McKinsey & Company

McKinsey on Risk

Institutional resilience starts with understanding risks

Number 12, April 2022

McKinsey on Risk is written by risk experts and practitioners in McKinsey's Risk & Resilience Practice. This publication offers readers insights into value-creating strategies and the translation of those strategies into company performance.

This issue is available online at McKinsey.com. Comments and requests for copies or for permissions to republish an article can be sent via email to McKinsey_Risk@McKinsey.com.

Cover image:
© Westend61/Getty Images

Editorial Board:
Venky Anant, Jason Atkins, Bob Bartels, Oliver Bevan, Richard Bucci, Joseba Eceiza, Carina Kofler, Marie-Paule Laurent, Mihir Mysore, Luca Pancaldi, Thomas Poppensieker, Inma Revert, Kayvaun Rowshankish, Sebastian Schneider, John Walsh, Olivia White

External Relations, Global Risk & Resilience Practice:
Bob Bartels

Editor: Richard Bucci

Art Direction and Design:
Leff Communications

Data Visualization:
Richard Johnson, Matt Perry, Jonathon Rivait, Jessica Wang

Managing Editors:
Heather Byer, Venetia Simcock

Editorial Production:
Nancy Cohn, Roger Draper, Gwyn Herbein, Drew Holzfeind, LaShon Malone, Pamela Norton, Kanika Punwani, Charmaine Rice, Dana Sand, Sarah Thuerk, Sneha Vats, Pooja Yadav

McKinsey Global Publications

Publisher: Raju Narisetti

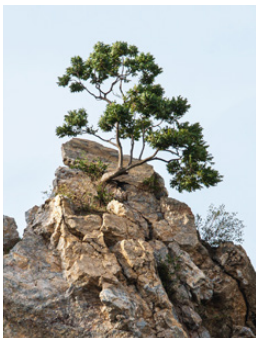
Global Editorial Director:
Lucia Rahilly

Global Publishing Board of Editors: Roberta Fusaro, Bill Javetski, Mark Staples, Rick Tetzeli, Monica Toriello

Table of contents

3 **Three keys to a resilient postpandemic recovery**

The path to sustainable, inclusive growth lies in building resilience now.



6 **From risk management to strategic resilience**

Senior executives at leading companies reveal their commitment to move from defensive risk management to a forward-looking stance based on strategic resilience.

13 **Financial institutions and nonfinancial risk: How corporates build resilience**

As nonfinancial companies move from enterprise risk management to a resilience-based approach, their experience in nonfinancial risk can provide a model for banks.

23 **Lessons from banking to improve risk and compliance and speed up digital transformations**

Banks are beginning to put in place a new approach to risk and compliance that accelerates their digital transformations and improves outcomes.

32 **Aligning portfolios with climate goals: A new approach for financial institutions**

Portfolio-alignment tools will help financial institutions chart more scientifically robust, realistic, and profitable climate strategies.

36 **Ransomware prevention: How organizations can fight back**

Ransomware has rapidly become one of the top cybersecurity nightmares. Strategies for prevention, preparation, response, and recovery can help.

42 **Model risk management 2.0 evolves to address continued uncertainty of risk-related events**

Organizations this year plan to enhance their MRM framework capabilities—including risk culture, standards, and procedures—and to upgrade their validation resources with MRM 2.0 firmly on the agenda.

Introduction

The thinking presented in *McKinsey on Risk* has lately stressed the need to develop resilience as a priority—the ability to absorb shocks, adapt, and pivot into the changing conditions that disruptions create. Three global situations now make resilience the most important quality for organizations. The war in Ukraine, the COVID-19 pandemic, and the climate crisis are very different challenges, but each has caused loss of life and put pressure on the global economy and society as a whole.

The Russian invasion of Ukraine has caused the greatest humanitarian crisis in Europe since the Second World War. Already, thousands of lives have been lost, and millions have been displaced—a shocking tragedy with consequences that will unfold for decades to come. The COVID-19 pandemic has revealed that increased global connectivity, a source of much economic growth after the financial crisis of 2007–09, created unseen or mostly ignored vulnerabilities in our economic and social structure. And the climate crisis, potentially the most disruptive of all, displaces populations and upends economic activity as the earth experiences natural catastrophes of increasing frequency and intensity.

Through the repeated shocks and disruptions, people have acted with extraordinary strength and compassion, companies have displayed remarkable ingenuity and speed, and economies have shown that they can bounce back. Demonstrations of the value of resilience are, thus, all around us.

The lead article in our 12th issue of *McKinsey on Risk* is "Three keys to a resilient postpandemic recovery." Coauthored for *Fortune* magazine by Bob Sternfels, McKinsey's global managing partner, and Klaus Schwab, founder and executive director of the World Economic Forum, the article advances a global goal of sustainable, inclusive growth, emphasizing that the foundations of future growth are laid largely in response to the weaknesses that crises expose. Currently, economies are confronting supply chain disruptions, technological challenges, labor shortages, and the return of inflation. Poverty as well as gender and racial inequalities persist as major growth inhibitors. And the slow progress toward renewable energy has been thrown into great relief by the conflict in Ukraine. Will the world pivot from fossil fuels faster as a result of supply uncertainties?

The following discussions are dedicated to building resilience, with an emphasis on integrated thinking, a scenario perspective, and strategic flexibility and responsiveness. Some articles address individual topics, including financing the energy transition, fighting the rising threat of ransomware, and tackling digital risks. All seek to bring into focus the resilient stance that will enable organizations to better adapt and grow under conditions of near-continuous disruption. Our overarching objective is to help firms navigate those conditions and grow stronger in the coming decade.

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

Thomas Poppensieker
Chair, Global Risk Editorial Board

Three keys to a resilient postpandemic recovery

The path to sustainable, inclusive growth lies in building resilience now.

by Klaus Schwab and Bob Sternfels

The global economy has demonstrated significant resilience through the COVID-19 pandemic, bouncing back faster than expected. Economic momentum remains strong, but nations and organizations are encountering crosscurrents in supply chains, workforce availability, and inflation. The pandemic response comes in the context of a worsening climate crisis and rising economic inequality. These compound challenges remind us that crises can become watersheds of policy and strategy.

Indeed, the foundations of future growth are often laid as societies respond to the weaknesses crises expose. At this juncture, our recovery's success is still not assured. History shows that in times of disruption, resilience depends on *adaptability* and *decisiveness*. Once the most acute period of the pandemic subsides, a resilience agenda will become the key to future prosperity.

To build a better future, the emphasis must now shift from defensive measures and short-term goals to a sustainable, inclusive growth agenda. Growth is a precursor to economic development. A sustainable, inclusive growth agenda will focus on growth that supports the health and repair of the natural environment while improving the livelihood of wider population segments. We need to find pathways to a genuinely better society so that our actions make our planet and our economies more resilient and secure.

But how can leaders meet this resilience challenge to achieve sustainable and inclusive growth? Getting there will depend on effectively and holistically addressing the conditions of our economies and societies and, crucially, their interrelationships—climate, healthcare, labor needs, supply chains, digitization, finance, and inequality and economic development. Three considerations suggest the path forward:

1. *Public- and private-sector leaders need to take a broad view of the resilience agenda.* At the moment, labor shortages, the rise of the digital economy, supply chain disruptions, inflation, and inequality are all addressed in isolation, with overly specialized solutions developed in organizational silos. Such an approach does not adequately address interdependencies that exist between them, as well as the broader, longer-term trends driven by climate change, societal developments, and geopolitical

The foundations of future growth are often laid as societies respond to the weaknesses crises expose. History shows that in times of disruption, resilience depends on *adaptability* and *decisiveness*.

dynamics. One model response is the European Commission's "Recovery Plan for Europe," with its emphasis on the interdependencies between education, healthcare, housing, climate change, economic growth, competition, and jobs and the need to address them in a holistic framework. The difficulties encountered in implementing such plans will be a measure of the distance we must travel to bring along everyone in society.

2. *Strategies and structures have to be designed for flexibility and speed.* We can assume disruption and accelerated change lie ahead. Nations and organizations must therefore approach issues with built-in adaptability and agility. Speed is important. The COVID-19 pandemic and its ever-changing trajectory and impact have shown that we need more timely information, up-to-date strategic agendas, and shorter decision cycles. The initial approach to stopping the virus spread, aimed at eliminating COVID-19 completely, is now being rethought. When circumstances change, so too must the responses from business and government. To face uncertainty, our organizations have to be flexible and always learning. These attributes will weigh more in our solutions than defensive economic buffers (the key answer in the financial crisis of 2007–08). The new stance allows us to respond to supply chain discontinuities, technological leaps, and societal changes. More value is placed on anticipating disruptions and trends than on developing detailed budgets and plans.
3. *Beyond building resilience in business and the economy, public and private leaders must also build societal resilience.* Truly sustainable and inclusive growth solutions go beyond improving business and economic performance. They also contribute to the reparation and sustenance of the natural environment, enrich low-income countries, and truly improve the lives and livelihoods of historically marginalized population segments. This understanding can be fully embraced in the purpose statements and actions of companies as well as public institutions. For companies, the adoption of environmental, social, and governance (ESG) standards and metrics can help optimize strategy for positive societal impact. For governments, measures such as New Zealand's Living Standards Framework take a step in the right direction, valuing more than top-line GDP numbers as indicators of national wealth.

We can shape a common resilience agenda, but to do it we must urgently intensify the dialogue between the public and private sectors. Key decisions and financial commitments made now will determine our direction in the aftermath of the pandemic. Our starting point is a consolidated view of the resilience themes. This will enable us to better understand the opportunities for sustainable and inclusive growth—for companies, countries, and societies. We must strengthen our resilience muscles now. At stake is nothing less than a prosperous future for organized life on our planet.

Klaus Schwab is the founder and executive director of the World Economic Forum. **Bob Sternfels** is McKinsey's global managing partner.

This article appeared in Fortune *on January 27, 2022, and is reprinted here by permission.*

From risk management to strategic resilience

Senior executives at leading companies reveal their commitment to move from defensive risk management to a forward-looking stance based on strategic resilience.

by Alfonso Natale, Thomas Poppensieker, and Michael Thun

In a volatile world, resilience is an increasingly critical prerequisite for corporate performance. The COVID-19 pandemic has caused a massive shock to public health, with dire human consequences. The crisis has dramatically demonstrated the sensitivity of economies to demand shocks, as well as industry vulnerabilities to supply chain disruptions. Furthermore, the pandemic spread in an environment defined by accelerating climate change and the increasingly urgent demand to reduce greenhouse-gas emissions.

On top of public-health and environmental pressures, organizations are subject to many business challenges, societal uncertainties, and geopolitical tensions. The disruptive currents include accelerating digitization, cyberthreats, and inflation and price volatility. The dynamic pace of change makes disruptions hard to predict, even as they grow in severity and frequency. Companies in all industries thus need to plan for the unexpected and build up their response capabilities in advance.

The pandemic crisis also revealed the true value of resilience management to business leaders. They recognized that their crisis contingency plans were instrumental to managing through the crisis. Though the magnitude of the pandemic and its domino effects were not generally foreseen, the processes and procedures companies had in place proved themselves (or not) in very trying conditions.

Key findings from the FERMA–McKinsey survey

McKinsey recently supported the Federation of European Risk Management Associations (FERMA) on a comprehensive survey about the pandemic's impact on corporate resilience. The survey drew responses from more than 200 senior executives and risk and insurance professionals, reflecting a wide range of industry sectors and countries. The survey probed for views on the relevance for organizations, the capabilities for managing strategic resilience, and the importance of resilience in and across corporate functions, including strategy, operations, and risk.

The executives revealed that in the past, the focus of their risk management was on a small number of well-defined risks—primarily financial risks. They told us that now, risk is encompassing the broader mandate of resiliency management. It is woven into long-term strategy development at top organizations, helping companies navigate a far more dynamic operating environment.

Almost 60 percent of respondents feel their organizations have excellent or very good resilience capabilities, meaning they are well equipped to build and manage resilience overall. In part, that is a direct response to the pandemic, which broadened leaders' view of the risk function beyond one or two specific risks. More than half of respondents acknowledged that the global pandemic has made risk and resilience significantly more important to their organizations.

Among specific areas of resilience, companies are clearly focusing on workplace safety and remote working in managing through the pandemic. More than 75 percent said implementation measures in these two areas are largely completed. Fifty-two percent of respondents said that, for their organizations, the most effective capabilities are in place to manage financial resilience.

At the same time, executives reported room for improvement. Management of business operations and the supply chain emerged as weak points during the pandemic. Many companies have yet to fully implement new remedial measures. Senior executives state that risk is still mainly involved in crisis response.

"We are learning from the crisis, reviewing, for example, our evaluation process for suppliers," said the chief risk officer at a company in Italy. "In the past, we focused mainly on financial impact but have since adopted a holistic view, looking at the geographic footprint and compliance issues, among other factors." Survey results included these findings:

— Nearly two-thirds of responding companies said that resilience is central to their organizations' strategic process—either as a top priority or to an important extent. Risk and insurance managers are strongly involved in resilience areas, including operational resilience and digital

and technology resilience. In addition to those two areas, finance and operations were more often cited by survey respondents as the four most important resilience areas.

— Foresight capabilities (scenarios and stress testing) emerged as one of the core areas for improvement. Companies were split in their use of scenarios and stress-testing exercises. Roughly half of executives rarely or never use them in strategic decision making, and half use them often or in every risk and resilience exercise.

— The pandemic continues to highlight the need for secure and flexible technical infrastructure and the strong intersection of digitization within other resilience areas, including implementing work-from-home processes.

— Risk functions and executive teams play leading roles in building a resilient organization, much more so than strategy teams. However, risk managers are not yet at the center of resolving crises at all times. A better risk governance model is key for efficient and effective decision making and crisis management.

To strengthen resilience in the future, most risk managers (75 percent) believe that the most important actions will be to improve risk culture and strengthen the integration of resilience in the strategy process. Important additional areas are improved risk-data aggregation and reporting and more advanced foresight capabilities. Executives also want to revisit risk governance and radiate a better understanding of the critical role the risk function plays.

The challenge now is to move out of a reactive, crisis-response mode and integrate risk with other core functions on a more permanent basis. Likewise, as they guide their organizations in the transition from crisis and risk management to resilience, top managers can can emphasize risk governance and risk-data aggregation to develop better reporting and foresight capabilities. The risk organization has a key role to play and should partner with strategy and the executive team to guide organizations in the transition from risk and crisis management to resilience.

From crisis response to a holistic resilience strategy

Like many crises, the pandemic revealed hidden vulnerabilities in organizations and weaknesses in their response capabilities. Executives had to respond quickly to a variety of arising challenges in operations, including workforce discontinuities and supply chain issues involving critical shortages and logistics barriers. Decision makers learned to value timely and insightful data as they defined priorities and actions under stressed conditions. The FERMA–McKinsey survey revealed some good examples of resilient responses to the immediate pandemic-driven challenges:

— *Operational and supply chain challenges.* Many companies enabled digital solutions, including advanced analytics, to address supply chain issues from the beginning of the crisis. A leading global consumer firm improved the reliability of its supply chain by moving toward predictive maintenance of its machinery; another global company applied next-generation AI technology to monitor and identify unusual ordering patterns and respond accordingly; an energy company applied a smart supply chain digitization plan to provide business continuity. As the crisis evolved, cargo demand surged, and ports became congested. Some companies took bold measures in response: a beverage giant shifted some operations from their container shipping to bulk carriers; big-box retailers began leasing their own containers and chartering ships.

— *Technological challenges.* During the pandemic, cyberattackers have been taking advantage of security vulnerabilities created in the shift to work-from-home operations. In response, many organizations have strengthened defenses, closing potential gaps before hackers can compromise networks. Some companies have made significant investments in their capabilities, sometimes hiring experts; tech giants and other global firms have also acquired smaller cybersecurity companies.

— *Organizational challenges.* At the beginning of the crisis, remote-working arrangements needed to be scaled and implemented for

office work, while on-site workers needed appropriate safety measures, including testing and protective equipment. The record for on-site work has been spotty, especially at the beginning of the pandemic, and many lessons should be incorporated into future plans. The switch from office to home, however, was handled with ready competence by many large companies. The remote workforce required a new cyberstrategy, extending the security shield into the remote endpoints in people's homes. Leaders then explored avenues to prevent the fragmentation of organizational culture, maintain high performance, and support the health and well-being of the remote workforce.

Beyond these often well-executed responsive actions, however, few firms have adopted a comprehensive strategic perspective to meet the challenges of the next disruption over the horizon. Yet this is what organizations need to do if they are to pivot during crises and accelerate into the new crisis-defined environment. The needed orientation is proactive, based on a business perspective, and goes beyond a reactive, second-line-of-defense approach to uncertainty. To build resilience into their long-term strategic decision making, organizations need to develop certain cross-functional capabilities and strengthen resilience in a number of strategic areas.

Overarching capabilities and core resilience areas

The overarching capabilities include foresight skills and disruption and crisis response preparedness. To develop foresight capabilities, organizations gather and study the relevant data, develop pertinent scenarios to discover gaps in resilience, and use this method to anticipate and prepare for future crises. Appropriate crisis response capabilities can then be pursued: those that can be developed and implemented in advance, to be applied quickly and effectively in case of disruptions. These capabilities—such as strengthened financials, better security (whether for IT and software or physical assets), market flexibility, and optionality—can, by design, create a competitive advantage that drives superior performance through the next industry cycle. The core resilience areas can be grouped as follows:

— *Financial resilience.* Institutions must balance short- and longer-term financial aims. A solid capital position and sufficient liquidity enable organizations to weather rapid drops in revenue, increased cost, or credit issues. Resilient companies are able to achieve superior margins by increasing revenue more than controlling costs. But McKinsey research also suggests that tomorrow's resilient firms are more likely to be those driving value-added growth while balancing optionality (retained earnings growth)—rather than those that focus most of their attention on maintaining operating margins at the expense of other proportionate measures.

— *Operational resilience.* Resilient organizations maintain robust production capacity that can pivot to meet changes in demand or remain stable in the face of operational disruption, all without sacrificing quality. They also fortify both their supply chains and delivery mechanisms to maintain operational capacity and the provision of goods and services to customers, even under stress of all forms, ranging from failures of individual suppliers or distributors to natural catastrophes and geopolitical events.

— *Technological resilience.* Resilient firms invest in strong, secure, and flexible infrastructure to manage cyberthreats and avoid technology breakdowns. They maintain and make use of high-quality data in ways that respect privacy and avoid biases, compliant with all regulatory requirements. At the same time, they implement IT projects both large and small—at high quality, on time, in budget, and without breakdowns—to keep pace with customer needs, competitive demands, and regulatory requirements. If something does go wrong, they maintain robust business continuity and disaster recovery capability, avoiding service disruptions for customers and internal operations.

— *Organizational resilience.* Resilient firms are able to attract and develop talent in areas critical to their future growth; where many others fail, they find a way to secure sought-after people—with limited analytics or cybersecurity skills, for

example. Such organizations foster a diverse workforce where everyone feels included and can perform at their best. They deliberately recruit the best talent, develop that talent equitably, and upskill or reskill flexibly and fast. They implement strong people processes that are free of bias and maintain robust succession plans throughout the organization. Culture and desired behavior are mutually reinforcing, supported by thoughtful rules and standards that promote fast and agile decision making.

— *Reputational resilience.* Resilient institutions align values with actions and words. A wide range of stakeholders—employees, customers, regulators, investors, and society at large—are holding firms accountable for their actions, brand promise, and stance on environmental, social, and governance (ESG) issues. Resilience demands a strong mission, values, and purpose that guide actions. It also requires flexibility and openness in listening to and communicating with stakeholders, anticipating and addressing societal expectations, and genuinely responding to criticism of firm behavior.

— *Business model resilience.* Resilient organizations develop business models that can adapt to significant shifts in customer demand, the competitive landscape, technological changes, and the regulatory terrain. This approach involves maintaining an innovation portfolio and valuing entrepreneurship. Particularly during times of crises, resilient organizations are able to adapt business models to the dynamic and uncertain environment.

Resilience as a competitive advantage

The holistic approach to building resilience advances the organization from a narrow focus on risk, controls, governance, and reporting to a longer-term strategic view of the total environment. Rather than hunting for blind spots in risk coverage within today's business model, resilient organizations embrace the holistic view, in which resilience becomes a competitive advantage in times of disruption.

An important aspect of the holistic approach involves using crisis scenarios to test for resilience in a downturn. Accordingly, foresight capabilities are used to develop the scenarios; scenario-based modeling can then pressure-test strategies and business models through future volatile environments—such as those defined by economic downturns, rising geopolitical tensions, disruptions in the regulatory landscape, or technological disruptions. Such an approach enables leaders to move beyond resilience capability assessments to active strategic thinking to find new opportunities and shape new business models.

Resilient organizations develop business models that can adapt to significant shifts in customer demand, the competitive landscape, technological changes, and the regulatory terrain.

Designing and implementing strategic resilience

Companies have lately developed tools to deal with the challenges of the COVID-19 pandemic, but the "resilience muscle" must still be strengthened. Future disruptions will be different, and institutions need to plan for the primary impact and also for second- and third-order effects. Some of these knock-on effects appear only after a long delay but then suddenly accelerate; others gather momentum incrementally until an emergency tipping point is reached.

For a number of reasons, few institutions have built sufficient strategic resilience. The goal of becoming a resilient company can sometimes run counter to the more immediate objective of value creation. Building redundancy in supply chains builds resilience, but it also increases costs and reduces returns on investment; thus, it can make resilience a tough sell to business leaders.

Another barrier is organizational forgetfulness. Resilience is not needed every day; big disruptions are not happening all the time. The importance of resilience can be forgotten between big crises. These trigger big investments, but the next crisis will not necessarily be recognizable as a repeat of the last one. Over time, the effort to achieve strategic resilience peters out, and new leaders shift priorities.

Resilience, as we have been defining it, cannot be achieved in a siloed approach. Due to inertia and biases, efforts to achieve a holistic resilience agenda can begin to veer off course, back toward familiar patterns. And siloed resilience efforts cannot collectively achieve the integrated solution.

Finally, as yet, we have no universal means of measuring resilience (*we are working on it!*). Consequently, the efficacy of investments in resilience tends to be based on qualitative judgements. Likewise, people are not trained in resilience, nor is their performance evaluated based on it. Managers are promoted for expertise in pattern recognition and for avoiding mistakes; however, resilience leadership requires creative thinking, first-principles problem solving for navigating through disruptions, and a predisposition to learn from and adjust to crises and downturns. A defensive stance and routinized thinking will prevent the organization from pivoting and accelerating in the next upswing.

Robust steps toward building sustainable resilience

Companies across industries have learned to successfully navigate fundamental disruptions, emerge stronger, and gain competitive advantage in tough times. The following steps briefly sketch a path to overcoming pitfalls while systematically building and strengthening strategic resilience. The steps are not, of course, a simple how-to guide. Rather, each element relies upon talent, capabilities, and deep commitment to the integrated effort.

— *Measure resilience and start to report it internally.* Taking a business model view, review resilience dimensions regularly and systematically, identifying strengths and weaknesses compared with industry peers. The ability to conduct these reviews is of critical importance to decision making and balancing value creation and resilience building.

— *Pick your disruptions.* A resilience agenda built around generic disruptions or overly specific scenarios is rarely useful. Instead, choose a particular type of disruption to start with, then probe it deeply for expected initial impact and longer-term secondary and tertiary effects.

— *Put less emphasis on extrapolations based on planning and budgeting processes.* The approach is too slow and narrow for our disrupted world. Define instead a mechanism for creating scenarios systematically. Define increasingly disruptive scenarios across a widening circle, and embed the impact of structural factors.

— *Risk functions need to move beyond the formal views of administration, control, and governance, as well as the formal processes for risk assessment.* Find a way to replace these structures, integrating their constituent activities into strategy. Like strategy, risk and resilience

management requires a strong business and market perspective, a risk mindset, and interdisciplinary thinking. For risk professionals, this is a call to come out of the ivory towers and into the marketplace.

— *Identify the organization's natural strengths and Achilles' heels.* Test strategy and underlying assumptions against different scenarios—for example, by deploying qualitative and quantitative scenario analyses.

— *Define a portfolio of resilience investments.* This step will entail revising short-term performance and corporate resilience strategies to enable longer-term profitable growth. Consciously invest in the resilience dimensions—with strategic options and big bets, when needed—to strengthen the strategies. Develop action plans for alternative futures.

— *Build first-line capabilities in resilience; build personal resilience and resilience within teams.* These efforts should also integrate people into the transition.

— *Create an early-warning system that truly monitors internal and external risks.* The board should be involved, but crowdsourcing can be used judiciously for a more secure view of the risks the organization is facing.

History teaches us that the conditions of future growth are often created as organizations respond to the vulnerabilities crises expose. In times of disruption, survival and the wherewithal to achieve future prosperity depend on strategic resilience, which, as the participants in the FERMA–McKinsey survey stress, importantly means adaptability and decisiveness.

Alfonso Natale is a partner in McKinsey's Milan office; **Thomas Poppensieker** is a senior partner in the Munich office, where **Michael Thun** is a senior expert.

Financial institutions and nonfinancial risk: How corporates build resilience

As nonfinancial companies move from enterprise risk management to a resilience-based approach, their experience in nonfinancial risk can provide a model for banks.

by Björn Nilsson, Thomas Poppensieker, Sebastian Schneider, and Michael Thun

Financial institutions, especially banks, have long been the leaders in developing advanced approaches to managing financial risks—credit risk, market risk, and funding and liquidity risk. These practices advanced alongside efforts to create more systematic regulation, beginning with the first Basel accord (1988). Basel II and Basel III followed in the 2000s, and amendments known as "Basel IV" are slated for implementation in 2023. In addition, annual stress-testing exercises are now required by various regulators. At the core of these approaches lies a fundamental understanding that risks can be quantified and expressed in terms of an equity-capital buffer that banks need to hold in order to compensate for potential losses.

Financial risks are reflected in the financial positions on banks' balance sheets and result from their risk-taking activity. Nonfinancial risks arise from operations (processes and systems) and are similar to risks faced by companies outside the financial sector ("corporates"). Over time, corporates have developed approaches to address nonfinancial risk while adapting approaches developed by banks to manage financial risk, which corporates also face. We believe that financial institutions can learn from the experience of corporates in managing nonfinancial risks. A cross-industry comparison can highlight promising opportunities in key areas:

— *Digitization.* As the banking industry moves rapidly to digitize its business model, new risks will emerge, including cyberrisks, IT delivery risks, business continuity risks, as well as new model risks from AI. Technology is the corporate sector that has the most experience with these risks.

— *Critical infrastructure.* Banking is considered highly critical infrastructure. Therefore, the industry could benefit from studying how risks are addressed by other critical-infrastructure sectors, including telecommunications, transport, and energy.

— *Regulation.* Banking is probably the most heavily regulated industry. As a result, it has developed a highly centralized approach to risk management. Banking is the only industry, for example, with a regulatory obligation to include a chief risk officer (CRO) in its C-suite ranks. For these reasons, banking may have the most important risk-management experience in the area of regulatory risk.

Nonfinancial companies hold a variety of views on nonfinancial risks and how to approach them, with differences mainly determined by market and sector. The divergent perspectives relate to each industry's risk appetite and risk-management practices. McKinsey explored these perspectives in a 2021 executive survey on corporate resilience (see sidebar, "The McKinsey–FERMA corporate risk survey: What executives revealed about resilience").

The survey revealed organizations' varying approaches to resilience. A prominent factor is the sector in which the organization operates. For instance, in the airline industry, safety is of paramount importance. Data on near accidents are valued so highly that pilots can be penalized more severely for not providing this information than for having made actual mistakes. In contrast, software providers thrive on developing stable products that are improved incrementally over time. In telecommunications, cloud providers focus on stability as well. Their services performed so well during the pandemic that many banks and nonfinancial companies overcame their doubts about cloud risks. These reservations were formerly a barrier to the transfer of critical software services. After observing the high security standards maintained by cloud providers, organizations came to regard them as safer than on-premises data centers. Finally, in the automotive industry, global production is highly sophisticated, with up to 80 percent outsourcing in the supply chain. This outsourcing allows for product scalability but creates vulnerabilities from geopolitical risks as well as regulatory and technological change. The industry is thus engaged in rethinking strategies across supply chains, software, and product and environmental compliance.

The lessons from particular industries suggest two caveats when comparing practices between banks and corporates:

— When deciding whether risk-management practices are transferable from another industry, financial institutions have to weigh these practices within the context of particular business models and risk appetites.

— Risk management cannot be seen as a collection of static practices but must evolve to keep pace with rapidly changing business models.

It will be worthwhile to explore these two points, comparing operational risk and enterprise-risk-management (ERM) frameworks in banking and corporates and then looking at the broader question of resilience over time. The importance of this second point has grown in recent years and intensified during the pandemic. Many corporates have begun rethinking their risk-management mindsets in light of the present disruptive and rapidly changing business environment. We believe that these developments hold potent lessons for financial institutions.

Corporate ERM approaches and their application to nonfinancial risk

A comparison of the ERM approaches of banks and corporates allows us to understand their different backgrounds and evolutionary drivers. An ERM system consists of four basic layers (exhibit):

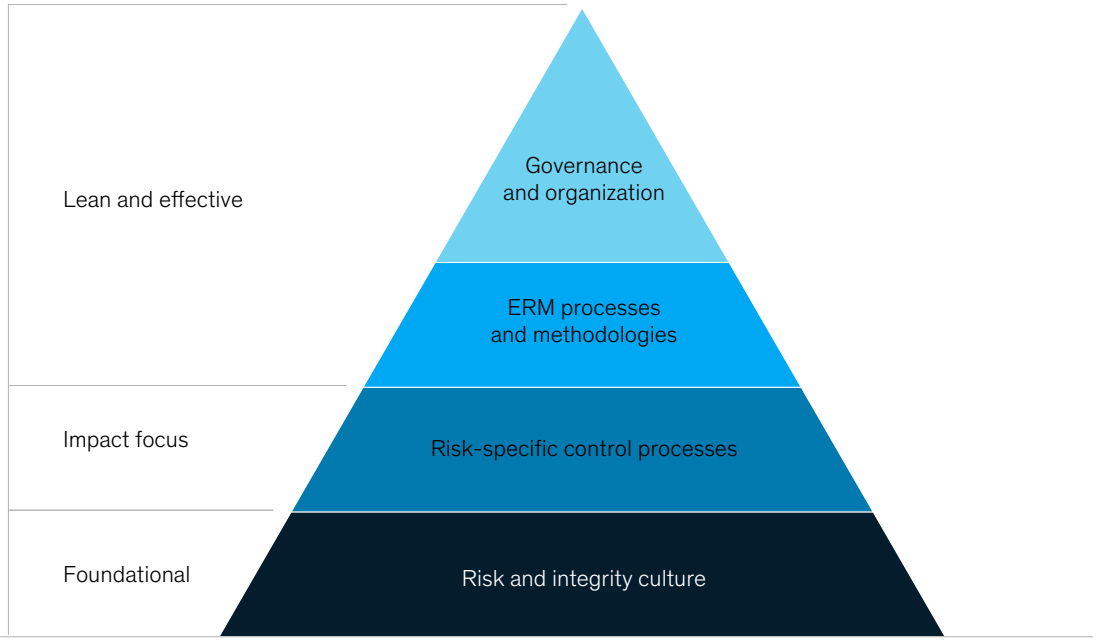
— *Governance and organization.* This layer covers the accountability structure (the three lines of defense) addressing how risk ownership, risk control, and assurance accountability are assigned, exercised through risk committees, and formalized through policy structure. This layer also includes the underlying risk taxonomy to assign accountabilities and acts as a basis for the policy structure.

— *ERM processes and methodologies.* Here, the general ERM approach and processes are defined. Different approaches are usually taken for financial risks versus nonfinancial risks.

Exhibit

The enterprise-risk-management framework has four layers.

ERM framework



The McKinsey–FERMA corporate risk survey: What executives revealed about resilience

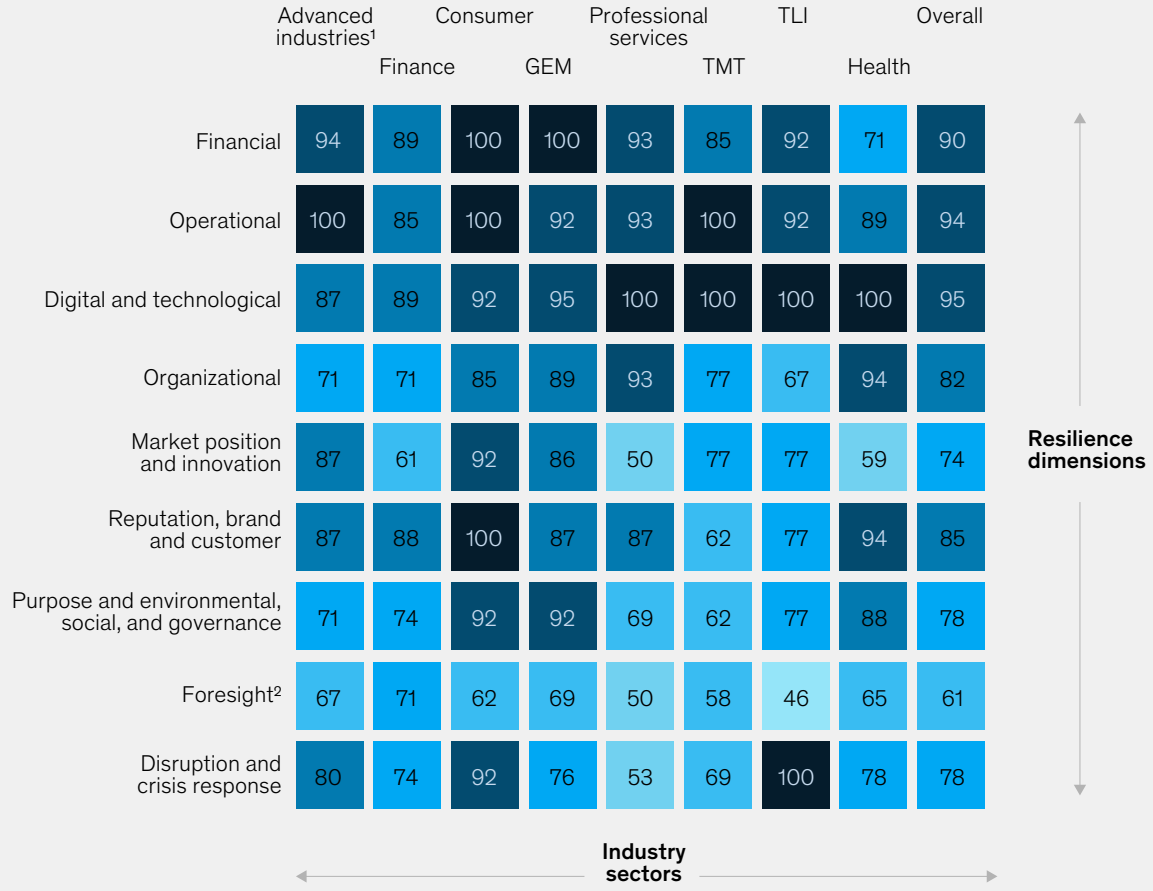
In 2021, McKinsey, in collaboration with the Federation of European Risk Management Associations (FERMA), surveyed senior executives across a number of industry sectors and countries to explore the impact of the COVID-19 pandemic on resilience behavior and organizational management. The survey highlighted the different dimensions of resilience and collected executives' perspectives on their organizations' capabilities to become more resilient in the future. Responses revealed the growing importance of resilience management in long-term strategic planning within organizations, as well as interesting insights on the measures needed to strengthen corporate resilience in the years to come.

Exhibit A shows how more than 200 executives in eight industries evaluated the importance of particular dimensions of resilience to their strategy and operations.

Exhibit A

More than 200 executives evaluated the importance of resilience dimensions to their strategy and operations.

Resilience aspects reported as 'very relevant,' by sector, % of respondents

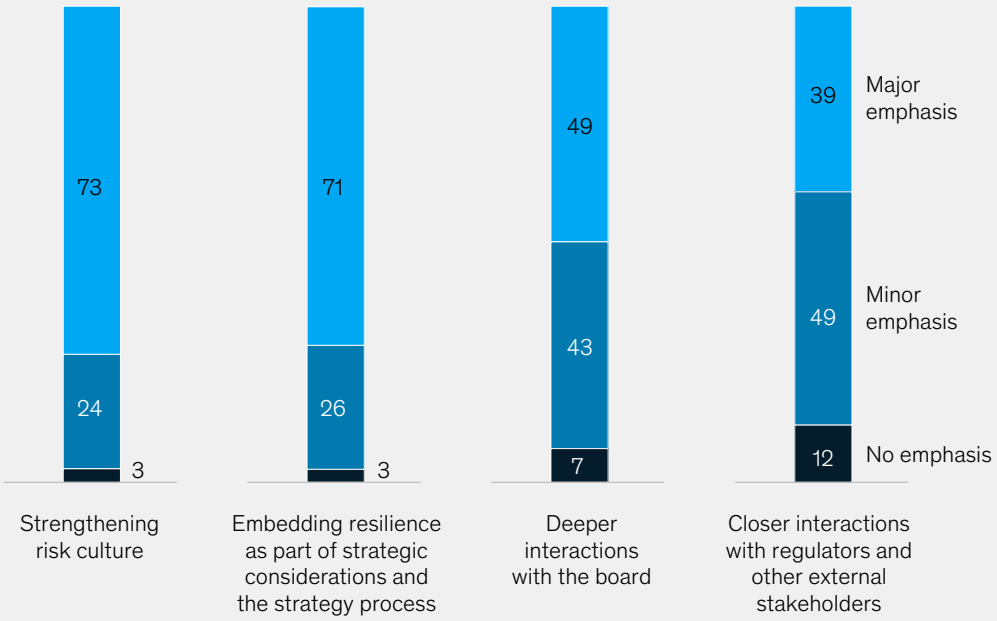


[1]Advanced industries includes advanced electronics, semiconductors, automotive and assembly, and aerospace and defense; finance includes banking, insurance, and private equity; consumer includes consumer packaged goods; GEM includes basic materials, chemicals and agriculture, power, and oil and gas; TMT includes high tech, media, and telecommunications; TLI stands for travel, logistics, and infrastructure; health includes healthcare, pharma, and social and public entities.
[2]Foresight refers to stress testing to assess potential impact of scenarios and simulated reactions on business and the capacity to identify resilience levers to reduce adverse effects.
Source: McKinsey–FERMA Corporate Resilience Survey 2021

Exhibit B

Risk managers would like to embed resilience more deeply in the strategic process while also promoting risk culture.

Actions that managers will use to strengthen future resilience, by level of emphasis, % of respondents



Priorities of risk managers as they look ahead:

- Around three-quarters of participating risk managers want to improve risk culture within their companies and integrate resilience more forcefully in the strategy process.
- Risk managers place less emphasis on engaging with external stakeholders and regulators as part of their resilience-strengthening priorities. This implies that risk managers are looking inward to build and manage resilience.

Note: Figures may not sum to 100%, because of rounding.
Source: McKinsey–FERMA Corporate Resilience Survey 2021

The resilience dimensions tested were financial; operational; digital and technological; organizational; market position and innovation; reputation, brand, and customer; purpose and environmental, social, and governance (ESG) capabilities; foresight (stress testing using scenarios and simulated reactions to identify mitigation actions); and disruption and crisis response.

Executive participants, drawn from within and beyond the resilience function, expressed general awareness of the importance of each of the resilience dimensions. The first three areas listed—*financial, operational, and digital and technological* resilience—were viewed as most important by respondents in all sectors. The fourth area, *organizational* resilience, was seen as highly important by participants in global energy and materials sectors (energy, chemicals, agriculture, and materials); professional services; and the health and public sectors, while it drew lower scores from companies in transport and logistics and advanced industries.

The survey responses show that executives overall are confident in their organizations' financial and operational resilience capacities. Most agree, however, that foresight capabilities are weaker and should be improved. Nearly 60 percent believe their organizations are very well equipped to build and manage resilience overall. Likewise, a majority said that their organizations had effective capabilities and tools in place for managing financial and operational resilience, followed by organizational resilience. Resilience

capabilities are being developed in crisis response; reputation, brand, and customer; and digital and technological areas.

As for the risk function, it plays the strongest role in the operational, digital and technological, and crisis-response resilience areas. Nearly 20 percent of companies assign the risk function the leading role in disruption and crisis response, the highest for any resilience category. The areas of least involvement are market position and innovation and reputation, brand, and customer. Exhibit B presents the priorities that risk managers across industries expressed as they look ahead.

It is important to note that risk functions and executive teams play a leading role in building a resilient organization, much more so than strategy teams. However, risk managers are not yet at the center of crisis resolution. A better risk-governance model, therefore, is needed for efficient and effective decision making and crisis management.

When asked to look forward, three-quarters of risk managers expressed the view that to strengthen resilience, they need to improve risk culture and integrate resilience more closely into the strategy process. Additional areas for improvement included risk-data aggregation, reporting, and more advanced foresight capabilities. Executives also want to review risk governance and foster a better understanding of the critical role the risk function plays throughout the organization.

Financial-risk approaches focus on limit structures, while approaches for nonfinancial risks focus on severity and probability matrices mapping inherent and residual risks. The risk profile is managed through numerous processes: incident management, risk and control assessments, risk appetite, and monitoring and reporting processes.

— *Risk-specific control processes.* This layer entails all mechanisms for managing specific risk types. Nonfinancial risks are managed through risk-specific controls, often called key controls, as they are formally governed by the ERM approach. These can be controls for reconciliations for financial disclosures, the "four eyes" principle for business partnership approvals, or systems-embedded controls often used for managing cyberrisks.

— *Risk and integrity culture.* This final layer refers to managing norms and behaviors around risk, including the incentive structure, the tone set by top management, the consistency of formal risk governance with actual behavior, and the approach used to discover and balance risk issues and conflicts throughout the organization (such as P&L performance targets and adherence to a company's risk and integrity norms).

These ERM layers and their components commonly exist in banking and corporates. Their maturity and development, however, can differ significantly. There are, for example, significant application differences, as risk management in banking is heavily regulated, whereas corporate ERM practices are driven by industry standards, such as those related to the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Differences in organization and governance

A striking difference between corporates and banks can be seen in their respective risk-governance structures and the extent to which they are formalized. As much as 10 percent of bank staff might be situated in central risk functions (risk, compliance); in large corporates, the corresponding share is often less than one-tenth of 1 percent. The reason for the difference is that banks need heavier central risk functions to meet more stringent regulatory requirements. These include a mandate to have a CRO as a distinct second-line executive. Corporates, on the other hand, focus more on embedding risk management into their operational processes within the front line. They usually assign risk and compliance functions to the CFO; rarely will a nonfinancial company have a dedicated risk chief executive.

For corporates, the risk-management function mainly identifies and reports on risks. It also manages a few frameworks for commercial compliance in such areas as business partner due diligence, capital markets and M&A compliance, antibribery and corruption risks, and export risks. Most nonfinancial risk management, as it relates to the corporate operating model, will be embedded in the businesses.

The differences become evident when we look at how risk issues are addressed in banks versus corporates. At banks, the CRO usually becomes involved, answering to the regulator about incidents and the remedial programs applied to address underlying issues. In corporates, the businesses in which the risks are materializing are usually responsible for identifying them and applying solutions to resolve them. Central risk and compliance functions often play supporting and coordinating roles (except for commercial-compliance issues, for which the response is centralized).

Many banks augment frontline ownership of risk with divisional control offices. This allows banks to address the root causes of issues more effectively and permanently. For corporates, central risk and compliance functions generally would not be responsible for certifying compliance for risks arising in the businesses—such as health and safety risks in mining, network security for telecommunications companies, or software risks for autonomous vehicles in the auto industry.

Corporates have, however, overcome the artificial first- and second-line delineation that banks often apply. For banks, the division can create a wall between an independent control function and a center of competence. Interestingly, the term "independent control" has recently been eliminated from the COSO's organizational standards with respect to the second line, whereas in banking, the term is still used in all regulations.

Banks manage financial risk through various quantitative means and balance sheet analyses with a more centralized approach than the business-embedded risk approach taken by corporates. Corporates can consider whether they might benefit from more a centralized ERM in certain areas.

Differences in the ERM approach

Banks perforce emphasize financial risk in their traditional ERM approach. They take a highly quantitative approach to capital as the balance sheet resource. The risk profile is usually defined from the top down in relation to available capital (after certain buffers), measured both in regulatory as well as economic terms and then cascaded into the organization.

For various reasons, this approach is impractical for nonfinancial risks, other than in measuring the potential impact these risks might have on capital as the last compensating resource. Banks apply capital models to gain a complete view of the adequacy of their capitalization levels and then allocate this capital across different businesses. They know that the ingoing assumptions are statistically weak. Nevertheless, the approach allows analogous steering on a capital basis aligned to financial risks.

The drawbacks are twofold: first, history is not a reliable predictor for nonfinancial risks, given continuous business-model changes, process enhancements, and regulatory changes. The contrast with credit and market risks is clear, since creditworthiness, for example, can be predicted quite accurately from balance sheet data, just as market volatility can be measured from market data. Second, nonfinancial risks have to be evaluated in the context of the specific business model and customer expectations. A more iterative approach to business or consumer software development acknowledges that bugs must be continuously fixed; the risk appetite is very different for risks involving health and safety, such as for software in nuclear-power plants or even consumer products such as cars.

Corporates have therefore developed risk-management approaches rooted in expert data and performance data for processes and systems. Such data provide a better basis for steering nonfinancial risk. Industrial corporates take this approach to quality control and the management of most product- and production-related risks. Banks, on the other hand, have a more difficult time, as they must address heterogenous processes and highly complex products built over time. Some have begun developing process or product-quality frameworks for managing nonfinancial risks. Most, however, have not. They still need to make that connection and, more important, find a way to address it.

Where does this leave banks when it comes to addressing nonfinancial risk? In a tight spot, actually, because risk-and-control self-assessments or capital-driven risk-appetite frameworks are only meaningful for nonfinancial risks when the nature of these risks is well understood. Only then can

banks establish specific business-related views and apply practical metrics in the same way that the businesses do in the first line of defense. Replicating centralized, capital-based quantitative approaches that cascade metrics across the organization will be of limited use.

Worth noting is that corporates also struggle to apply business-linked logic universally within their ERM approach. In attempting to make risks comparable, define risk appetite, and centralize reporting, corporates have found that their second-line teams begin to replicate the banking approach. This leads to central functions at corporates hitting the same limitations that banks experience.

Differences in risk-specific control approaches

Banks can thus learn from highly sophisticated approaches for managing nonfinancial risk developed by some corporates for their business models. Experiences from particular industries can provide helpful guidance to the banking sector (and corporates from other sectors).

— *Managing process risks.* Those financial institutions—mainly banks—that develop complex products and business models can learn important lessons from the auto and pharma industries. In automotive, approaches to managing process and production risks incorporate considerable experience and are highly sophisticated, especially in relation to product cost, quality, and safety. The high level of outsourcing in the auto industry (as much as 80 percent) requires continuous monitoring of suppliers in relation to cost and quality. In pharma, the management of risks related to R&D and (heavily regulated) production standards is highly developed.

— *Managing software development and deployment risks.* Banks have begun to develop and deploy software in rapid cycles, an approach mirroring that of tech companies. However, the relative stability of products developed by tech companies, as well as the smoothness of their subsequent adoption, stand in contrast to the experience of many banks. Banks, therefore, have plenty to learn from the tech experience.

— *Corporate security and business continuity.* The airline industry has been addressing geopolitical risks and safety requirements since its inception. Its vast experience includes many mechanisms to deal with physical security.

— *Debiasing strategic decisions.* Industries in which capital expenditure is high, such as oil and gas, basic materials, or transport, have extensive experience in assessing and managing large projects and their attending risks. They can be especially adept at removing biases in decision making on the business case, as well as identifying risk mitigants.

Risk and integrity culture

Given the small size of corporates' risk functions in relation to those of banks, corporates have had to place greater emphasis on cultural elements. Most of the major nonfinancial risks that corporates contend with have serious integrity issues associated with them, as evidenced in some spectacular cases: from the emissions scandals in automotive to autopilot failures in the aircraft industry.

To counter these dangers, corporates have deployed an array of measures: whistleblower systems, investigations, training and communication programs, and employee surveys. Banks have adopted some of the same measures but on a smaller scale. Some banks little value risk culture as a risk-management lever. Risk culture may also play a smaller role in managing financial versus nonfinancial risk, given the greater transparency afforded the former in bank operations.

Resilience: The new risk-management paradigm for corporates

The discussion so far has focused on nonfinancial risk in a continuously changing world. Nonfinancial risk is found to be deeply embedded in corporate operations. As the 21st-century business environment became more volatile and disruptive, however, companies began to question standard risk-management approaches. The thought leaders among them are now calling for new approaches that go beyond risk management, toward corporate resilience. A report on a recent CFO conference

of global companies noted, "Caution and preparation dominate the current strategies of many companies.... They rely on early warning systems and greater resilience in order to be able to withstand another shock."[1]

Resilience is still an emerging approach. Many companies have taken early steps, including efforts to manage resilience levels holistically across the enterprise. Executive teams and boards are raising new topics with their risk teams, discussions that could provide useful insights for banks. The new conversations have centered on four questions.

Identifying blind spots

Many boards are blindsided by risk events that seem to come out of the blue. A keen eye, however, can usually detect warning signals that precede these events—as long as leaders are receiving appropriate reporting. The executive team and board must have timely reporting that permits critical evaluation of the key elements of their risk profile, including the risk drivers and how they are evolving. Many existing reporting systems are simply inadequate for this crucial purpose. They provide too much extraneous detail, swamping the important messages; assessments can be too diffuse, covering everything but lacking the needed focus on important trends; reporting can fail to highlight the most important risks and can hide connections between internal and external developments.

Managing transformations

Often underestimated are the risks emerging from transformations of all kinds, including cost or lean transformations, growth programs, or fundamental changes in the business model due to digital, AI, or other technologies. The current static ERM processes are often unable to understand and address the company's changing risk profile. Specific approaches are therefore needed, quite apart from project-risk measures, to understand and mitigate transformation risks.

Derisking strategy

Both banks and corporates often relegate strategy to planning exercises in which the business mix is adjusted according to the changing business environment. In a world of growing uncertainty and disruption, however, the typical three- to six-month planning cycle is proving inadequate. The spectrum of outcomes supporting planning is generally unable to incorporate dramatic technological change, public-health and climate crises, and volatile social-media trends. The more disruptive changes mean that strategies must be stress-tested against shorter timelines, and scenarios have to account for a broader set of potential outcomes. At the same time, banks need to develop dynamic capabilities and structural resilience assets:

— *Dynamic capabilities.* These are critical skills that involve foresight—the ability to anticipate disruption—and informed action, incorporating implications into business decisions. To develop them, banks will need to invest in data and information gathering to analyze the potential implications of expected disruptions before they happen. The specific practices include continuous scenario analyses, cyberattack simulation, and fast decision making within corporate governance.

— *Structural assets.* While capital and cash are key resources to compensate for risks, organizations need to pay more attention to other resilience assets in order to manage disruptions effectively. This includes developing organizational capabilities, strengthening the supply chain, deepening technological capabilities, and safeguarding market positions, reputation, sustainability profiles, and other societal expectations.

These structural assets relate to common risk taxonomies. However, leading corporates are including them in the strategy debate, moving beyond the question of controls. They are looking at fundamental capabilities and structures that mitigate risks. The key tools are broad-range scenarios (in terms of outcomes and time periods) used as starting points to identify risks and risk-mitigation requirements.

Creating strategic options

The opportunity question arises in any well-designed strategy process. The financial crisis

[1] Bert Fröndhoff, "What CFOs have learned from the pandemic," *Handelsblatt*, June 6, 2021.

of 2007–08 demonstrated that during crises the winners of the next cycle are created. The outperformers often build on more flexible cost structures; they might be able to dispose of noncore assets more quickly, while focusing on growth. This could involve internal actions to adapt the business model as well as external opportunities, which are seized using available financial resources and skills. The winners emerging from the financial crisis looked at more than the downside of strategic scenarios; they saw upside, too, and sought to invest in strategic optionalities that could provide competitive advantage. The current semiconductor shortage in the auto industry provides one example of a resilient strategy through a crisis. In 2020, Toyota did not cut back on orders of this relatively low-cost item at the beginning of the pandemic, while other OEMs did just that. The result was that, for a time, Toyota was better able to maintain production and meet demand.

Lessons for banks

The experience of corporates provides banks with lessons for improving how they address nonfinancial risk. Corporates continue to develop their ERM systems, going beyond the formal processes. They are focusing on embedding risk management in the front line and elevating strategic-resilience questions to the executive team and the board. Banks can profitably heed these steps, as they lead to a more advanced approach. Banks have a second-line focus for financial risk, which they otherwise tend to replicate for nonfinancial risk. Banks can become better adjusted to the changing risk landscape by effectively embedding the management of nonfinancial risk into the front line and rethinking their approach to risk appetite (beyond the current cascading of capital metrics or an arbitrary selection of KPIs and KRIs). The approach ensures that banks comprehend the full and varied spectrum of nonfinancial risks and understand that a generic, governance-focused nonfinancial-risk system is clearly inadequate. Like the leading corporates, banks can build an effective approach to nonfinancial risk by improving the management of relevant processes and systems and strengthening resilience overall.

The risk profile of a bank, like that of a nonfinancial company, is shaped by the strategic decisions it makes. Banks can learn from the experience corporates have accrued in developing effective approaches to managing nonfinancial risks. These include embedding risk into strategy and improving overall resilience. These measures are particularly important in the current economic environment—one that is bound by pandemic-related disruptions, accelerating technological change, and increasing regulatory layers. Our times are forcing organizations to take actions that would be regarded as drastic in an ordinary period. They must, therefore, understand the implications of these actions for their institution's risk profile.

Björn Nilsson is an associate partner in McKinsey's Stockholm office; **Thomas Poppensieker** and **Sebastian Schneider** are senior partners in the Munich office, where **Michael Thun** is a senior expert.

This article was adapted from "Financial institutions and nonfinancial risk: How corporates build resilience," published in *Non-Financial Risk Management: Emerging Stronger after Covid-19*, Thomas Kaiser, ed., London: Risk Books, Infopro Digital Services, 2021. Download the article at risk.net/non-financial-risk-management-emerging-stronger-after-covid-19.

Lessons from banking to improve risk and compliance and speed up digital transformations

Banks are beginning to put in place a new approach to risk and compliance that accelerates their digital transformations and improves outcomes.

by Jim Boehm, Jan Shelly Brown, Lama Sabbagh, and Karim Thomas

A midsize bank wanted to go completely cloud native: modern core-technology architecture, agile, and DevSecOps. It moved aggressively, recruiting top engineering talent and automating many controls. However, it quickly realized that it needed to bring its risk and security functions along on the transformation journey. These control teams were still using traditional risk-and-security management practices in the new operating model and couldn't keep up with the new, faster ways of working. As a result, the company's regulatory-examination team found deficiencies in its control partners' ability to provide credible challenge, and the need for remediation ultimately delayed the release by about five months.

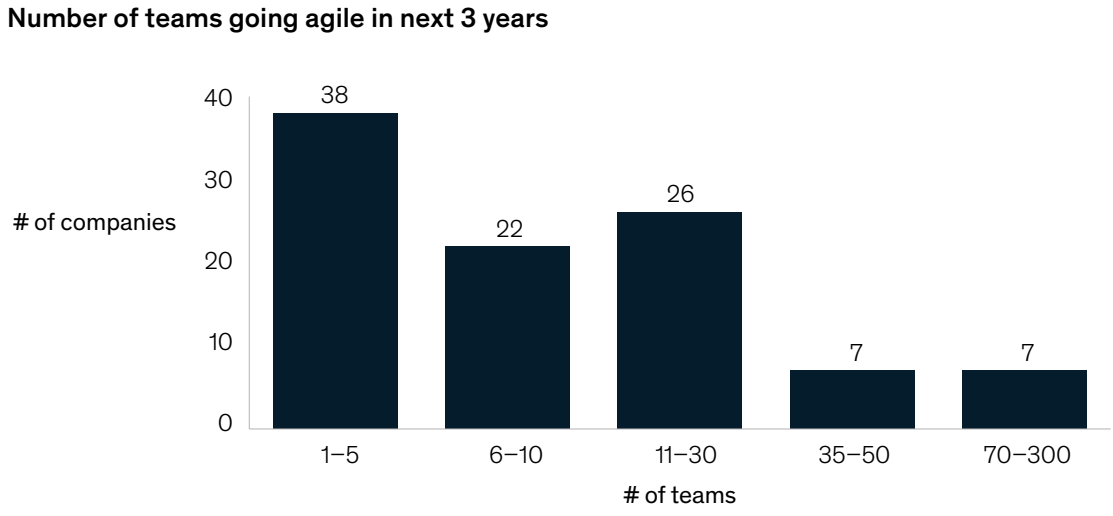
Unfortunately, this situation is all too familiar in many sectors when companies undertake large-scale digital transformations. In many cases, they focus initially on how to be more digital—move at speed, use data to make decisions, respond rapidly, and so on—and only later think about risk and compliance. At a small scale, this is fine because companies can muscle through issues on an exception basis. But as companies scale from ten agile teams to 40 or more, that ad hoc approach breaks down. This is particularly worrisome because 60 percent of companies we analyzed still have only ten or fewer working agile teams in operation, and only 14 percent have more than 35 (Exhibit 1). To scale their transformations, they will need systems in place that can provide necessary leverage and support to agile teams, particularly for control functions such as risk, compliance, legal, cybersecurity, and safety. While banking has been at the forefront of these issues due to the highly regulated nature of the sector, the issues are similar and relevant in other industries as well.

New pressures on risk and compliance

In our experience, many companies have accepted the notion of "risk by design," where the risk function is embedded into the development process. The issue, however, is that few companies know what the risk issues are or how to systematically approach them (see sidebar, "Types of transformation risk"). In fact,

Exhibit 1

Most companies are in the early stages of moving to agile, with plans to transition one to ten teams in the next three years.



our research on 100 C-suite leaders and business-unit heads from companies across industries and around the globe found that almost half of them had difficulty understanding the risks generated by digital and analytics transformations—by far the top risk-management pain point.

Even when companies do appreciate the importance of managing risk correctly, their efforts are often on a surface level, such as setting up forums between first- and second-line risk, taking a limited set of risk actions within a single organizational silo, or adopting a few agile ceremonies, such as stand-ups. Risk teams sometimes try to force-fit traditional practices into the transformation framework and, as a result, simply can't keep pace with agile development teams, leading to further tech and regulatory debt.

The price for not keeping up will just keep rising in the form of significant delays, regulatory scrutiny when companies are unable to provide credible challenge in the new environment, or (worst of all) risk failures and large penalties. A revenue boost of $200 million generated by a digital transformation doesn't mean much if a company is fined $300 million in related risk-violation penalties.

Simply put, companies need to actively account for risk in their digital transformations or they may destroy the value that digital creates.

Avoiding these costly breakdowns during a digital transformation requires a fundamental change in the risk-and-compliance function at an enterprise level. In particular, we've found that the best companies establish active collaboration between risk, security, IT, and the business units. They have a comprehensive understanding of the changes needed at the operating-model, technology, and culture levels and a coordinated approach to the actions to take and in what order. Our analysis shows that the most successful companies significantly outstrip their peers in a few specific actions, including retraining personnel, automating processes, and using new tools.[1]

Companies that make this enterprise-level shift see significant benefits. Not only do they avoid fines and breaches; they are also able to accelerate the pace of their digital transformations and improve customer experience. We've also found that remediating risk-function defects through better governance and management earlier in tech delivery can reduce remediation costs by about 10

[1] Jim Boehm and Joy Smith, "Derisking digital and analytics transformations," McKinsey, January 5, 2021.

Types of transformation risk

There are about 15 risk categories that companies need to account for. Here are a few of them:

— technology and cybersecurity (such as system stability or unauthorized access to systems)

— privacy (gaining customers' consent to use their data)

— credit (for example, which offers are automatically pushed out to customers)

— legal (failure to meet differing jurisdictional requirements in digital channels)

— reputational (customer experiences that negatively affect customer satisfaction)

percent, while embedding tech-risk management in technology delivery can reduce defects by 50 percent. One financial institution was able to reduce overhead by 85 percent by embedding technology-risk nonfunctional requirements (NFR) in Jira backlogs, and it was able to deploy new code 90 percent faster by embedding security checks into agile sprints rather than requiring stage-gate review.

Six concrete actions

We have found that successful risk-and-compliance functions focus on six coordinated actions during digital transformations (Exhibit 2). That point about coordination bears emphasis. Leaders we've spoken to have often made progress on one or two of these actions, but rarely more than that, with the result that risk-and-compliance efforts continue to fall short of where a "digital-first" business needs them to be. Successfully implementing these six actions requires leaders and teams in security, risk, IT, and the business unit to work together. Embedding more risk decision making with the front lines, for example, can't happen unless the corresponding business unit commits to training its people on risk.

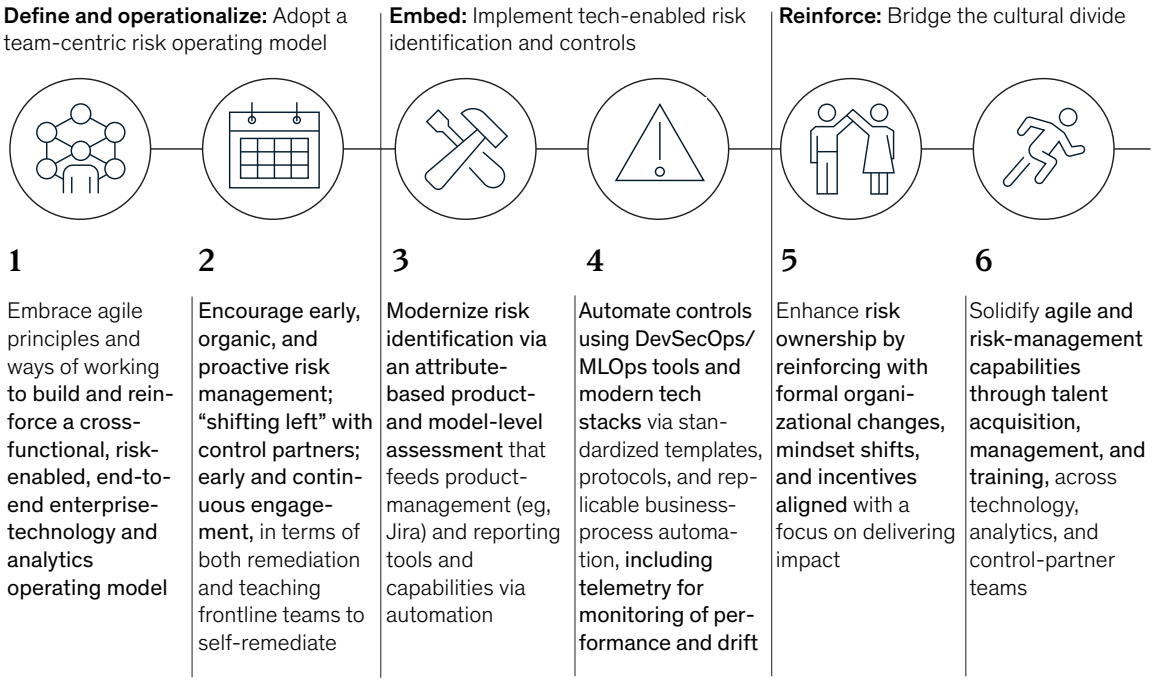
1. Increase risk ownership at the first line of defense

For risk management to be more than an afterthought, agile teams working on the front lines need to own it and be accountable for it. That requires sufficient tools and training (see more in actions 3 and 6), of course, but the key point is that teams on the front lines have to be given specific decision rights and encouraged to focus on risk from the very beginning. This helps to avoid the "not my job" mindset that undermines risk efforts.

Leadership must be clear about management and oversight responsibilities, including governance, standards, guardrails, and risk taxonomy. At a large European bank, for example, increasing risk ownership at the first line of defense not only reduced the number and severity of risk issues but also significantly increased speed to market.

Exhibit 2

A holistic transformation is needed to enable agile risk management.



2. Identify and manage risk in a more agile way

To rapidly identify and remediate risks, regular agile events (such as quarterly business reviews and release planning) should include risk discussions from the very beginning of the transformation, with clear roles defined for both the first and second lines of defense. This "shift left" approach does not destroy credible challenge; it just moves it earlier in the life cycle and gives regulators something concrete to measure against. Advanced organizations maintain a pool of experts with various risk profiles (operational, compliance, price, reputational, security, and so on) that can be embedded into working agile teams as needed. Risk assessments then happen in the regular flow of development (Exhibit 3).

At one financial-services company, this approach not only helped to decrease the number of defects the products delivered but also streamlined the risk and governance processes, reducing the number of governance review groups from 33 to seven.

3. Modernize risk identification

Our analysis indicates that, although 75 percent of companies have not adequately assessed their digital-transformation risks, those that have done so have experienced a 75 percent increase in risk understanding. While this may seem obvious, in practice companies rarely do it at sufficient granularity. Top companies adopt a thorough risk taxonomy and implement an integrated and comprehensive risk assessment that covers all digital and analytics risk areas, such as third party, people and capabilities, audit and compliance, and change risk or overspend (Exhibit 4). This effort helps to identify and monitor risk and develop mitigation activities.

Our analysis further revealed that companies with the most mature risk practices manage risks in a single place so they can more easily track and address them. We have found that advanced organizations are also increasingly using automated risk-assessment tools on every new feature or user story.

Exhibit 3

Risk assessments are conducted iteratively as part of the agile operating cadence.

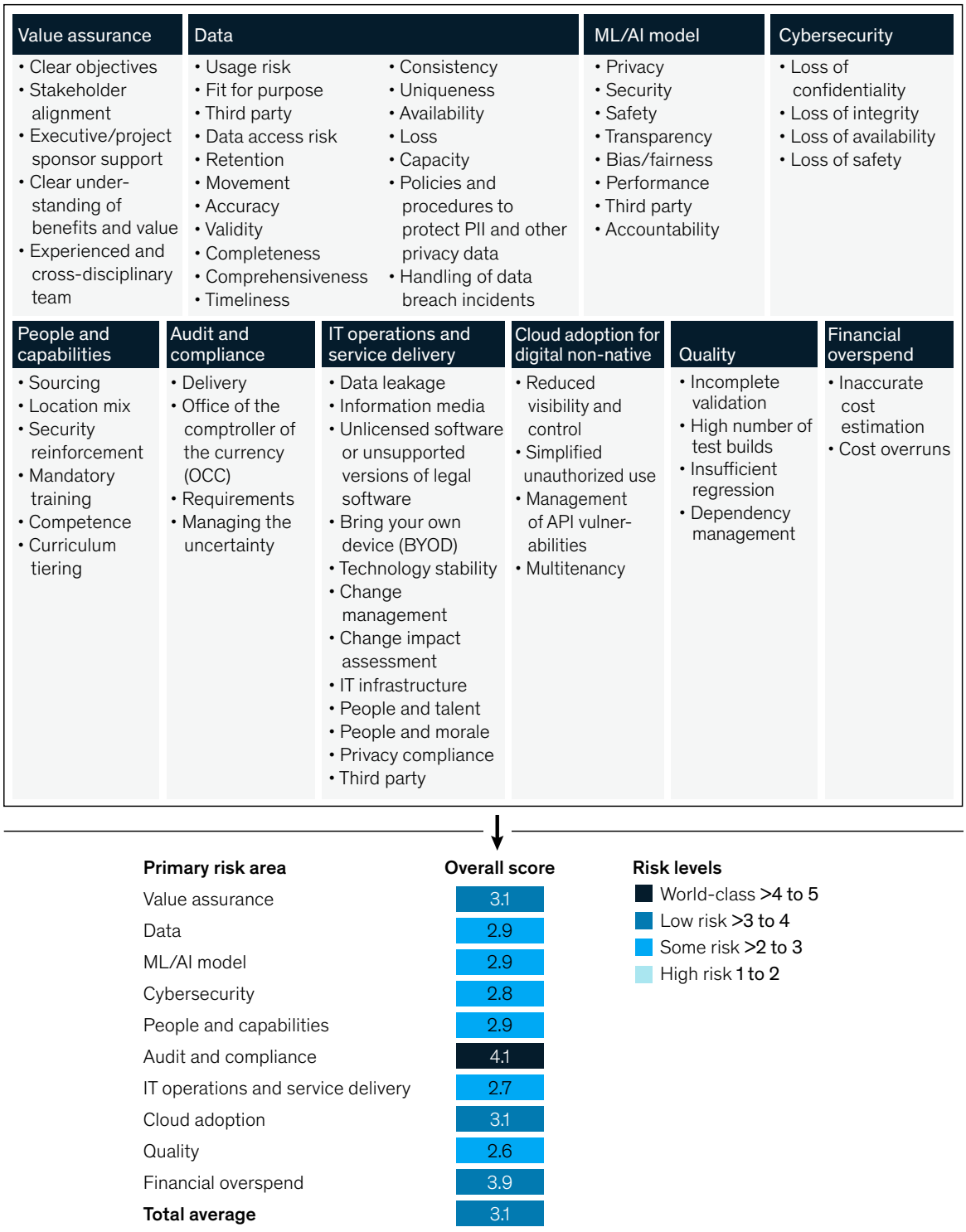
Example

	Product road map planning →	Quarterly business review (QBR) →	Release planning →	Sprint planning and sprinting →	Release review and deployment
		Quarterly		Every release	
1st line of defense	Complete **initial risk assessment** to identify risks and relevant risk subject-matter experts	**Refine risk assessment** and update risk-rating dashboard to be reviewed in QBR	**Create mitigation activities** in collaboration with product owner and risk subject-matter experts and include in team backlog	**Work with product owner to ensure assigned** risk-mitigation user stories are executed, and update **risk ratings to reflect new status**	Provide evidence to demonstrate that risks are appropriately mitigated and present **risk-rating dashboard**
2nd line of defense	Review and validate initially completed risk assessment **Set risk-acceptance thresholds,** ideally linked to risk appetite	Provide **risk approval during QBR** against organization's **risk-acceptance thresholds**	Confirm that **product is fully within risk-acceptance thresholds** (or has approved exceptions) prior to releases	**Track mitigation, risk rating, and requested exceptions** to risk-acceptance thresholds	Participate in release reviews to **confirm risks have been identified** and mitigated appropriately by product owner, risk generalist, and subject-matter experts

Exhibit 4

Product- and model-level risk identification across a wide swath of digital and analytics risk areas enables holistic mitigation.

Illustrative



These help product owners review the risks associated with new features right from the start of the development process. They also use quarterly business reviews (QBRs) to anticipate risks and work through how to address them.

4. Automate controls

Top companies automate not only risk controls but also their monitoring and testing (for example, compliance as code) to ensure that risk-related requirements are being met. Controls such as distribution of duties, code reviews, and application security testing (Exhibit 5) can also be automated and embedded within the existing continuous-integration and continuous-deployment (CI/CD) flow. Many companies run into issues during the automation process because the technology and risk organizations don't have a clear view of priorities. Consequently, the automation process is haphazard or generates only the limited value of simplifying the legacy processes. Organizations that successfully automate the risk function, on the other hand, prioritize the technology backlogs that address material risk areas as well as speed to market.

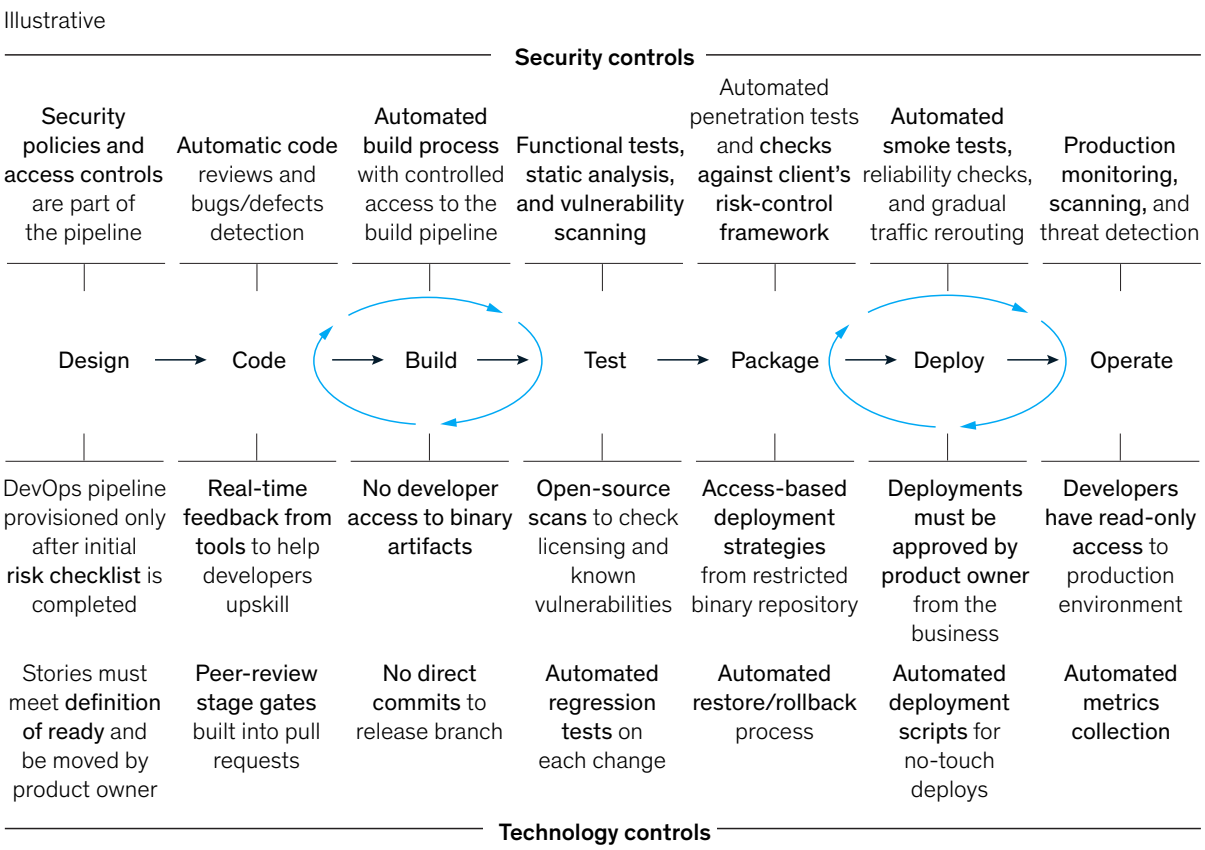
5. Invest in shifting mindsets

Even when the risk function and other teams work together, they can still butt heads. Risk experts block business initiatives because their risk controls are insufficient, for example, while the business regards risk control as a source of constant delays.

Exhibit 5

Tech-enabling control activities improve risk mitigation, speed, and automated control interrogation.

Illustrative



That needs to change. Risk needs to be part of everyone's job. One area that companies tend to overlook in this regard is the value of having the second line of defense—typically, risk subject-matter experts—more closely involved in daily team activities so that they can participate more in finding solutions rather than just challenging risk (still maintaining their objectivity, of course).

While training (see action 6) and clear roles and responsibilities help, one of the most effective ways to effect mindset shifts is by building risk-related objectives and key results (OKRs), such as open remediation activities and time to remediation, into performance management. These metrics have an even greater effect on mindsets when product owners have accountability for them; some companies even have them specifically sign and certify the scorecards.

6. Upskill and manage talent

While plenty of transformation funding goes to engineering and development, risk—particularly the second line of defense—rarely sees much of it. That neglect hamstrings the risk function and ultimately undermines the digital transformation itself. Building up a solid, digital-ready risk-and-compliance function requires investment in new hires and in upskilling existing talent. Acquiring the kind of talent that can balance risk and digital requires some creativity.

One US bank, for example, decided to hire former top tech architects and train them on risk. Upskilling people requires a clear understanding of the specific risk-control skills for which they need training and well-developed programs (for example, to train the trainers) to scale the training across the organization. A financial-services organization trained its product owners (the second line) to incorporate risk controls and processes into the team backlog. These people then became trainers and helped the first-line teams adopt key risk-management practices (such as version control and security checks) in their development process.

A successful transformation, risk controls included

A US bank realized it needed to become more digital, so it launched an enterprise-wide agile transformation across its business and technology functions. As leadership was creating the transformation blueprint, however, they spotted a big problem: the risk-control team wouldn't be able to keep up with the increased flow of products that the new agile teams would generate. So they pulled in a senior product owner from the second line to partner with the transformation team to reengineer risk processes to not only enable the transformation but also strengthen the business's overall risk posture.

One of the areas addressed was governance, which typically required more than 30 meetings to get the various approvals needed for each product. The team noticed that, in many of these meetings, the product team was asked the same questions, so they eliminated the redundant meetings. They also assigned a point person from risk to work with the product teams to identity risks, make remediation recommendations, and make sure risk was prioritized in the backlogs. Providing a single point of contact also greatly clarified who had risk responsibility—a big issue before—when there sometimes were as many as 40 to 60 stakeholders for a given product but no certainty about who was actually in charge.

To help manage the program, the transformation team deployed tools to reconfigure workflows so that they could be integrated with backlog tools such as Jira. These helped to clearly identify what risks needed to be addressed, who would address them, and when. As a result, everyone knew what to do, and the product owner had a single view into where progress was (or was not) being made.

To ensure that this process worked, the transformation team invested significant time in training. They trained people on the risk team on how to work in agile teams, how the new operating

model worked, and what the benefits of the new system were. They trained product teams on how to identify and remediate risk. The key point of this program, in addition to providing a basic theoretical explanation about how to address risk, was that it paired each product owner with a risk person for on-the-job training in which they worked closely together on real projects to address risk issues rapidly and effectively. The product owners could then help their own teams understand and address risk issues as well.

As a result of this approach, the bank's risk-approval timeline was reduced from roughly 180 days to around 40, while controls automation reduced the number of required artifacts by about 40 percent.

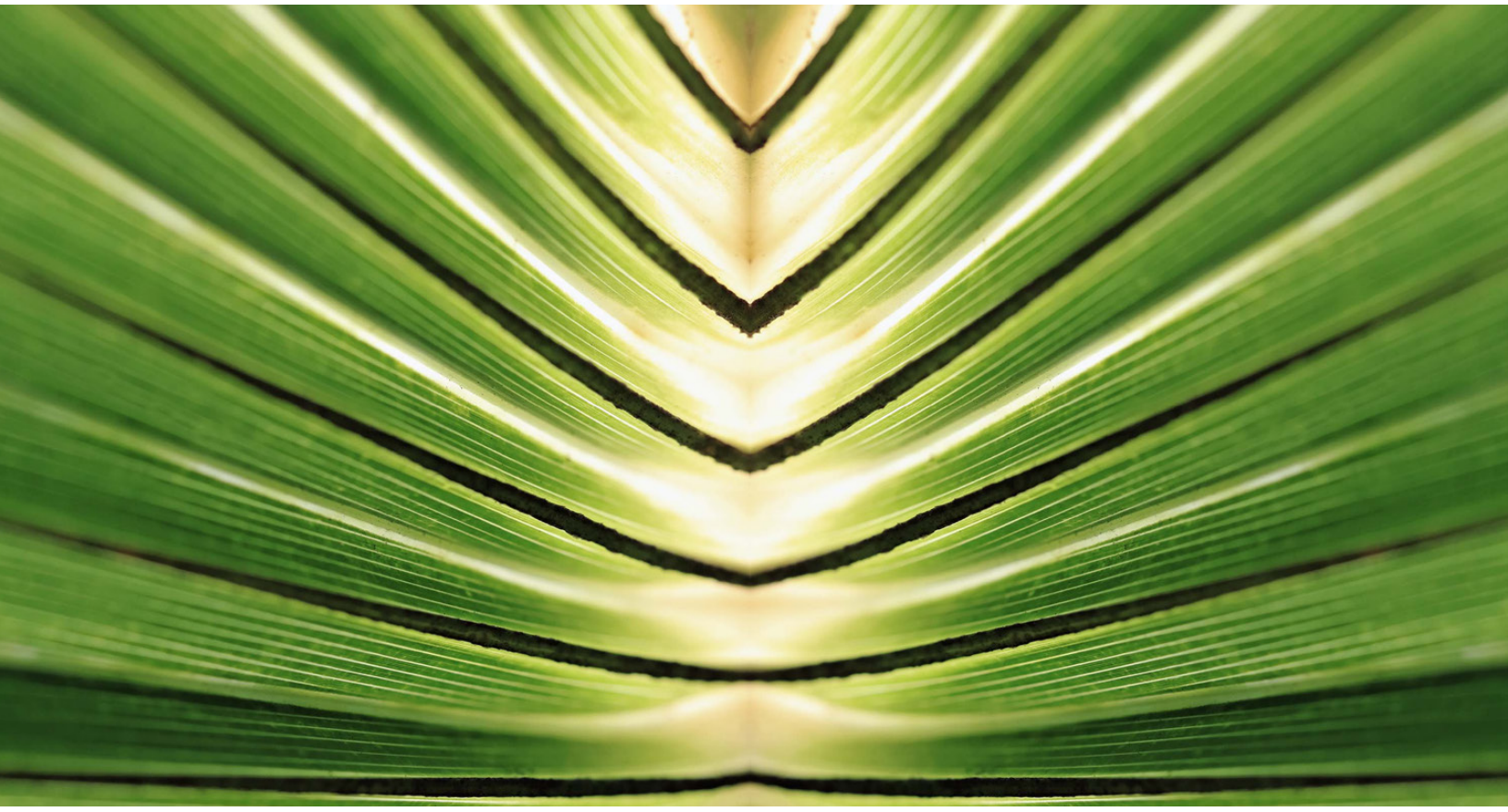
The days of "build it now and manage the risk later" are over. Risk is too important—not just for banks, but for any company that wants to become more digital. By taking a more comprehensive approach that treats risk as an enterprise-level issue, companies can not only avoid the fallout from poor risk practices but can actually accelerate their digital transformations.

Jim Boehm is a partner in McKinsey's Washington, DC, office; **Jan Shelly Brown i**s an associate partner in the New Jersey office; and **Lama Sabbagh** is an associate partner in the Toronto office, where **Karim Thomas** is a partner.

Aligning portfolios with climate goals: A new approach for financial institutions

Portfolio-alignment tools will help financial institutions chart more scientifically robust, realistic, and profitable climate strategies.

This article is a collaborative effort by Sudeep Doshi, Cindy Levy, Dickon Pinner, Carter Powis, and Dan Stephens, representing views from McKinsey's Financial Services, Risk & Resilience, and Sustainability Practices.



To achieve the goals of the Paris Climate Agreement and restrict further increase in global average temperatures to well below 2°C, human society needs to reach net-zero emissions of long-lived greenhouse gases by midcentury. To keep average global temperatures from rising more than 2°C between now and then, we will have to limit cumulative carbon emissions on the path to net zero to fewer than 1,000 metric gigatons; to prevent a rise of more than 1.5°C, no more than 400 metric gigatons can be emitted. Both targets require substantial near-term reductions in emissions levels, which are around 40 metric gigatons annually. To reach the 1.5°C target, the world must cut present emissions levels by two-thirds over the course of the next decade.[1]

This great transformation will only be possible if we replace, at scale, the global economy's productive asset base with nonemissive technologies. Financial institutions understand that the capital needs for this historic undertaking are enormous. Success in the transition to a net-zero society depends on the ability to keep capital flowing to emissive industries engaged in decarbonizing activities while redirecting funding away from activities that do not support the 1.5°C ambition.

The financial sector consequently needs appropriate tools and metrics to set climate targets and measure progress against them. In cooperation with leading financial institutions, McKinsey joined the Portfolio Alignment Team, set up by Mark Carney in his capacity as the UN special envoy for climate and finance. Our collective purpose has been to enable measurement of the relative alignment of investor and lender portfolios with the objectives of the Paris Agreement. We emphasize that these technical supports are being designed in ways that engage with counterparties and facilitate their transition. Only through engagement, rather than divestment, can we ensure the transition to a 1.5°C future.

The financed-emissions approach and its challenges

Today, the tool most widely used to measure climate impact across the global financial sector is the calculation of financed emissions. The concept of financed emissions is fairly straightforward. It begins when a financial institution invests in, lends to, or insures a company. That company goes on to produce emissions. The financial institution then accounts for a proportional fraction of that company's emissions in its own carbon footprint. The climate impact of a financial institution can be measured as the sum of the emissions it finances across all the companies in its lending book, investment portfolio, or insurance portfolio.

The financed-emissions calculations are an important and useful tool. The bulk of climate commitments made by financial institutions—now representing nearly $100 trillion in assets under management—are made in terms of financed emissions. Most infrastructure for managing and analyzing climate data produces these metrics.

The use of financed emissions creates three challenges related to the development of effective climate strategies, however. First, by calculating financed emissions, institutions can tell where they are now but not where they need to go. The physical science makes clear that attaining a warming limit of 1.5°C or 2°C is dependent both on achieving net-zero emissions and on limiting the cumulative amount of greenhouse gases we emit en route to the goal. To align with the ambition of the Paris Agreement, the world needs a climate strategy built around a total carbon budget, not only a net-zero target for some point in time.

The second challenge is the complexity of determining portfolio-level carbon. To achieve an effective net-zero transition, we must recognize that different geographies and sectors will need to decarbonize at different rates, based on their different capabilities and needs. Industries in developed economies must reduce emissions more quickly than the global average; financed emissions in portfolios focused on these economies can and should reflect the faster rate of decarbonization. For emerging economies and the portfolios focused on them, the rate will be necessarily slower. Failing to account for these crucial differences can lead to climate strategies that are impossible to carry out or inadequate to slow global warming.

[1] "Climate math: What a 1.5-degree pathway would take," *McKinsey Quarterly,* April 30, 2020.

To achieve an effective net-zero transition, we must recognize that different geographies and sectors will need to decarbonize at different rates.

The third challenge for the financed-emissions approach is that this metric would discourage financial institutions from funding decarbonization and the responsible retirement of existing emitting assets. By simply measuring emissions, institutions would be encouraged to avoid large emitters in favor of smaller emitters, taking no account of decarbonizing companies versus nondecarbonizers. Institutions extending financing to a rapidly decarbonizing emitter would raise their financed-emissions levels, negatively affecting their measured climate impact. Thus the approach would constrain the strategic space available, forcing a focus on green growth only while deprioritizing the greening of carbon-intensive assets. Yet right now, the transformation of carbon-intensive assets into green ones is a problem (and opportunity) at least as large and important as the fostering of new green growth.

The refined approach: Portfolio-alignment tools

In response to these challenges, the Portfolio Alignment Team has worked with leading institutions, method providers, and thinkers across the financial sector to codify a new approach to measuring climate impact: using portfolio-alignment tools. Portfolio-alignment tools are computational models that use forward-looking climate scenarios to estimate the division of the global carbon budget by sector and geography. This allows users to measure emissions performance along a trajectory rather than at points in time; it further permits measurement down to the level of each counterparty in the portfolio.

Portfolio-alignment tools can resolve the three challenges of the financed-emissions approach. First, financed emissions are evaluated in the context of a carbon budget or emissions trajectory. This helps institutions plot their course toward the Paris Agreement's goals. Second, the carbon budget or trajectory is built as a composite of the trajectories of the portfolio's constituent companies. The overall trajectory thus reflects a portfolio's unique sector and geographical composition. This helps reveal whether an institution's climate strategy is both achievable and sufficient for the collective goal. Third, the trajectory analysis allows financial institutions to differentiate between decarbonizing and nondecarbonizing companies. This frees financial institutions to extend decarbonization financing to high emitters—provided that they are achieving necessary climate progress by retrofitting, replacing, or retiring existing assets.

Portfolio-alignment tools thus provide much-needed context to financed-emissions metrics. In doing so, they can guide financial institutions in building climate strategies that are based on science, informed by economic and technological realities, and open to addressing the financing needs of decarbonizing companies.

The Portfolio Alignment Team was commissioned by the Task Force on Climate-Related Financial Disclosures to produce a survey and synthesis of existing best practices in building and using portfolio-alignment tools.[2]

[2] *Measuring portfolio alignment: Technical considerations,* Task Force on Climate-Related Financial Disclosures, 2021.

What the new approach means for financial institutions

Leaders of financial institutions know that this decade is critical for climate action. Portfolio-alignment tools can help facilitate needed changes to existing approaches to climate strategy and to decision-making processes. It is important, then, to begin thinking now about these changes, even though the tools are still very new.

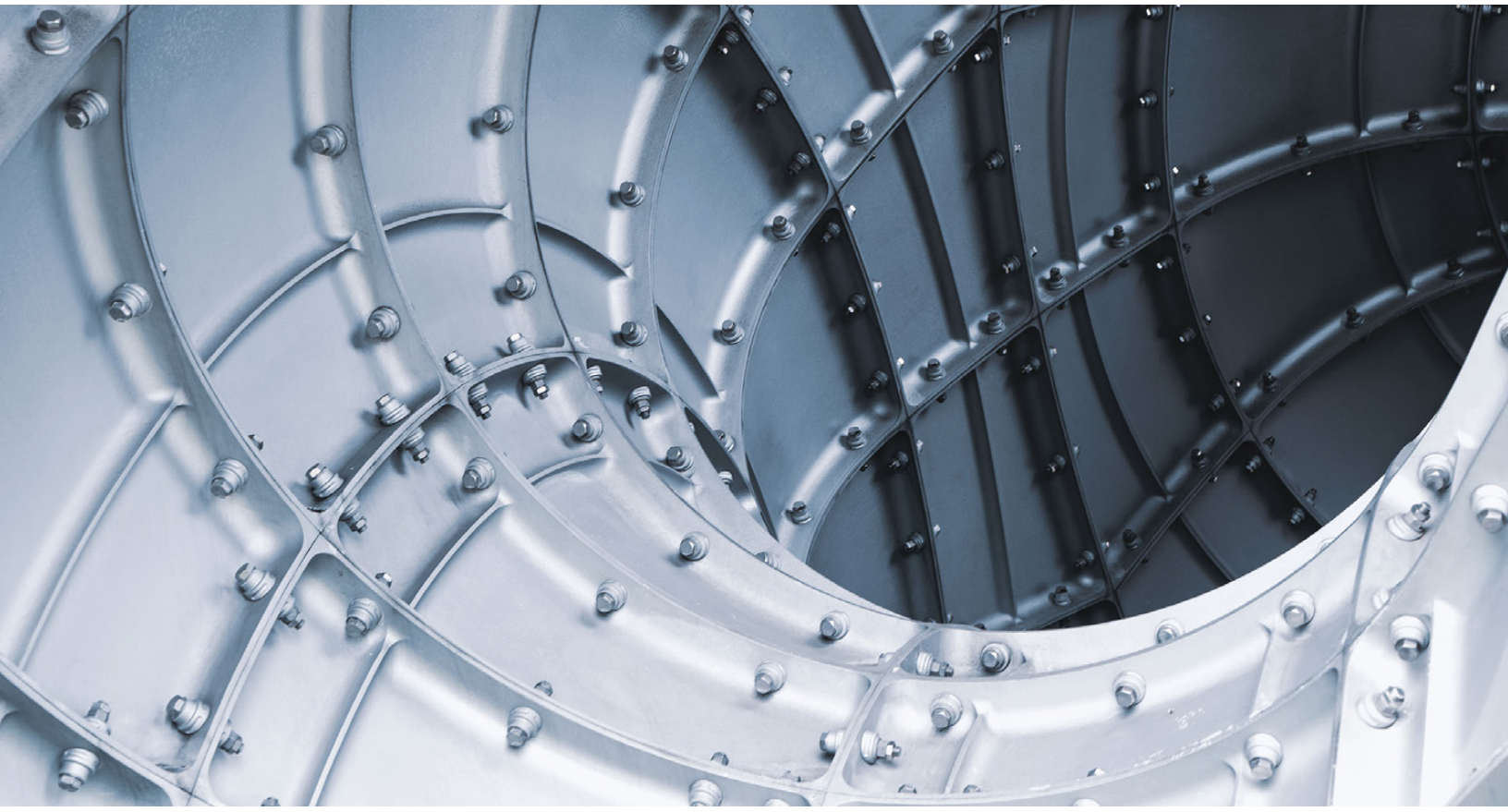
Commitments to cease financing in specific industries could, for example, be reconsidered. Portfolio-alignment tools give financial institutions the freedom to extend financing to heavy emitters, provided that the financing goes toward the responsible retirement or decarbonization of emitting assets and that the decarbonization or retirement is successfully achieved. It is also worthwhile to begin thinking about how to tell the portfolio-alignment story to shareholders, customers and regulators. The story is complicated but essential, because it reveals a clearer picture of the path we need to take to achieve the goals of the Paris Agreement. Leaders can also begin investing in improving the data environment and technical fidelity needed to support portfolio-alignment tools at scale.

Sudeep Doshi is a partner in McKinsey's New York office, **Cindy Levy** is a senior partner in the London office, **Dickon Pinner** is a senior partner in the San Francisco office, **Carter Powis** is a McKinsey external adviser and an alumnus of the Toronto office, and **Dan Stephens** is a senior partner in the Washington, DC, office.

Ransomware prevention: How organizations can fight back

Ransomware has rapidly become one of the top cybersecurity nightmares. Strategies for prevention, preparation, response, and recovery can help.

by Jim Boehm, Franz Hall, Rich Isenberg, and Marissa Michel



No one can deny ransomware has hit new levels of sophistication, with demands for payment skyrocketing into the tens of millions of dollars. The reasons are manifold. Some are straightforward: vulnerabilities posed by pandemic-weary organizations and workers logging in from unsecured home networks. Other reasons are highly complex, such as ever-increasing connectivity driven by advancing digitization. Still other reasons include threat actors who are committed to perfecting their craft—rather than the "smash and grab" approach, hackers are now "dwelling" undetected within victims' environments to better understand where the highest-value data and information are and then selling those data to other bidders. Finally, as the number of companies that are forced to pay ransoms to regain control of their networks and data increases, so does the number of hackers attracted to this type of lucrative threat.

To that end, Cybersecurity Ventures estimates ransomware costs should reach $265 billion by 2031.[1] Supply chain attacks rose by 42 percent in the first quarter of 2021 in the United States, affecting up to seven million people,[2] while security threats against industrial control systems (ICS) and operational technology (OT) more than tripled in 2020.[3]

Sometimes, when looking at the overall numbers, it is hard to grasp the reality of a ransomware attack's effect on a company. To put it in perspective, here are some specific costs: Colonial Pipeline paid a $4.4 million ransom after the company shut down operations, global meat producer JBS paid $11.0 million, and global insurance provider CNA Financial paid a reported $40.0 million. Additionally, a ransomware attack on US software provider Kaseya targeted the firm's remote-computer-management tool and endangered up to 2,000 companies globally. These figures do not reflect the additional costs of an attack, including paying third parties, such as legal, PR, and negotiation firms; the opportunity costs of having executives and specialized teams turn away from their day-to-day roles for weeks or months to deal with an attack and its aftermath; or the lost revenue that results. With the use of low-cost ransomware-as-a-service (RaaS) campaigns, this cyberthreat has surged beyond the quiet confines of the C-suite to where boards of directors, regulators, law enforcement, industry associations, insurance providers, and the cybersecurity vendor community all need to be a part of the solution.

While governments, law enforcement, and regulators continue to grapple with ransomware issues such as transparency and oversight of cryptocurrencies, companies need to ensure they remain resilient by focusing on ransomware prevention, preparation, response, and recovery strategies. The payment or nonpayment of a ransom could well depend on whether an organization masters the basics of these four strategies and then continues to build higher levels of cyber maturity that create a resilient environment where attacks may still occur but do not have the same effect they would otherwise.

Prevention

To achieve a secure work environment, you need to know what technology you have, as well as what and who it is talking to; then, watch it like a hawk. Vigilance is key. To get there, everyone from the board and C-suite down the line must be on the same page and treat security as a continuous endeavor that balances technology with people and processes to ingrain security into an organization's DNA.

To achieve that balance, organizations need to understand that 75 percent of ransomware breaches begin with either a phishing email or a Remote Desktop Protocol (RDP) compromise, according to Coveware's quarterly ransomware reports for the fourth quarter of 2020 and the first quarter of 2021. In addition, it appears that in 60 percent of ransomware cases, the malware

[1] David Braue, "Global ransomware damage costs predicted to exceed $265 billion by 2031," *Cybercrime Magazine*, June 3, 2021.
[2] Charlie Hart, "'Troubling' rise in supply chain cyber attacks," Supply Management, April 13, 2021.
[3] *ICS cybersecurity year in review 2020*, Dragos, 2021.

To achieve a secure work environment, you need to know what technology you have, as well as what and who it is talking to; then, watch it like a hawk.

ends up installed directly or via desktop-sharing apps, according to Verizon's 2021 *Data Breach Investigations Report (DBIR)*.[4] Such insights show how crucial cybersecurity hygiene is across an entire organization, from employees and vendors to third-party supply chains. It is the first line of defense in mitigating a cyberattack. Companies are finding success with the following tactics:

- *Securing all RDP.* COVID-19 saw workforces shift to work from home—and home networks are often rife with poor security. Solid basic hygiene would include strong passwords, multifactor authentication, software updates, restricted access, and network-level authentication.

- *Multifactor authentication (MFA).* MFA for critical assets and high-risk users is strongly recommended. This tactic can be a strong barrier for attacks that leverage credential-based access or privilege escalation like ransomware.

- *Patch management.* Legacy systems, whether OT or IT, chug along on old software with security gaps. After RDP and phishing attacks, vulnerable software is the next largest attack vector, which is why securing communication channels and patching Windows operating system exploits remain vital.

- *Disabling user-level command-line capabilities and blocking Transmission Control Protocol (TCP) port 445.* Ransomware threat actors run free or low-cost software and scanning tools, searching for things like credential harvesting and internal unsecured port discovery from command-line prompts. If command-line capabilities end up disabled, the company becomes a more difficult target. Additionally, blocking port TCP 445 on external-facing infrastructure and internal firewalls also helps reduce the attack surface.

- *Protect Active Directory.* Active Directory is a database and set of services that connects users with the network resources they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what.

- *Education and training.* Cyber awareness training and education should be mandatory. Not everyone needs to be to be a highly trained and skilled cybersecurity professional, but basic changes in behavior and awareness of where and how threats can enter your organization can further reduce risks.

Preparation

A core team—which includes senior leaders—that has worked to prepare for an attack is in far better shape to respond than one figuring it out on the fly. "The threat has really evolved from targeting big business to also targeting small and medium-size

[4] *2021 Data breach investigations report (DBIR)*, Verizon, January 2022.

businesses," says Greg Hughes, CEO of Veritas, in a recent McKinsey article about recovering from ransomware. So creating a business continuity plan and then practicing all types of scenarios will pay off. That approach includes the following:

— *Knowing your decision rights.* The timing, urgency, and stress of an attack escalate when decision rights are unclear. Who will lead the response team? Is the CEO directly involved or deliberately removed from the tactical details of response? After the business uncovers an attack, is the IT team fully empowered to take quick steps to stem the bleeding, regardless of business impact? And who will ultimately make the decision to pay and defend that decision internally and externally? Designate a person accountable for keeping the crisis response moving forward in a methodical and detailed manner and ensure decision trees end up aligned, from the chief information security officer (CISO) or chief security officer (CSO) to the CEO or response leader.

— *Preparing for all options and understanding negotiating constraints.* Prior to experiencing a ransomware attack, the majority of companies say they will not pay a ransom. However, when nearly two out of three organizations ended up victimized by a ransomware attack over the past 12 months, more than 80 percent paid the ransom demands, according to a 2021 report from Delinea on the state of ransomware. Constraints can range from the level of insurance coverage to whether customers' data are also at risk and premerger or preacquisition sensitivities. Given that these factors will change over time, ensure this view is refreshed periodically.

— *Getting your board up to speed.* Generally, board members will want to help and bring issues to closure—the success of which all comes down to communication. That is why the board and executive leaders need to engage in a critical conversation detailing roles and how to activate them. This level of communication and advanced planning can facilitate faster decision making and collaboration. Resiliency becomes baked in when cybersecurity becomes a joint capability between the board and executives and through all levels of the organization.

— *Enhancing resilience.* Business continuity answers the question, "How do we operate this process if a particular technology or person is disrupted?" Operational resilience targets the bigger question, "How do we organize such that a particular event does not disrupt us?" Companies should have answers to both questions to prepare for cybersecurity attacks.

There are quite a few tactical reasons why companies choose to pay, but they all stem from the same underlying concern: we are not confident that this attack will not disrupt us, so paying is the "safer" option.

Approaching ransomware prevention and preparedness from a resilience perspective frames the requirements and outcomes differently:

— Know which assets are important (crown jewels, critical assets) and where they live. This can not only help assess potential impact in a ransomware attack but also allows for better prioritization and spending policies for infrastructure and security investments.

— Know the backup process, which will help assess how feasible recovery is. It's also good data hygiene to only keep what you need.

— Recovery testing is always helpful. Testing in advance of disruption builds muscle memory, uncovers dependencies, and encourages creative thinking and problem solving.

— Practice—and knowing whether a system will be rebuilt (and how long that will take) or whether systems will failover to an alternate data center—builds confidence in the ability to minimize disruption.

Response

In a ransomware attack, time is of the essence, so collaboration and transparency prevail. When an organization becomes aware of a ransomware

attack, it should not compartmentalize the challenges ahead. The CISO or CSO needs to ensure transparency and collaboration with internal stakeholders across the company, including the board, C-suite, affected business groups, compliance and risk, and legal and crisis communications teams. However, your organization's network of external stakeholders can provide valuable input and help expedite risk-based decision making, such as the following:

- *Phone a friend.* An organization's first call should be to the FBI or a regional and supervisory law-enforcement agency for notification and disclosure. For very large financial institutions or companies managing and operating critical infrastructure, there is a broad range of law-enforcement agencies available to assist.

- *Proceed carefully.* The US Department of the Treasury's guidance on ransomware payments requires organizations to consult with them if they need to pay the ransom. However, since ransom payments could violate sanctions against certain individuals or designated organizations, the Treasury's Office of Foreign Assets Control and its Financial Crimes Enforcement Network say organizations could be held liable for ransom payments, even if they were unaware or unable to determine that the recipient is on a prohibited list.

- *Seek counsel and check insurance policies.* External counsel, as well as insurers, are significant partners to have at the table. From discerning who to notify and when, to working through the finer points of negotiation and possible implications and thinking through the legal requirements for customers and partners—especially third parties—these stakeholders bring practical benefits.

- *Expect pressure.* Some RaaS groups have call centers that will proactively reach out to down-stream customers and activist investors to put pressure on a victim to pay. Expect this and have a plan to engage stakeholders, whether proactively or in response to their queries.

- *Activate third-party partners.* Your response leader can serve as "air traffic control" to manage the responsibilities of all parties involved.

Remember that you are collaborating with criminals, so the closer a company gets to paying the ransom, the more it needs proof that the attackers actually have what they say they have.

— *Dig into forensics and intelligence.* In the earliest stages of the attack, use intelligence to determine who is behind the attack and how they were able to gain access and maintain persistence and detonate the malware. This knowledge will aid in understanding how bad the attack is and assist in decryption and negotiation.

— *Investigate alternatives to payment.* Attempt to locate or access known unencrypted shadow copies of data or even a decryption key using member institution initiatives to determine if their information can be decrypted without paying.

Recovery

No matter what, recovery from a ransomware attack can be messy. If you decide to pay and get a decryption key—and if it works—there is usually a considerable amount of cleanup because the attackers shut down servers and databases not designed to shut down hard. If you don't pay, rebuilding networks from backups is time consuming.

Indeed, the average downtime a company experienced after a ransomware attack is 21 days, according to a Coveware report. In addition, the average ransom fee requested increased from $5,000 in 2018 to about $200,000 in 2020, according to the National Security Institute. But keep in mind, the ransom requested depends on multiple variables like the company size, revenue, industry, and importance.

Also, remember, if an organization suffers an attack and feels it has to pay, the attacker now becomes a business partner, so keep these guidelines in mind:

— *Verify.* For attackers, ransomware is a business, and they want to keep their reputations intact. Remember, however, that you are collaborating with criminals, so the closer a company gets to paying the ransom, the more it needs proof that the attackers actually have what they say they have. Ask to see a sample.

— *Know what's up for debate.* For large and more mature institutions, forensic teams can generally figure out how to find or trigger the decryption key. In these cases, whether or not to pay the ransom depends on the at-risk data elements and how much a company is willing to pay to keep them from being destroyed or exposed.

Make no mistake about it, ransomware is ugly. But making your enterprise resilient by following prevention, preparation, response, and recovery strategies will allow a company to recover from attacks and not have to pay a huge ransom. Communication, advanced preparation, and understanding and then minimizing risk is the best way to keep the operation up and running.

Jim Boehm is a partner in McKinsey's Washington, DC, office, where **Marissa Michel** is a leader, Global Resilience and Response; **Franz Hall** is a senior adviser in the Stamford office; and **Rich Isenberg** is a partner based in Atlanta.

Model risk management 2.0 evolves to address continued uncertainty of risk-related events

Organizations this year plan to enhance their MRM framework capabilities—including risk culture, standards, and procedures—and to upgrade their validation resources with MRM 2.0 firmly on the agenda.

by Pankaj Kumar, Marie-Paule Laurent, Christophe Rougeaux, and Maribel Tejada

The macroeconomic environment over the past year has been characterized by rising uncertainty, bouts of volatility and a sharp increase in event risk. These factors and an uneven economic recovery have motivated many financial institutions to leverage new analytics capabilities for a range of business processes. In parallel, the commercial landscape has continued to evolve amid accelerating digitization and a wave of acquisition activity that has led to the expansion of model inventories in both Europe and the United States.

Over the past year, McKinsey has invited groups of risk managers to come together to discuss the state of the art in risk modeling and model risk management (MRM). At roundtables and through our global MRM survey, we have gathered insights from institutions in Europe and the United States on a range of modeling challenges and opportunities.[1]

The outputs from our discussions shed light on the state of the art in bank MRM and reveal a range of themes that are likely to shape institutional approaches over the coming year. In particular, they reveal three key transformations: an increased focus on efficiency, digitization, and automation of the model life cycle; an expansion of the scope of MRM into new areas, including climate, cyber, sales and marketing, and even human resources; and a focus on derisking and maximizing the potential of artificial intelligence and big data. All of these have informed a range of strategic and tactical adjustments that will define the parameters of MRM in the year ahead.

Transforming efficiency, digitization, and automation of the model life cycle

In response to an increasingly complex economic and business environment and the powerful economic impact of the COVID-19 pandemic, many banks have expanded their model inventories over the recent period. US banks have seen as much as a 25 percent jump in number of models since 2019, while European institutions report a 13 percent rise. Still, the process remains a challenge. In Europe, initial validation for Tier 1 models takes 20 weeks on average, while Tier 2 and Tier 3 models take 13 and nine weeks, respectively. For periodic validation, the timelines are 11 weeks, six weeks, and four weeks, respectively. In the United States, the validation timelines are typically lower across banks, with initial validation for Tier 1 models taking 12 weeks, while Tier 2 and Tier 3 models take six and four weeks, respectively. For periodic validation, the timelines are, on average, seven weeks, five weeks, and four weeks, respectively.

As activity has ramped up, banks report that costs in areas including inventory management, reporting, and risk-limit setting have risen. In response, a large number have taken steps to improve the efficiency of the MRM function. Team leaders have tried to ensure that overlaps and redundancies are minimized, processes are optimized, and risk-based approaches are operationalized across the organization.

With capacity pressure rising, automation has become an increasingly urgent priority, supported by ever-more standardized workflows. Commonly cited benefits of automation include increased effectiveness (more consistency and rigor across activities) and greater efficiency (for example, freeing up of model validation capacity).

In Europe, the most automated process among survey respondents is ongoing monitoring and testing, particularly for models subject to frequent testing, followed by periodic validation testing. There is no particular variance across model types. Looking forward, the highest priority is automation of MRM workflows, followed by automation of validation, testing, and documentation. US banks are also focused on automation of MRM workflows, as well as managing validation frequency for some models. Many report they have acted to align validation depth with model tiers.

Still, many banks report that automation remains at an early stage, with automated testing and standardized codes used sporadically rather than over the whole model life cycle. Indeed, despite advancements over the past year, 50 percent of

[1] McKinsey–RD MRM Survey, 2021.

European banks have yet to commence automation across all model life cycle activities. No more than 30 percent of the group report automation being fully implemented in any single function. Among US banks, 60 percent are prioritizing automation of development and validation activities for models subject to frequent testing or documentation activities. Second in line are models sharing a similar methodology. Across banks, manual inputs are still most dominant in model documentation and initial validation documentation.

Effective automation is contingent on clear standards across model types. However, many banks are constrained by challenges in implementing tiering effectively, which is a precondition of setting the right standards for different levels of materiality. Looking ahead, the priority for many is to focus on the next level of automation, which is to put in place dedicated teams to drive efficiency. Time-consuming tasks such as documentation and reporting are high on executive agendas.

Enhanced standards

Many banks report that they have started the process of introducing more granulated standards for MRM, including drafting model-specific or tier-specific documents, prioritized by risk exposures, regulatory needs, and the potential for reputational damage. Among other efficiency initiatives, roundtable participants highlighted the migration to model life cycle digitization and the positive effects of cloud transformation programs, with efficiency benefits again seen as significant—or at least potentially so. However, these kinds of transformations also bring challenges. Life cycle digitization is tough in the absence of strong data processes (collection, quality, and management), the lack of which can undermine repeatability and reproducibility. In addition, the broad scope and continuous evolution of model families requires frequent adaptions, a task complicated by the common involvement of multiple stakeholders across functions and lines of defense as well as the need for senior stakeholder buy-in.

Roundtable participants agreed that the appropriate response to these challenges is to ramp up MRM team capabilities, with many now seeing this as a priority. Cloud migration was also commonly described as a potentially important enabler but was seen as contingent on high levels of standardization and process simplification. In addition, many banks said that they required a risk-based approach to tiering. With these building blocks in place, it may be possible to achieve an "automation leapfrog," putting the program at the top of the strategic agenda and working to automate across the board.

Finally, in building out their digital capabilities, increasing numbers of banks reported moving

In building out their digital capabilities, increasing numbers of banks reported moving toward an agile approach, characterized by short sprints, test-and-learn environments, and program flexibility.

toward an agile approach, characterized by short sprints, test-and-learn environments, and program flexibility. Key enablers for agile methodologies include a unified technology platform for data and systems and the use of advanced IT tools to capture model information on the fly. This approach may comprise proactively screening data warehouses and analytics platforms, telemetry, and alternative approaches to information capture. Once these are in place, perceived advantages include better consistency and reproduction in reporting, efficiency gains through a refocus on high-value activities, and faster turnarounds. Several banks said they are increasingly reliant on external data, which requires more management attention but can produce excellent analytical outcomes.

Empowering MRM in new areas

One driver of inventory expansion over the past two years has been the emergence of a range of new use cases. Those categories include emerging risks related to cyber, climate, and COVID-19, as well as the redevelopment of other categories to cater to structural market changes. The emergence of the new secured overnight financing rate is one example. Moreover, there is a consensus that the validation burden will rise over the next two years amid higher levels of demand in areas such as climate and AI.

Against this backdrop, a large number of institutions have worked to recalibrate their organizational setups and have expanded mandates to widen the scope of MRM. There has been a wave of investment in new tool kits and validation approaches to support risk-management activities. A common trend in the EU has been for banks to divide their MRM resources into two primary teams, with one focusing on regulatory models and the other tasked with the remainder. Another dominant trend has been to elevate oversight at senior levels. To that end, many banks have started to incorporate model risk in their broader assessments of risk appetite. Indeed, 81 percent of European banks have formulated a statement of risk appetite for model risk. This shows the growing importance that institutions attach to the subject and a high level of C-suite engagement in setting tolerances.

Statements of risk appetite are often based on standard types of metrics. The most common are the quality of models, compliance with MRM policy, and risk capital add-ons. Banks commonly use a score card to put a number on risk and provide a benchmark for reporting. When it comes to model risk capital, many European banks report subsuming the cost under operational risk capital, with a sizeable minority assigning the budget to margin of conservation frameworks. One in four holds no specific capital against model risk.

To ensure effective oversight at all levels, the majority of banks in both Europe and the United States have centralized their MRM and validation functions (the United States for some time now)—albeit split into regulatory and nonregulatory capabilities. European banks report adding support through colocated teams or, less commonly, localized teams. A few have adopted a hybrid federated and localized approach to MRM. For model development, the vast majority of banks operate teams that are fragmented across business and model types. However, around 28 percent of European banks have set up single or multiple centers of excellence, for example in credit risk, market risk, and AI/machine learning (AI/ML).

Heads of MRM and validation often have different reporting lines, particularly in Europe, with validation heads seeing more variance than others. In the United States, MRM reports tend to be directly to the chief risk officer or another senior executive on risk committees. The challenge amid this mix of approaches, beyond meeting regulatory expectations, is to raise skill levels to match the diversity and range of models and to ensure that validators become de facto “risk managers” in the way they approach their work.

Across most banks, MRM policies and standards are typically shared between the first and second line of defense (LoD) in about equal measure, with operations and technology teams taking responsibility for end user computing, alongside operational risk management. However, given the events of the past year, across geographies, a majority of MRM teams are planning to work closely with the first LoD to assess the effects of the

As AI and ML have become core elements of the tool kit, many banks have worked to manage risks through enhanced model governance, validation frameworks, and more powerful knowledge capabilities.

COVID-19 pandemic on models and standards, with a focus on model performance-monitoring activities.

As banks develop their internal standards, they are aware that the regulatory burden is set to intensify. Many participants in the US roundtable highlighted recent discussions on the Office of the Comptroller of the Currency's MRM Handbook and the interagency statement on MRM for Bank Secrecy Act and Anti-Money Laundering (BSA/AML) compliance. They noted that, in practice, the effect is likely to be largest on small and medium-size banks. Discussions highlighted continuing uncertainty about how best to meet supervisory expectations for governance of non-model tools.

Derisking and maximizing the potential of AI/ML and big data

One of the most exciting areas of innovation in modeling is in artificial intelligence, machine learning (ML), and deep learning, the development of which has enabled banks to ask more nuanced questions of much larger data sets. As a result, risk areas such as financial-crime compliance and cyber have become much more amenable to interrogation. Sales and marketing has also been a key beneficiary, with banks able to analyze customer data to offer a more streamlined and tailored proposition.

As AI and ML have become core elements of the tool kit, many banks have worked to manage risks (data ethics, black box, biases) through enhanced model governance, validation frameworks, and more powerful knowledge capabilities, supported by training where appropriate. Many have built or acquired digital tools and infrastructure to ensure they maximize the value of advanced modeling techniques. Banks also reported a heightened regulatory focus, which reflects the extent of potential ethical and reputational risks associated with complex models.

Many roundtable participants said they had ramped up efforts to enhance AI/ML model definitions. However, a large number still need to tackle AI validation standards and tools, as well as the deficit in AI talent. In addition, there are practical challenges in the use of AI. For example, when it comes to financial-crime compliance models, banks need to pay close attention to their obligations under regulations such as the European Union's General Data Protection Regulation. Regulators are often not fully prepared for new models and lack the frameworks or responsible persons to make full assessments, bankers said. The same kinds of challenges are presented by climate models, where colleagues may have an intimate understanding of risk but are not acquainted with the data and methodologies that support modeling. This implies the need for a more flexible approach to validation so that development in these fast-evolving areas can proceed in parallel.

Often in AI use cases, a lack of historical data can inhibit comparability. Roundtable participants emphasized that validation approaches might initially require flexibility and pragmatism, reflecting

the fact that the data in AI models and frequency of calibration are different from traditional models. Given the novelty of AI use cases, the flexibility enabled by agile approaches was seen as a good match.

The number of AI models varies across banks globally, with some using 60 or 70 (or as many as 290 at the margins) while others are comfortable with ten or 15. However, in Europe, 60 percent of banks plan to develop at least ten AI/ML models in the next two years, and 30 percent plan to validate at least ten models next year, our survey shows.

The emergence of AI and its use cases has brought a distinct set of challenges, described by some market participants as "cultural." At a minimum, new use cases require an agile or interactive-engagement model for the first and second LoD, as well as the early involvement of support functions such as legal and IT. Roundtable participants highlighted the advantages of a dedicated support structure and of securing strong sponsorship, which should be accompanied by a tailored risk-based approach to validation and review. In addition, bankers acknowledged the need to foster validation awareness among modeling teams, many of which are populated by data scientists who are unfamiliar with validation protocols. With that in mind, one task is to clearly define standards and expectations, supporting deeper collaboration between modeling teams in the nonregulatory space and validation.

One of the primary roles for MRM teams is to define explainability requirements for the first LoD, alongside working to enhance monitoring standards. At larger banks, MRM teams are often required to benchmark AI/ML models against simpler approaches. Among common initiatives, banks have updated their model definitions, provided new guidelines to the first LoD, and renewed their governance frameworks. Still, institutions report being at varying stages of planning and implementation. In addition, there are still distinctive gaps in coverage. For example, most banks do not have defined roles for assessment of bias.

Looking to the year ahead, bankers cited two key priorities: to enhance their MRM framework capabilities (including risk culture, standards, and procedures) and to upgrade their validation resources. "MRM 2.0" is firmly on the agenda, which for many banks will mean getting to the next level of reporting and KPIs, strengthening risk appetite frameworks, and embedding good governance and the right culture. Culture is seen to be particularly important at senior levels so that decision makers fully understand the potential risks and impacts that models—and analytics in general—may bring. These efforts should be built on the three pillars of increased efficiency, supported by digitization, a more empowered MRM function, and advancements in the use of AI. In a world that continues to be defined by uncertainty, much work—but also much opportunity—lies ahead.

Pankaj Kumar is a partner in McKinsey's New York office, **Marie-Paule Laurent** is a partner in the Brussels office, **Christophe Rougeaux** is an associate partner in the Boston office, and **Maribel Tejada** is a senior expert in the Paris office.

McKinsey Risk & Resilience Practice

Global coleader and North America
Fritz Nauck
Frederic_Nauck@McKinsey.com

Global coleader and Europe
María del Mar Martínez
Maria_Martinez@McKinsey.com

Asia–Pacific
Gabriele Vigo
Gabriele_Vigo@McKinsey.com

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

Latin America
Elias Goraieb
Elias_Goraieb@McKinsey.com

CEO, Risk Dynamics
Andreas Kremer
Andreas_Kremer@McKinsey.com

Chair, Risk & Resilience Editorial Board
Thomas Poppensieker
Thomas_Poppensieker@McKinsey.com

Coleaders, Risk Knowledge
Luca Pancaldi and Lorenzo Serino
Luca_Pancaldi@McKinsey.com and
Lorenzo_Serino@McKinsey.com

In this issue

Three keys to a resilient postpandemic recovery
From risk management to strategic resilience
Financial institutions and nonfinancial risk: How corporates build resilience
Lessons from banking to improve risk and compliance and speed up digital transformations
Aligning portfolios with climate goals: A new approach for financial institutions
Ransomware prevention: How organizations can fight back
Model risk management 2.0 evolves to address continued uncertainty of risk-related events

April 2022
Designed by McKinsey Global Publishing

McKinsey.com