functions that humans associate with other human minds; cognitive functions include all aspects of perceiving, reasoning, learning, and problem solving	Major approach to realizing artificial intelligence by learning from and making data-driven predictions on data and experiences; categories include supervised learning, unsupervised learning, and reinforcement learning	Branch of machine learning where systems of algorithms, based on simulating connected neural units, mimic how neurons interact in brain; uses large-scale neural networks that can contain millions of simulated "neurons" structured in layers; successful in many different applications

Exhibit 2

Neural networks can enable fast and accurate exposure calculations.

Problem: Future-exposure modeling is main bottleneck in current valuation-adjustment models; portfolio-valuation and risk calculations must be fast, accurate, and consistent with FO[1]-pricing models, but typical approaches fail to meet all 3 goals at same time

	Nested Monte Carlo method	Analytical approximations/ LSM[2]-style regressions
Fast		●
Accurate	●	
Consistent with FO-pricing models	●	

Solution: Neural-network approach proposed to achieve all 3 goals at same time:
1. Perform portfolio-valuation and risk calculations via neural networks
2. Train neural networks using simulated risk-factor paths and pathwise-evaluated cash flows—no extra cost to generate training sample
3. Use differential regularization to optimize accuracy for both pricing and risk while achieving fast training

[1]Front office.
[2]Least-squares method.
 Source: Danske Bank SuperFly Analytics

attention are valuations of level-3 assets, XVA calculations, profit-and-loss attributions ("P&L explains"), adaptations for Fundamental Review of the Trading Book (FRTB), and stress testing.

A "discovery phase" of an ML transformation could proceed as follows:

- Identify concrete cases based on accepted criteria, such as the complexity of models, exposure in books, or computational bottlenecks. For example, complex, hard-to-value derivatives such as structured callable trades could be good targets.

- Size the estimated impact and align various stakeholder groups.

- Create an action plan, including the effort and time required for implementing the identified use cases.

2. **Build capabilities to embrace a culture enabled by machine learning**
   Machine learning has the potential to create significant efficiencies in a range of activities. However, financial institutions cannot maximize the ML opportunity without acquiring the necessary capabilities to build, maintain, and apply ML-enabled models. They must also take steps to help employees understand and exploit potential benefits so that ML is embedded in the culture of the organization.

   This could be achieved by following through with the earlier approach and establishing and executing pilot programs to implement prioritized use cases. During these pilots, the following practices can be applied:

   - build capabilities via learning on the job

   - understand typical challenges and pitfalls and how to solve them

- acquire continuous feedback on how new applications can fit into the wider organization

3. **Roll out at scale**
   Over time, sprints, prototypes, and quick wins will have accumulated sufficiently to create the conditions for a more sustained machine-learning rollout. Assuming a critical mass of use cases, quant teams should move to integrate ML into a wider range of activities. They may begin with the front office and extend into risk, finance, compliance, and research.

   A plan to scale up the machine-learning program could include the following activities:

   - strategic execution of identified priority use cases

   - continuous exploration of additional areas where ML could be relevant, such as anti–money laundering, know your customer, or cybersecurity

   - updating risk-management practices, such as model governance and risk assessment, to monitor and control new risks introduced by ML

   ⸺

Machine learning has the potential to enable institutions to do more in capital markets, to move faster, and to move with greater accuracy. The working conditions created during the pandemic have accelerated reliance on digital access and the data-driven environment. Given these factors, machine learning could easily begin to migrate into mainstream operations. With this in mind, firms must not delay in building their capabilities. They must experiment, develop use cases, and move quickly to the production of machine-learning-enhanced models. Those that create and execute a sensible implementation strategy are likely to emerge from the current crisis stronger, more assured of risk exposures, and better prepared for what lies ahead.

Juan Aristi Baquero is a partner in McKinsey's New York office, **Akos Gyarmati** and **Pedro J Silva** are consultants in the London office, **Marie-Paule Laurent** is a partner in the Brussels office, and **Torsten Wegner** is an associate partner in the Berlin office.

Derisking digital and analytics transformations

While the benefits of digitization and advanced analytics are well documented, the risk challenges often remain hidden.

by Jim Boehm and Joy Smith
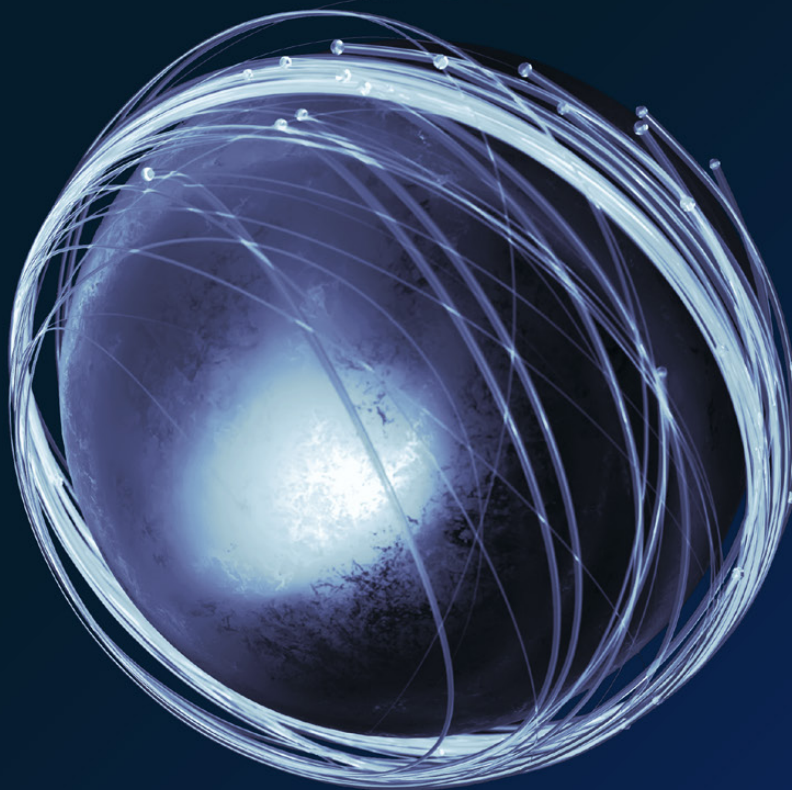
A bank was in the midst of a digital transformation, and the early stages were going well. It had successfully transformed its development teams into agile squads, and leaders were thrilled with the resulting speed and productivity gains. But within weeks, leadership discovered that the software developers had been taking a process shortcut that left customer usernames and passwords vulnerable to being hacked. The transformation team fixed the issue, but then the bank experienced another kind of hack, which compromised the security of customer data. Some applications had been operating for weeks before errors were detected because no monitors were in place to identify security issues before deployment. This meant the bank did not know who might have had access to the sensitive customer data or how far and wide the data might have leaked. The problem was severe enough that it put the entire transformation at risk. The CEO threatened to end the initiative and return the teams to waterfall development if they couldn't improve application-development security.

This bank's experience is not rare. Companies in all industries are launching digital and analytics transformations to digitize services and processes, increase efficiency via agile and automation, improve customer engagement, and capitalize on new analytical tools. Yet most of these transformations are undertaken without any formal way to capture and manage the associated risks. Many projects have minimal controls designed into the new processes, underdeveloped change plans (or none at all), and often scant design input from security, privacy, and risk and legal teams. As a result, companies are creating hidden nonfinancial risks in cybersecurity, technical debt, advanced analytics, and operational resilience, among other areas. The COVID-19 pandemic and the measures employed to control it have only exacerbated the problem, forcing organizations to innovate on the fly to meet work-from-home and other digital requirements.

McKinsey recently surveyed 100 digital and analytics transformation leaders from companies across industries and around the globe to better understand the scope of the issue.[1] While the benefits of digitization and advanced analytics are well documented, the risk challenges often remain hidden. From our survey and subsequent interviews, several key findings emerged:

— Digital and analytics transformations are widely undertaken now by organizations in all sectors.

— Risk management has not kept pace with the proliferation of digital and analytics transformations—a gap is opening that can only be closed by risk innovation at scale.

— The COVID-19 pandemic environment has exacerbated the disparity between risk-management demands and existing capabilities.

— Most companies are unsure of how to manage digital risks; leading organizations have, however, defined organizational accountabilities and established a range of effective practices and tools.

McKinsey has developed approaches and capabilities to address the challenges implicit in these findings. They include a new four-step framework to define, operationalize, embed, and reinforce solutions; supporting methodologies to accelerate frontline teams' risk-management effectiveness and efficiency; and a cloud-based diagnostic assessment and tracking tool. This tool is designed to help companies better identify, assess, mitigate, and measure the nonfinancial risks generated and exacerbated by digital and analytics transformations at both the enterprise and product level.

Fortunately, to take advantage of these approaches, most companies will not have to start from scratch. They can apply their existing enterprise-risk-management (ERM) infrastructures. This is typically used for financial and regulatory risks but can be modified to be more agile and adaptable to meet the

---

[1] The McKinsey Global Survey on digital and analytics transformations in risk management, 2020. The 100 participants were a representative sample of companies from all geographic regions; nearly 89 percent have annual revenue of at least $1 billion. The companies spend, on average, 12 percent of their IT budgets on digital and analytics transformations.

risk-management demands of digital and analytics transformations.

The advantages of digital and analytics transformations are real but so are the risks (Exhibit 1).

By understanding the insights from our research and taking the approach outlined here, companies can achieve the value of digital and analytics transformations while also safeguarding their organizations and customers. Ultimately, companies can inspire more productive relationships among groups and foster a sustainable competitive advantage for the company by preserving the impact of their transformation activities for the long term.

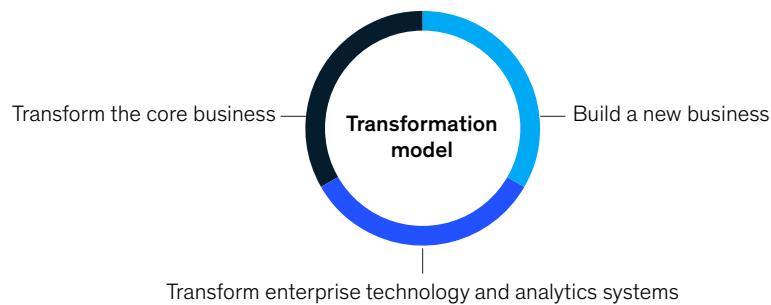## A broad set of new (and expensive) risks

Most companies appear to do little about the nonfinancial risks generated and exacerbated by digital and analytics transformations. The scope of these risks is broad. Digital and analytics transformations are often deployed across organizations, involving many departments and third parties. Soft factors such as skills, mindsets, and ways of working, as well as hard factors such as technology, infrastructure, and data flow are all being changed at once during such a transformation.

Some traditional risks are more common to most projects—including those arising from budget and schedule overruns, talent (employees and

Exhibit 1

Digital and analytics transformations use machine intelligence, automation, and agile approaches to improve products and operations.

Approach to digital and analytics transformations

Transform the core business — **Transformation model** — Build a new business

Transform enterprise technology and analytics systems

Transformation domains

- Multichannel customer experience: redesign and digitize top customer journeys end to end

- Digital marketing and pricing: revenue management, promotions-dynamic B2B pricing, cross-selling and upselling

- Sales digitization: digital sales, remote-selling effectiveness

- New digital propositions: create new revenue streams by building digital propositions, using next-generation artificial-intelligence (AI) technologies to achieve cost savings

- Supply chain and procurement: digitally redesign and manage operations to improve safety, delivery, and costs

- Next-generation operations: drive step changes in efficiency through digitization, AI, advanced analytics, and agile lean approaches

- Digital architecture: set up digital architecture combining application programming interfaces (APIs), microservices, and containers

- Data transformation: unify data governance and architecture to enable next-generation analytics

- Core-system modernization: achieve through refactoring or platform replacement

- Cloud and DevOps: migrate applications to hybrid cloud and/or software as a service (SaaS) and implement software development and IT operations (DevOps)

- Digital and analytics talent and capabilities: acquire new talent and build capabilities at scale

third parties, including contractors, suppliers, and partners), IT performance, and compliance and regulatory issues. Yet digital and analytics transformations also introduce new cyberrisks, data risks, and risks from artificial-intelligence (AI) applications. Digital and analytics initiatives require more detailed data to be collected from a wider range of sources. These data are then used in different parts of the organization to generate insights. The moving data create inherent risks in data availability, location, access, and privacy. Sources of risk to operational resilience include new IT services and migration to the cloud. Predictive analytical models could be biased or deviate from the original focus of the initiative exposing an organization to legal liability or reputational risk. If not handled appropriately, such risks can lead to expensive mistakes, regulatory penalties, and consumer backlash.

The business disruptions caused by the COVID-19 crisis have compounded these additional risk layers. In a sense, the pandemic has set off the largest wave of digital and analytics transformations in history, compressing transformations that would have taken years into a few hectic months (or even weeks), often with little advance planning. Most organizations had some security policies and training in place before the pandemic struck. Few, however, had established detailed policies or training on how to safely set up a remote work space or think through other risks associated with the rapid acquisition and deployment of new tools.

One oil and gas company, for example, had to divide its virtual private network to expand bandwidth so that all employees could have access to the corporate network from their homes. This caused slowdowns in patching on employee laptops, which exposed the company to vulnerabilities commonly exploited by attackers.

A telecom company allowed its call-center staff to work from home, but it left specific policies up to team managers. The result was that 30 percent

of the staff was permitted to use unsecured personal devices to connect remotely, exposing the company to "bring your own device" attacks. Similarly, a bank found that employees were printing documents on their home printers, thus running corporate data through unsecured home routers, which are notoriously vulnerable to hackers. Another firm expressed concerns about employees having "smart home" listening devices that could record discussions during video calls in executives' home offices.

Artificial intelligence is also poised to redefine how businesses work and is already unleashing the power of data across a range of crucial functions.[2] But the compliance and reputational risks of AI pose a challenge to traditional risk-management functions.

The different concerns have arisen from the rapid changes in the way we work now. Current risk-management capabilities are falling short in addressing them, since the risks are new and growing exponentially. A new risk-management approach is needed.

A snapshot of digital and analytics transformation risk management

The results of the McKinsey Global Survey permitted a holistic view of the risks facing digital and analytics transformations and how well companies are managing them. Several salient points emerged from participants' transformation experiences.

Transformations are becoming commonplace across industries
Survey participants completed an average of six transformations in the past three years, with a range of objectives. More than 80 percent have implemented at least one end-to-end customer journey transformation, and 70 percent developed new digital propositions and ecosystems. Organizations are also changing their operating models to support the changes. Approximately 80 percent of companies intend to shift up to

[2] Juan Aristi Baquero, Roger Burkhardt, Arvind Govindarajan, and Thomas Wallace, "Derisking AI by design: How to build risk management into AI development," August 2020, McKinsey.com.

30 teams to work in agile ways in the next three years; the remaining 20 percent are shifting more than 30 teams to agile. This means, of course, that 100 percent of the 100 companies we surveyed intend to adopt or scale agile in the coming years. If done well, this is very good news for risk managers, given the inherent risk-mitigating structures and culture of early identification and remediation of defects inherent in well-implemented agile teams.

Risk management is not keeping pace
Companies' risk-management capabilities are lagging behind their transformation efforts. Organizations are transforming far more frequently than they are updating their risk frameworks to include new and exacerbated risks, and risk and legal professionals often operate in separate silos. Hence, the risk infrastructure is not keeping pace with the innovation. Overall, most respondents assess their risk-management maturity as average, but more than 75 percent have not conducted a formal, holistic risk assessment for half of their digital and analytics

transformations. Surprisingly, 14 percent have never formally assessed the risks for these initiatives—a big oversight for established companies.

**Companies are unsure of how to manage digital risks**
Unlike for financial risk management, in which companies tend to have established roles and processes (such as model risk management), companies in our survey do not have established roles, processes, or even consolidated understanding of digital and analytics risk drivers. The biggest challenge leaders say they face in managing digital and analytics risks is simply identifying them. The challenge gives credence to the maxim, "You cannot manage what you do not measure."

Notably, the results show virtually no relationship between IT spending levels and overall risk-management maturity for digital and analytics transformations. Simply put, the challenges are not solved by budget size (Exhibit 2).

Exhibit 2

Risk-management maturity in digital and analytics is not related to IT spending.

Average reported risk-management maturity by IT budget, scale 1–5[1]
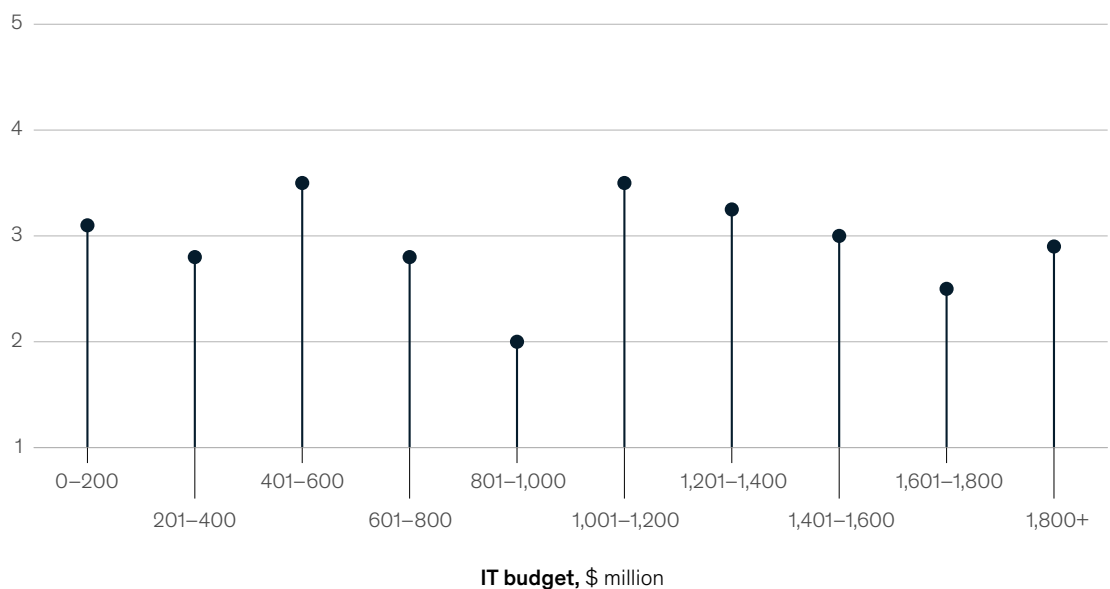
IT budget, $ million

[1]Question: At a company like yours, how mature are digital and analytics risk-management capabilities? Companies rated their risk-management capabilities from 1 to 5, with 5 representing the most advanced in effectiveness and efficiency.
Source: McKinsey Global Survey on Digital and Analytics Transformations in Risk Management, 2020

Roles and responsibilities are insufficiently clear

Survey participants little agree on where responsibility should lie for addressing digital and analytics transformation risks. For almost all respondents, the chief information or chief data officer leads digital and analytics transformation activities; participants do not align, however, on the lead for identifying and mitigating the associated risks. For more than 40 percent of respondents, the task falls to the digital and analytics transformation leads themselves. Unfortunately, these individuals often lack a detailed understanding of embedded risk factors and are given incentives to "get the transformation done." Even for those individuals who do focus on risk management, responsibilities are perceived as ancillary and less of a priority than project completion.

Leading companies apply a range of effective practices and tools to manage risks

Companies in our survey with the highest risk-management maturity are more comfortable with managing digital and analytics transformations. These companies are more likely to centralize or automate their risk-management functions, and they report using an array of practices and tools to identify and reduce the risks of their digital and analytics transformations (Exhibit 3).

Here are the most relevant approaches leaders cite:

— *Reengineering processes and retraining employees.* Respectively, 74 and 69 percent of respondents across industries and regions cite these practices, making them the most

Exhibit 3

Companies with higher risk-management maturity use several transformation practices and tools to manage risks.

Reported use of transformation practices by risk-management maturity level,[1] % of respondents
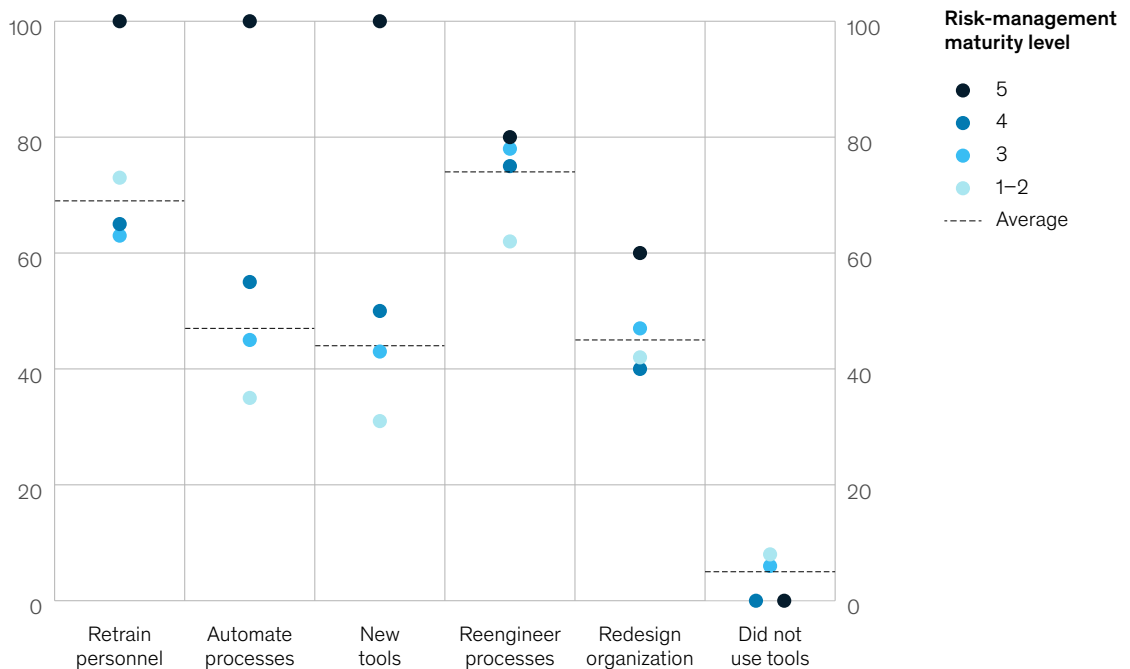
[1]Question: At a company like yours, how mature are digital and analytics risk-management capabilities? Companies rated their risk-management capabilities from 1 to 5, with 5 representing the most advanced in effectiveness and efficiency.
Question: What levers would a company like yours use to identify and reconcile risks associated with digital and analytic transformations?
Source: McKinsey Global Survey on Digital and Analytics Transformations in Risk Management, 2020

popular for managing digital and analytics transformation. These practices are especially important for agile ways of working. When implemented well, they can be critical to derisking technology using agile methodologies. The agile approach permits companies to automate, create new organizations, or deploy new tools with less effort, and has early identification and remediation of defects inherent in its culture.

— *Formal risk assessments.* Companies do not conduct these assessments as broadly as necessary; however, companies that do conduct them report an increase of 75 percent in their understanding of risks from digital and analytics transformations. Formal risk assessments also correlate to higher comfort levels in managing those risks (+47 percent), and greater risk-management maturity (+33 percent).

— *Automated feedback loops.* The risk-maturity scores of companies that have them are more than 30 percent above the average.

— *Centralization.* Companies with the highest risk-management scores are more likely to track digital and analytics risks in a single, centralized source, rather than several sources.

Pain points in managing digital and analytics transformation risks
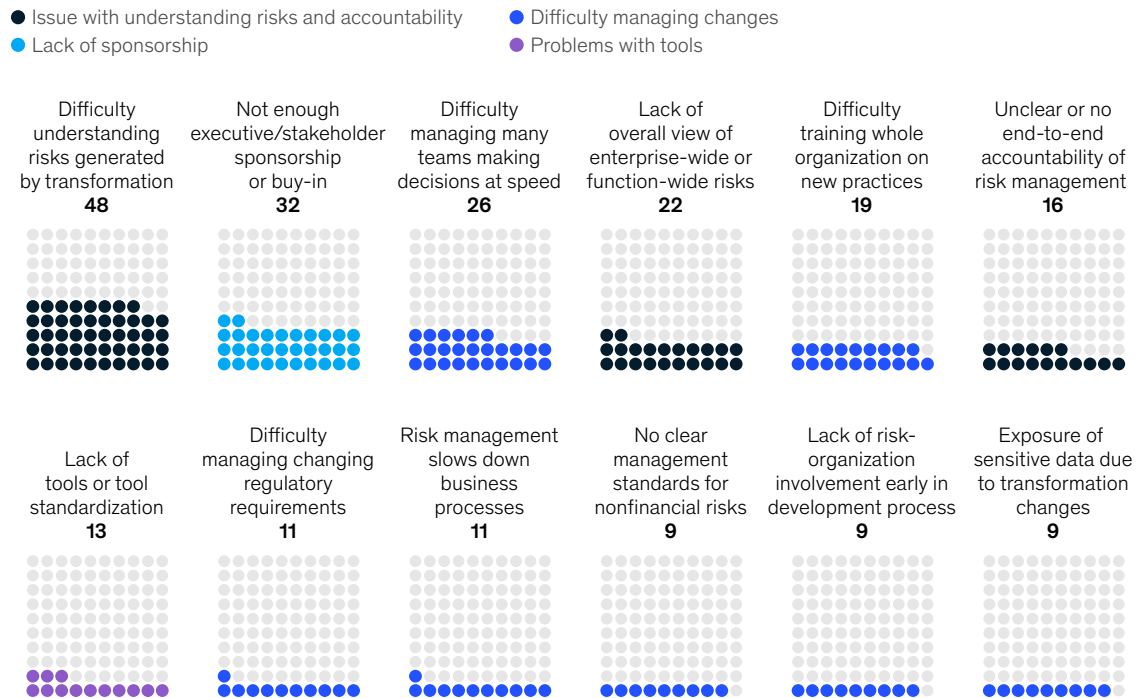Survey participants also describe their biggest pain points in identifying and mitigating risks.

Understanding risks
The top concern, which 48 percent of respondents cite, was simply understanding the risks associated with digital and analytics transformations (Exhibit 4). Many transformation leaders are essentially flying

Exhibit 4

The top risk-management pain point is in understanding the risks generated by a digital and analytics transformation.

Reported risk-management pain points,[1] % of respondents

● Issue with understanding risks and accountability   ● Difficulty managing changes
● Lack of sponsorship   ● Problems with tools

| Difficulty understanding risks generated by transformation **48** | Not enough executive/stakeholder sponsorship or buy-in **32** | Difficulty managing many teams making decisions at speed **26** | Lack of overall view of enterprise-wide or function-wide risks **22** | Difficulty training whole organization on new practices **19** | Unclear or no end-to-end accountability of risk management **16** |

| Lack of tools or tool standardization **13** | Difficulty managing changing regulatory requirements **11** | Risk management slows down business processes **11** | No clear management standards for nonfinancial risks **9** | Lack of risk-organization involvement early in development process **9** | Exposure of sensitive data due to transformation changes **9** |

[1]Question: In your most recent digital and agile projects, what were the top five risk-management pain points?
Source: McKinsey Global Survey on Digital and Analytics Transformations in Risk Management, 2020

blind: risk ownership is not clear, the complex and changing technology and regulatory environments are not well deciphered, and design and test plans do not consider risks early enough in the process. Unlike financial risks, nonfinancial risks are hard to benchmark, and there is no one standard to manage them.

Managing changes at speed

Digital and analytics transformations are often delivered rapidly through agile and other methodologies. If traditional risk-management practices are not also transformed along with the new ways of working, they can introduce delays that threaten ambitious timelines. In some cases, even complying with new policies can create problems due to unforeseen interdependencies. For example, a North American distributor launched an analytics transformation and, during the implementation phase, also established a new information security policy. Suddenly, all work on the transformation was subject to the new policy—which meant that data had to be logged daily, maintained in the cloud, and removed after 30 days. Because of these changes in data-handling processes, the transformation was delayed by four weeks, triggering a loss of more than $20 million—a financial risk directly connected to a new digital way of working. Risk management should be designed, implemented, and supported to keep pace with digital and analytics transformation teams and avoid these and other similar risks.

Accessing resources

Nearly one-third of respondents cite a lack of sponsorship or buy-in from executives or other stakeholders in prioritizing risk-identification and management activities. Generating short-term revenue is prioritized over managing embedded risks. The latter, of course, is critical to preserving long-term value. More than half of participants face resource limitations when improving risk management with needed talent and capacity. Companies also struggle in putting the right tools and processes in place. For example, some organizations still manage digital and analytics transformation risks manually using an array of spreadsheets. Even those that apply more advanced tools do not do so consistently across organizational boundaries.

Overcoming operational limitations

In digital and analytics transformations, the whole organization must be trained to work in new ways (such as the agile approach) and be vigilant about mitigating new risks. One common goal of digital and analytics transformations is to better serve end users, who are often the weakest link in a risk-management chain. Low risk-awareness can expose the enterprise to significant risks associated with the new digital and analytics tools and processes. Risks may even be generated by the front line through user errors, where, for example, cloud buckets have been misconfigured or access rights have been wrongly granted.

IT infrastructure can be a source of operational constraints as well. Digital and analytics transformations deploy new systems and decommission legacy systems, yet organizations sometimes lack adequate training and experience to manage patches and vulnerabilities of the new systems. Legacy systems, if not decommissioned properly, may additionally leave vulnerabilities that malicious actors can later exploit. For example, a company implemented a piece of hardware in a data center for research purposes but did not include the device in regular production-patching cycles. After a vulnerability was exploited on the device, malware spread across the whole data center, causing a loss of data and rendering the system unavailable. Cloud migrations can mitigate or even eliminate many of these risk types, but only if the cloud migration is done properly with security as a part of its core.

A framework for digital and analytics transformations

The risks engendered in a digital and analytics transformation may be different from those that companies normally face—or they may be traditional risks that happen with extraordinary frequency and potential for significant impact. Fortunately, most companies already have a foundation in place to begin addressing these risks: their existing enterprise-risk-management infrastructure, which is used for financial and regulatory risks. Enterprise risk management typically consists of several common activities, including the following:

— defining a mature enterprise-risk framework

— developing an effective risk governance with taxonomy, risk appetite, reporting, and key risk indicators

— building a risk organization and operating model (including the three lines of defense, where relevant) and assembling the needed resources and talent

— establishing risk-management processes

— creating a risk culture

These activities are critically important to digital and analytics transformations. They must be transformed alongside digital and analytics teams, however. This is because risk management will have to keep pace with the rapidly changing digital-risk landscape to continue mitigating risks but avoid slowing down the business. Our framework makes

it easier for organizations to do this. It consists of four steps that define, operationalize, embed, and reinforce the elements of the transformation. The framework fosters a dynamic approach, helping adapt the existing ERM infrastructure for an increasing flow of risk-mitigating information and actions. Within the framework, organizations design transformation activities and make appropriate interventions. The framework is updated as the activities change ways of working, risk appetites, risk exposure, and talent needs (Exhibit 5).

— *Define:* In the first step, organizations apply the technology-specific elements of their existing risk-management framework—in place to address traditional categories such as financial and regulatory risk—to the transformation scenario. Organizations without an ERM framework in place will need to start there, ideally creating one with a transformation-specific framework to address digital and analytics risks. The objective is to articulate risks and

Exhibit 5

Successful digital and analytics transformations need a tailored framework to keep pace with a rapidly changing digital-risk landscape.

Current state

- Cumbersome risk and compliance reviews lead to frequent delay of product launches

- Challenges from second line are perceived as convoluted and do not always lead to clear set of actions for front line

- Inadequate tools for risk identification, resulting in a lack of appropriate transparency and guardrails

Transformed state

Digital and analytics risk-management framework
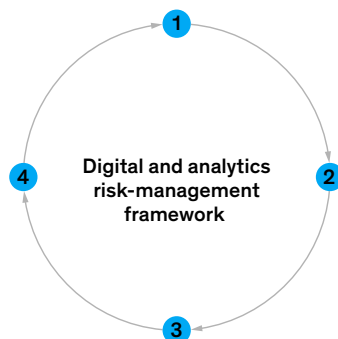
1 **Define:** articulate risks and hypothetical solutions for a given data and analytics transformation (via diagnostic risk assessment, interviews, review of metrics)

2 **Operationalize:** convert solution hypotheses into action; controls tie directly to risks, and control program is tracked with both effectiveness and efficiency metrics

3 **Embed:** drive efficient risk management through transformed operating model, organization design, processes, and governance

4 **Reinforce:** strengthen and scale risk-management ways of working through cultural and talent changes

hypothesize potential solutions through a relevant risk matrix with a clear taxonomy, defined risk owners, available controls and resources, and a governance structure for the initiative.

— *Operationalize:* In the second step, transformation leaders work with risk subject-matter experts or a risk center of excellence to convert risk-management hypotheses into solutions. Specific actions could include introducing software and data controls, validating algorithmic models, implementing systems and infrastructure patching, teaching frontline technologists relevant cybersecurity practices, and validating product resilience through defect and unit testing. As a part of this step, teams also start generating risk reports based on clearly defined metrics such as key risk indicators and key performance indicators that critically measure not only risk effectiveness but risk-management efficiency as well.

— *Embed:* This step is designed to embed the lessons from risk management—including testing results, risk assessments, incident reports, and performance measurement—into existing control implementation operating models, processes, governance, and, if needed, organizational design. In this step, new derisking initiatives are generated based on these lessons. Frontline colleagues in the transformation team and in units being transformed are fully trained on risk awareness, identification, and mitigation.

— *Reinforce:* In this final step in the cycle, transformation teams strengthen and scale risk-mitigation practices by entrenching these practices in talent management and culture change. They also feed critical insights, learnings, and new risks back to core risk teams to update risk infrastructure as needed and pull inputs and feedback back into the "define" step. This keeps risk management, mitigation, and performance current with transformation activities.

Benefits of the framework and transformation roles

The framework enables companies to manage the risks of a digital and analytics transformation systematically, so that it keeps pace with an organization's innovation. It incorporates lessons from the front line to improve the conceptual matrix and adjusts risk-management methods along the transformation journey. It meshes with agile working models to enable better risk management, encourages collaboration, and fosters an enhanced risk culture.
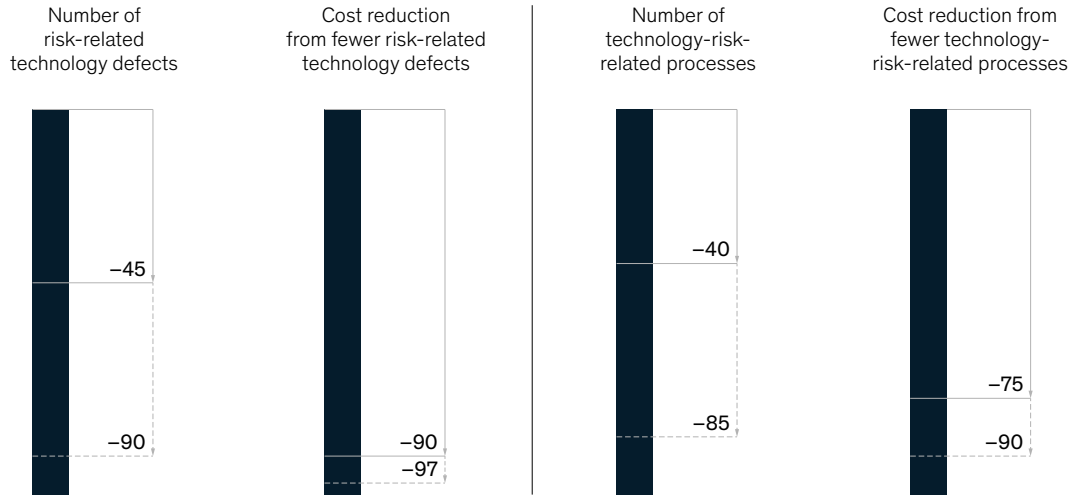
Companies have already seen significant risk-mitigation effectiveness and risk-management efficiency benefits from taking this approach. Although in its early stages, the approach promises to yield further benefits to risk managers and transformation teams (Exhibit 6).

To support the framework and put its approach into practice, companies will need to also define these roles and responsibilities for digital and analytics transformation risks:

— *Digital and analytics transformation lead:* This lead is accountable for delivering the digital and analytics transformation activities.

— *Digital and analytics transformation-risk owner:* This role is responsible for all transformation risks.

— *Transformation working teams:* These groups typically work in agile squads, with risk-management resources assigned.

— *Transformation-product customers:* These are end users of the transformed-products, services, and features; the changes here may affect transformation-risk appetite and risk posture.

Exhibit 6

Improved technology-risk management better mitigates risk while significantly increasing efficiency and reducing costs.

Reductions from improved technology-risk governance and management, range, %

Number of risk-related technology defects	Cost reduction from fewer risk-related technology defects	Number of technology-risk-related processes	Cost reduction from fewer technology-risk-related processes

−45

−90

−90
−97

−40

−85

−75

−90

— *Enterprise-risk-management and control partner organizations:* Transformation-risk leads will work closely with the enterprise-risk-management group and individual control partner groups to ensure transformation risks are accounted for at the enterprise level, and enterprise risks are considered at the transformation level.

— *Transformation-risk manager:* Risk managers specialize in change risks and risks arising in digital and analytics transformations. They work closely with transformation teams on the front line and take part in designing risk controls from the early planning phases of the transformation.

— *Transformation sponsors:* The sponsors of the overall transformation should be on board during the entire change process.

In most cases, defining such roles will not require adding head count. Companies have found that existing team members are ready and eager to take on these responsibilities. They may need some training to become fully effective, but generally most team members are motivated to take on such training simply because they know about the risks being generated or exacerbated in transformation activities.

Finally, companies will have to raise awareness of digital and analytics risks in the organization, including with the executive team and board. Likewise, they must adequately incorporate digital and analytics risk management into their formal risk-governance models (see sidebar, "Snapshot of a successful transformation").

———————

Snapshot of a successful transformation

What does successful risk management in a digital transformation look like? One bank successfully integrated risk controls into its digital transformation through a systematic approach. A number of aspects in its approach stand out.

The bank clearly defines all roles and responsibilities, accountabilities, and oversight related to digital and analytics risk management and creates a governance model across the lines of defense. Risk generalists are involved early in design processes—even sitting with agile development teams as necessary. Those leading the project conduct a formal risk assessment to identify and mitigate risks using a best-of-breed risk-management tool that covers different risk taxonomies. That tool digitally feeds derisking interventions into the work-management software backlogs of product teams. Risk interventions then are pulled forward into product-team sprints as capabilities and features in and of themselves that enhance the product and extend its impact.

A risk and cybersecurity resource is integrated into the transformation-delivery hub to ensure that risk is always part of the conversation and that all risks are tracked with a single source. Competencies, skills, and qualifications are clearly defined for each risk-management role to inform the requirement needed to build and retain a strong risk-management talent pool.

In this bank example, risk management is deeply embedded in all phases of product development, including product road map planning, business review, release planning, and deployment. Other companies implementing digital and analytics transformations should consider adopting a similar model.

In the current business environment, digital and analytics transformations are core to success. If transformations go forward without the right risk-management approach, however, companies simply trade one set of problems for another, potentially larger, set. As digital and analytics capabilities become more pervasive, the companies that will capture the most long-term value from their digital and analytics transformations are those that manage to accomplish their target objectives while also systematically identifying, understanding, and mitigating the associated risks.

Risk & Resilience Practice leadership

Cindy Levy
Global
Cindy_Levy@McKinsey.com

Fritz Nauck
Americas
Frederic_Nauck@McKinsey.com

Maria del Mar Martinez
Europe
Maria_Martinez@McKinsey.com

Gabriel Vigo
Asia
Gabriel_Vigo@McKinsey.com

Gökhan Sari
Eastern Europe, Middle East, North Africa
Gokhan_Sari@McKinsey.com

Kevin Buehler
Risk Dynamics, Cyberrisk
Kevin_Buehler@McKinsey.com

Marco Piccitto
Risk People
Marco_Piccitto@McKinsey.com

Luca Pancaldi, Olivia White
Risk Knowledge
Luca_Pancaldi@McKinsey.com
Olivia_White@McKinsey.com

Thomas Poppensieker
Corporate Risk; chair, Risk & Resilience Editorial Board
Thomas_Poppensieker@McKinsey.com

In this issue