McKinsey & Company

McKinsey on Risk

New risk challenges and enduring themes for the return

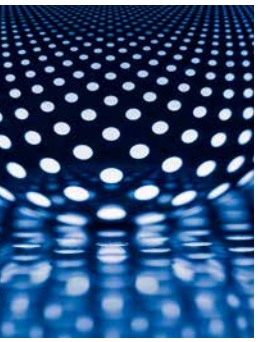
Number 9, June 2020

McKinsey on Risk is written by risk experts and practitioners in McKinsey's Global Risk 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:
© boonchai wedmakawand/Getty Images

Table of contents



3 **Responding to coronavirus: The minimum viable nerve center**

Amid the coronavirus pandemic, companies need a crisis response coordinated by top management that gives experts and managers the autonomy to implement creative, pragmatic solutions.

11 **Supply-chain recovery in coronavirus times—plan for now and the future**

Actions taken now to mitigate impacts on supply chains from coronavirus can also build resilience against future shocks.

19 **How banks can ease the pain of negative interest rates**

With better governance and data collection, treasurers can stanch the effects of margin erosion.

27 **Banking imperatives for managing climate risk**

More than regulatory pressure is driving banks to manage climate risk. Financing a green agenda is also a commercial imperative—but specialized skills are needed to protect balance sheets.

35 **The future of operational-risk management in financial services**

By partnering with the business, the operational-risk discipline can create a more secure and profitable institution. Here's what has to happen first.

46 **The investigator-centered approach to financial crime: Doing what matters**

The investigator-centered approach to fighting financial crime fosters collaboration among banks, law-enforcement agencies, and regulators for greater effectiveness, efficiency, and social impact.

57 **The consumer-data opportunity and the privacy imperative**

As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage.

66 **Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity**

New cyberrisk management information systems provide executives with the risk transparency they need to transform organizational cyberresilience.

Introduction

Our ninth issue of *McKinsey on Risk* arrives amid the greatest global crisis since the Second World War. McKinsey and the Risk Practice have been in constant conversation with healthcare, public-sector, and business leaders to help assess and meet the diverse challenges raised by the COVID-19 pandemic. As we go to press, confirmed cases are counted in the millions, deaths in the hundreds of thousands. Countries and regions struggle with the asymmetrical damage and continue to ramp up testing and treatment as the race to develop and distribute an effective vaccine takes its marathon course.

The spread of the virus led ultimately to near-universal disruption of the global economy as country after country applied preventative restrictions on movement. Then, where the infection rate appeared to fall below the danger level, restrictions were incrementally lifted. As the world's leading companies resume full operations, they need to tackle the immediate challenges raised by the crisis and address the principal risk areas affecting performance.

McKinsey on Risk is our premier publication presenting McKinsey's global perspective and strategic thinking on risk. In this issue, two articles describe enduring lessons that emerged directly from the struggle against the pandemic. One discusses the "minimum viable nerve center," a leadership approach to steering effectively through a fast-moving situation impervious to familiar remedial actions. The second, showing how supply chains can recover after the crisis, explains that actions companies take to mitigate the immediate damage can also build resilience against future shocks.

Two pieces present timely considerations for financial institutions. One discussion, recognizing that banks must operate in a low-interest environment for the foreseeable future, reveals how they can reduce the pain of eroding margins through better governance and data collection. A further discussion explores the regulatory and commercial demands on banks to manage climate risk—one of the steepest challenges our societies will ever face. The authors dissect the specialized skills that banks will need to finance the green agenda while protecting the balance sheet.

The theme of nonfinancial risk is a recurring one for financial institutions. We present two important considerations here. One describes the pathway to the future state of operational-risk management—a future defined by the risk function's close partnership with the business. A second discusses a new, highly productive and efficient way to prevent financial crime. This novel approach, which shifts the focus from regulatory compliance toward the interception of proscribed transactions, is led by a collaborative investigative team.

Further articles discuss important topics in the management of cyberrisk. One reveals how the regulatory requirements for data protection can become a source of business advantage for companies willing to offer customers greater privacy. In a final consideration, our authors explore a superior risk-based approach to cybersecurity and how it must be supported by enhanced cyberrisk reporting.

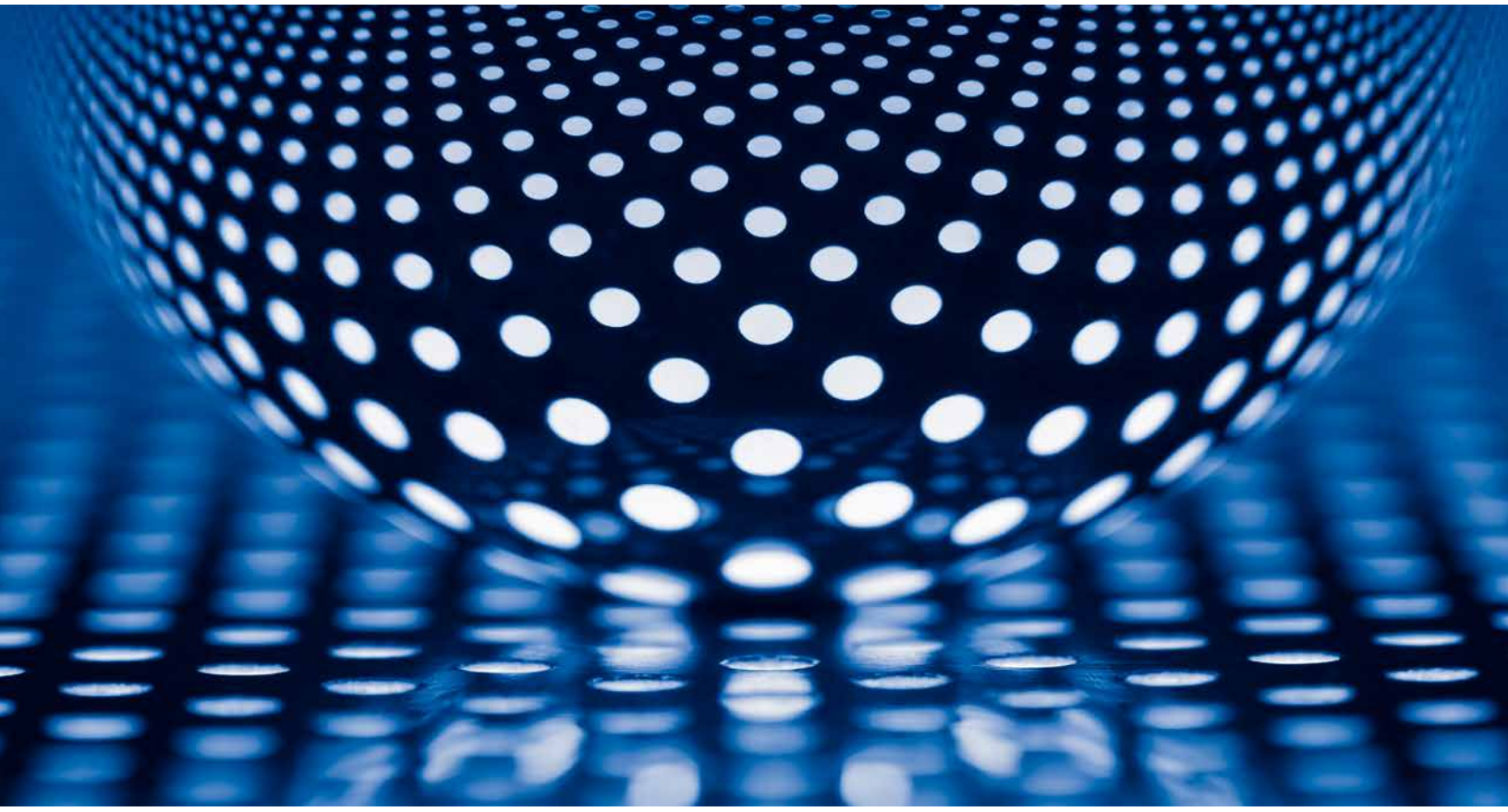
In facing both immediate and enduring risk-management challenges, our experts take a global view across business sectors and functions. The industry insights they offer reflect the hands-on experience of companies' steering through the current crisis and transforming risk management for the future. Let us know what you think, at McKinsey_Risk@McKinsey.com and on the McKinsey Insights app.

Thomas Poppensieker
Chair, Global Risk Editorial Board

Responding to coronavirus: The minimum viable nerve center

Amid the coronavirus pandemic, companies need a crisis response coordinated by top management that gives experts and managers the autonomy to implement creative, pragmatic solutions.

by Mihir Mysore and Ophelia Usher



The COVID-19 outbreak, caused by the coronavirus (SARS-CoV-2), is a deep humanitarian crisis that has also gravely affected the global economy. It is posing difficult—even unprecedented—challenges for business leaders. They are finding that the fast-moving situation is impervious to familiar remedial actions. By the time a response is mounted, the situation has changed, and the scale, speed, and impact of issues have unexpectedly intensified. Leaders everywhere have experienced some form of such disruption, though the magnitude of the present crisis is trying the lessons of human experience. The struggle to avoid ineffective, reactive approaches has consequently been all the more difficult.

Together with many leading companies, we have developed a better approach—a flexible structure for guiding the work—called the integrated nerve center. In an unfamiliar crisis, such as the COVID-19 outbreak, the nerve center concentrates crucial leadership skills and organizational capabilities and gives leaders the best chance of getting ahead of events rather than reacting to them.

The integrated nerve center is not a formulaic panacea. It is, rather, an efficient means of coordinating an organization's active response to a major crisis. It is endowed with enterprise-wide authority and enables leaders and experts to test approaches quickly, preserve and deepen the most effective solutions, and move on ahead of the changing environment. In hundreds of discussions conducted in the past few weeks, we have looked at the efforts of many companies now in the process of building COVID-19 nerve centers. We feel that the insights of this common experience are of wide and pressing importance.

Discover, decide, design, deliver: Lessons from past crises

Common crisis-management failures arise according to the demands of the crisis, which can be understood in a fourfold manner. The first task of crisis management is to discover the current situation and form an accurate view of how it might evolve, deriving implications for the organization. From discovery, leaders must move on to decide on and design the necessary immediate and strategic actions, speedily establishing a pragmatic, flexible operating model. This model is ideally based on adequate stress testing of contextualized hypotheses and scenarios. It should also adhere to company and societal values. Finally, companies must deliver the solutions in a disciplined and efficient way, with enough built-in flexibility to accommodate late pivotal changes. In real crises, things go awry in each of these four categories:

— *Inadequate discovery.* This is a failure to invest in an accurate, full determination of

In an unfamiliar crisis, the nerve center concentrates crucial leadership skills and organizational capabilities and gives leaders the best chance of getting ahead of events rather than reacting to them.

the depth, extent, and velocity of the crisis. Companies typically reflect an optimist bias in initial assessments, for example, and then in subsequent reassessments as well. Eventually the false hopes embodied in these inaccurate assessments become obviously insupportable, at which point, however, the crisis has worsened, and much valuable time and resources have been wasted.

— *Poor decision making.* Most poorly handled crises are defined by poor decision making. Bad decisions can result from many causes, such as acting on incomplete information (action bias). In our experience, reluctance to act until "all the facts are in" is a more common fallacy. The tendency for decision makers to analogize a new and unfamiliar situation to past experience (pattern recognition) is another serious pitfall. Groupthink and political pressure commonly lead decision makers astray. Reputations—and sometimes, compensatory incentives—are often at stake in large, expensive projects. Consequently, undue pressure can be exerted to push through an unforeseen problem whose resolution is disregarded or seen as insufficiently important to revise timelines and budgets. Relatively minor arising technical issues can, by this dynamic, become major problems and even lead to catastrophic failures.

— *Constrained solution design.* Many crises have one or more technical causes—the problem in itself—that must be addressed with tailored solutions. These solutions must be either newly invented or imported to a new domain. Responding organizations must not allow themselves to be constrained by poor or inadequate solution designs. The immediate technical solution for diagnosing COVID-19—the starting point for treatment solutions—is the effective test. A type of test known as polymerase-chain-reaction (PCR) testing, developed in China, Europe, and South Korea for the disease, has become the standard for effective testing and is now being produced at scale around the world. The test was first produced in Germany in January 2020, not long after COVID-19 appeared in China. Yet in the United States, the presence of an ineffective test delayed the adoption of the effective one for a crucial early period in the spread of the virus.

— *Delivery failure.* For anyone with actual experience in handling a crisis, execution failure is a constant risk. Small contingent (random) failures can cause larger failures of the most well-thought-out plans. Faulty solutions can command undue loyalty from managers suffering from "operations addiction": instead of recognizing the root problem, responsible parties look for patches to preserve the flawed response. Chaotic conditions will necessarily cause disruptions, but the presence of accountable leaders with good judgment and the freedom to act and improvise as needed can minimize execution delays and failures.

Responding organizations must not allow themselves to be constrained by poor or inadequate solution designs.

The COVID-19-response structure

The nerve center is designed to resolve these four challenges under the heavy pressures of a major crisis. Certainly, companies and institutions are facing such a crisis with the COVID-19 outbreak, which has triggered travel restrictions, border closings, supply-chain disruptions, and work stoppages across the globe. The exhibit shows one example of a COVID-19-response structure.

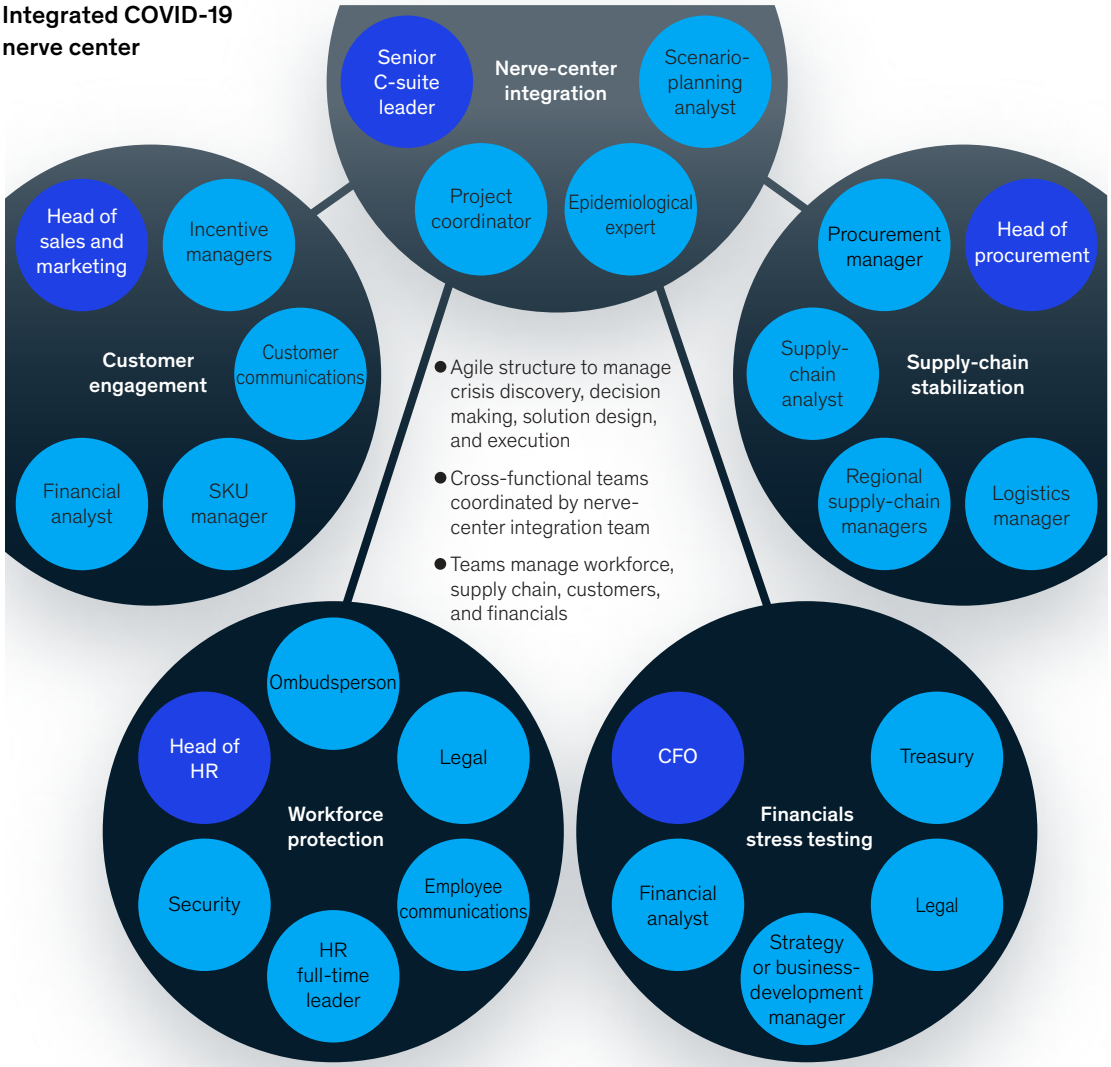
In this example, the nerve-center structure is organized around five teams, each responsible for a number of work streams. It is designed as an agile structure, coordinated through an integration team, but there is enough autonomy of action granted to constituent team leaders to work through bottlenecks and keep the response moving.

Nerve-center integration team

The nerve-center integration team is the coordinating head of the larger nerve-center structure. Its purpose is to set the overall tone of the COVID-19-response work, acting as a single source of truth, in real time, for all information and

Exhibit

The integrated COVID-19 nerve center is based on five cross-functional teams.



actions related to the outbreak and response. It must maintain close two-way communication with all teams. It is headed by a senior C-suite leader and includes an epidemiological expert, a project coordinator, and a scenario-planning analyst. The organization should empower this team to command whatever resources it deems are necessary to integrate closely and accomplish the work of the other four teams. The team's responsibilities can be summarized as follows:

— acting as the single source of truth for issue resolution

— ensuring that sufficient resources are deployed where and when needed

— coordinating the portfolio of remedial actions across the work streams of all teams, based on scenarios and triggers

— aligning team leaders on scenarios, with the help of roundtables and other exercises as needed

Workforce protection

For most organizations, business as usual cannot be expected to reign during the COVID-19 outbreak. Organizations need to develop a plan to support employees that is consistent with conservative health and safety guidelines. The plan must be flexible enough to accommodate policy changes as needed through the outbreak. It is useful for companies to compare their efforts in this domain with the actions that other organizations of similar size are taking, to determine the right policies and levels of support for their people.

The most helpful workforce-protection models provide clear, simple language to local managers on how to deal with COVID-19 that is consistent with the guidelines provided by WHO, national health organizations (such as the US Centers for Disease Control and Prevention), and local health agencies. The model should provide managers with a degree of autonomy sufficient to allow them to deal with any quickly evolving situation. Free two-way communication is also important so that managers can monitor adherence to policies as they evolve and employees can safely express their reservations about personal safety, as well as any other concerns.

The recommended workforce-protection team includes the head of HR (team leader); the HR full-time leader; representatives from security, legal, and employee communications; and the ombudsperson. The workforce-protection team is charged with the following work streams:

— developing brief policy papers, issue-escalation criteria and call trees, and actions (including preventative actions), as needed

— managing multichannel communications, including confidential feedback and reporting channels

— aligning policies and incentives for third-party and real-estate contractors

— establishing or maintaining communications platforms to enable employees to work from home (necessary infrastructure includes a virtual private network, telephony, and broadband readiness), including, as appropriate, deployment of collaborative software tools to enable video and audio conferencing, screen sharing, "whiteboarding," polling, chat, and other interactive capabilities

— helping manage productivity, using such means as staggered work times; respecting social-distancing norms; and instituting health checks

— developing "issue maps" and clear ownership and deadlines for issue resolution

— engaging with local, state, and national political leaders and health officials

Supply-chain stabilization

Companies need to define the extent and likely duration of their supply-chain (including tier-one, -two, and -three suppliers) exposure to areas that are experiencing community transmission and their inventory levels. Most companies are now primarily

focused on immediate stabilization, given that, in China (where few new COVID-19 cases are being reported), most plants are now restarting. In addition to supporting supplier restarts, companies should explore bridging strategies, including supply rationing, prebooking logistics capacity (shipping, rail, and airfreight), using after-sales stock, and gaining higher-priority status from suppliers. Companies should plan to manage supply for products that may be subject to unusual spikes in demand as they come back on line. In some cases, longer-term stabilization strategies may be necessary. Here, companies will have to use updated demand planning, optimize their networks further, and identify new suppliers. These approaches may be generally warranted to ensure enduring supply-chain resilience against risks beyond COVID-19, once the crisis is over.

The supply-chain-stabilization team will include the head of procurement (team leader), the procurement manager, a supply-chain analyst, the regional supply-chain managers, and the logistics manager. This team will manage four work streams:

— ensuring risk transparency across tier-one, -two, and -three suppliers; supporting supplier restarts; managing orders; and ensuring the qualifications of new suppliers

— managing ports, prebooking logistics capacity, and optimizing routes

— identifying critical parts, rationing parts as needed, and optimizing locations

— developing scenario-based sales and operations planning for SKU-level demand and managing the planning for production and sourcing

Customer engagement

Companies that truly navigate through disruptions often succeed because they invest in their core customer segments and anticipate those segments' needs and actions. In China today, for example, while consumer demand is down, it has not disappeared—far from it. People have dramatically shifted toward online shopping and ordering for all types of goods, including for food and produce delivery. Companies should invest more in online channels as part of their push for multichannel distribution. The investment should include ensuring the quality and delivery of goods sold online. Keep in mind, too, that changing customer preferences may not return to preoutbreak norms.

The customer-engagement team will include the head of sales and marketing (team leader), a financial analyst, and managers for customer communications, customer incentives, and SKUs. The customer-engagement team will manage three work streams:

— communicating to B2B customers (through a dedicated site) and developing scenario-based risk communications

— intervening as needed across the customer journey to prevent leakage, training customer-facing employees, and monitoring customer-service execution

— developing customer communications about COVID-19 situations and practices, as well as fact-based reports on COVID-19-related issues

Financials stress testing

Companies need to develop business scenarios tailored to their own contexts. Experts using analytics can define the values for the critical variables that will affect revenue and cost. Companies should model their financials (cash flow, profit and loss, and balance sheet) in each scenario and identify triggers that might significantly impair liquidity. For each trigger in each scenario, companies should define moves to stabilize the organization. Such moves could include optimizing accounts payable and receivable, cost-reduction measures, and divestment or M&A actions.

The financials-stress-testing team will include the CFO (team leader), the leader of strategy or business development, the leader of treasury, a representative

from legal, and one or more financial analysts. The team will manage two work streams:

— developing relevant scenarios based on the latest epidemiological and economic outlooks

— assembling relevant financials data according to different scenarios, especially working-capital requirements

Getting started quickly: The minimal viable nerve center

A common pitfall in nerve-center design is needless complexity. A good way of avoiding this is to aim at a minimal viable nerve center. Companies taking this approach quickly assemble the bare essentials needed to get operations up and running. The core nerve-center group, which might include all the team heads, will shape the structure, as needed, as the crisis evolves. Experience points to four essential elements that should be put in place right away.

Nerve-center organization

The teams need to be staffed quickly, with individual roles, responsibilities, and accountabilities made clear. Flexibility will be an important principle, since roles will change over time, sometimes quite rapidly. Also important is that nerve-center leaders be authorized to make timely decisions, sometimes without the opportunity to syndicate with other leaders.

Operating cadence

Meetings should be limited to those in which vital deliberations are conducted and actions decided on. They should, however, be frequent enough to foster collaboration. Ensure that meetings address essential topics and elicit the best thinking for the relevant work streams. The responsible members for each work stream should have the opportunity to seek input from the coordinating leaders. Solutions should be tested and decisions made to commit to effective methods and set aside ineffective ones. Select meeting attendees with care: Meetings of only senior leaders tend to encourage purely upward reporting rather than constructive debate and real problem solving. Meetings with too many frontline managers and individual contributors can become overly focused on tactical issues rather than the central problems. The difficulty of a high-quality operating cadence lies in maintaining a basic underlying structure and then allowing flexibility so that the organization can pivot when it needs to.

Issue identification

The nerve center will first identify the critical issues present in each work stream, with the expectation that these will evolve over time. Issues should be described in an issue map for risks and threats. In their totality, these maps will represent the core problem statement for the crisis situation and allow the group to articulate and address the challenges clearly and relatively quickly. The mapping can be divided between immediate, addressable risks and unforeseen, arising threats. Risk maps can be longer and more comprehensive; threat maps, however, can address the biggest issues—those that could drive significant disruption as the crisis continues.

Some known COVID-19 risks, such as those posed to traveling employees, could be readily addressed with policies (such as travel restrictions). Unforeseen threats that could arise as the crisis continues can be anticipated in "premortem" workshops. Nerve-center teams therein work out possible responses—ones to take if, for example, a sudden gap should open in the supply chain because of policies imposed beyond the company's control.

Once companies establish a good understanding of the critical issues across all work streams, they will find it helpful to run financial calculations (balance sheet, cash flow, and profit and loss) on issues and responses. This will project scenarios for particular issues, allowing companies to form views on issue likelihood, timing, and magnitude.

Response plan

Leaders can find it extremely difficult to craft sensible goals during a crisis. Many trade-offs usually have to be made between ideal outcomes and the many real constraints the organization

faces. Once more realistic goals reflecting the trade-offs are arrived at, they can be assigned a few milestones and key performance indicators (KPIs) so that progress toward them can be tracked in simple ways.

Additional elements

A few other elements can become helpful as the nerve center evolves. For the COVID-19 crisis, these could include common operating pictures, giving a single view on the current status of the response; KPI dashboards, to confirm whether or not hoped-for outcomes are being achieved; and listening posts, which are early-warning indicators that can point out forthcoming changes in the trajectory of a crisis.

The cultural challenge

The hard truth about effective business leadership is that leaders operate within powerful cultural and social contexts. The largest organizations, with hundreds of thousands of employees, might appear, in normal business conditions, to operate according to a command-and-control structure. The reality is more complex. While large organizations use many top-down, pyramid-like structures and processes, these work only when outcomes are predictable. On the other hand, routinized ways of working impede the creativity and flexibility that organizations need to respond at speed amid a crisis.

The exhibit of the integrated-nerve-center structure we have offered is not meant as a precise instruction manual. It is a general outline in need of contextual tailoring from organization to organization. The form described is most applicable to large corporations with global supply chains. For financial institutions, the structure would give little prominence to supply-chain stabilization and much more weight to financials stress testing. The structure is, however, adaptable for any large organization and can be effectively deployed in any crisis. From a business standpoint, the COVID-19 outbreak is a particular kind of crisis, quite different from those affecting a single large, multinational company. Rather, it is more like the financial crisis of 2008 to 2009, in that it presents as a shock to the greater part of all global economic activity: all the more reason that organizations need to concentrate leadership and capabilities in a fast-acting, integrated nerve center.

With senior-leadership support and participation, the nerve-center structure can provide the organizational parameters that companies need to navigate through the disruptions caused by the COVID-19 outbreak. The approach works because it enables a coordinated response led by top management while also giving experts and managers the autonomy they need to implement creative, pragmatic solutions.

Mihir Mysore is a partner in McKinsey's Houston office; **Ophelia Usher** is an expert in the New York office.

The authors wish to thank Kevin Carmody for his contributions to this article.

Supply-chain recovery in coronavirus times—plan for now and the future

Actions taken now to mitigate impacts on supply chains from coronavirus can also build resilience against future shocks.

by Knut Alicke, Xavier Azcue, and Edward Barriball

Even as the immediate toll on human health from the spread of coronavirus (SARS-CoV-2), which causes the COVID-19 disease, mounts, the economic effects of the crisis—and the livelihoods at stake—are coming into sharp focus. Businesses must respond on multiple fronts at once: at the same time that they work to protect their workers' safety, they must also safeguard their operational viability, now increasingly under strain from a historic supply-chain shock.

Many businesses are able to mobilize rapidly and set up crisis-management mechanisms, ideally in the form of a nerve center. The typical focus is naturally short term. How can supply-chain leaders also prepare for the medium and long terms—and build the resilience that will see them through the other side?

What to do today

In the current landscape, we see that a complete short-term response means tackling six sets of issues that require quick action across the end-to-end supply chain (Exhibit 1). These actions should be taken in parallel with steps to support the workforce and comply with the latest policy requirements:

1. *Create transparency* on multitier supply chains, establishing a list of critical components, determining the origin of supply, and identifying alternative sources.
2. *Estimate available inventory* along the value chain—including spare parts and after-sales stock—for use as a bridge to keep production running and enable delivery to customers.

Exhibit 1

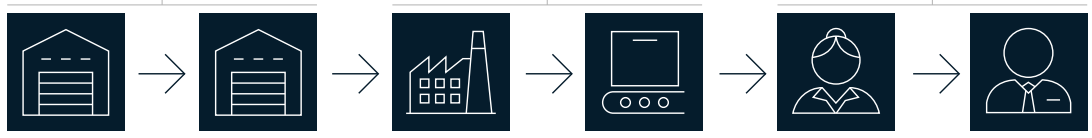
There are multiple immediate, end-to-end supply-chain actions to consider in response to COVID-19.

Supply-chain actions

Create transparency on multitier supply chain
- Determine critical components and determine origin of supply
- Assess interruption risk and identify likely tier-2 and onward risk
- Look to alternative sources if suppliers are in severely affected regions

Optimize production and distribution capacity
- Assess impact on operations and available resource capacity (mainly workforce)
- Ensure employee safety and clearly communicate with employees
- Conduct scenario planning and assess impact on operations, based on available capacity
- Optimize limited production, according to human-health impact, margin, and opportunity cost/ penalty

Assess realistic final-customer demand
- Work with sales and operations planning to get demand signal to determine required supply
- Leverage direct-to-consumer channels of communication
- Use market insights/external databases to estimate for customer's customers



Estimate available inventory
- Estimate inventory along the value chain, including spare parts/ remanufactured stock
- Use after-sales stock as bridge to keep production running

Identify and secure logistics capacity
- Estimate available logistics capacity
- Accelerate customs clearance
- Change mode of transport and prebook air/rail capacity, given current exposure
- Collaborate with all parties to leverage freight capacity jointly

Manage cash and net working capital
- Run supply-chain stress tests vs major suppliers' balance sheets to understand when supply issues will start to stress financial or liquidity issues

3. *Assess realistic final-customer demand* and respond to (or, where possible, contain) shortage-buying behavior of customers.

4. *Optimize production and distribution capacity* to ensure employee safety, such as by supplying personal protective equipment (PPE) and engaging with communication teams to share infection-risk levels and work-from-home options. These steps will enable leaders to understand current and projected capacity levels in both workforce and materials.

5. *Identify and secure logistics capacity,* estimating capacity and accelerating, where possible, and being flexible on transportation mode, when required.

6. *Manage cash and net working capital* by running stress tests to understand where supply-chain issues will start to cause a financial impact.

In the following sections, we explore each of these six sets of issues.

Create transparency

Creating a transparent view of a multitier supply chain begins with determining the critical components for your operations. Working with operations and production teams to review your bills of materials (BOMs) and catalog components will identify the ones that are sourced from high-risk areas and lack ready substitutes. A risk index for each BOM commodity, based on uniqueness and location of suppliers, will help identify those parts at highest risk.

Once the critical components have been identified, companies can then assess the risk of interruption from tier-two and onward suppliers. This stage of planning should include asking direct questions of tier-one organizations about who and where their suppliers are and creating information-sharing agreements to determine any disruption being faced in tier-two and beyond organizations. Manufacturers should engage with all of their suppliers, across all tiers, to form a series of joint agreements to monitor lead times and inventory levels as an early-warning system for interruption and establish a recovery plan for critical suppliers by commodity.

In situations in which tier-one suppliers do not have visibility into their own supply chains or are not forthcoming with data on them, companies can form a hypothesis on this risk by triangulating from a range of information sources, including facility exposure by industry and parts category, shipment impacts, and export levels across countries and regions. Business-data providers have databases that can be purchased and used to perform this triangulation. Advanced-analytics approaches and network mapping can be used to cull useful information from these databases rapidly and highlight the most critical lower-tier suppliers.

Combining these hypotheses with the knowledge of where components are traditionally sourced will create a supplier-risk assessment, which can shape discussions with tier-one suppliers. This can be supplemented with the described outside-in analysis, using various data sources, to identify possible tier-two and onward suppliers in affected regions.

For risks that could stop or significantly slow production lines—or significantly increase cost of operations—businesses can identify alternative suppliers, where possible, in terms of qualifications outside severely affected regions. Companies will need to recognize that differences in local policy (for example, changing travel restrictions and government guidance on distancing requirements) can have a major impact on the need for (and availability of) other options. If alternative suppliers are unavailable, businesses can work closely with affected tier-one organizations to address the risk collaboratively. Understanding the specific exposure across the multitier supply chain should allow for a faster restart after the crisis.

Estimate available inventory

Most businesses would be surprised by how much inventory sits in their value chains and should estimate how much of it, including spare parts and remanufactured stock, is available. Additionally,

after-sales stock should be used as a bridge to keep production running (Exhibit 2).

This exercise should be completed during the supply-chain-transparency exercise previously described. Estimating all inventory along the value chain aids capacity planning during a ramp-up period. Specific categories to consider include the following:

— *finished goods* held in warehouses and *blocked inventory* held for sales, quality control, and testing

— *spare-parts inventory* that could be repurposed for new-product production, bearing in mind the trade-off of reducing existing customer support versus maintaining new-product sales

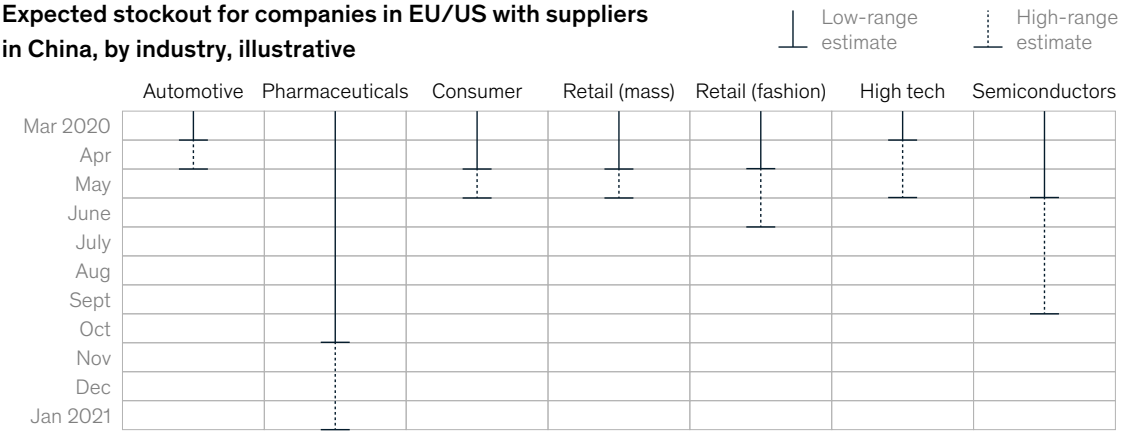
— *parts with lower-grade ratings or quality issues,* which should be assessed to determine whether the rework effort would be justified to solve quality issues or whether remanufacture with used stock could address supply issues

— *parts in transit*, which should be evaluated to find ways to accelerate their arrival—particularly those in customs or quarantine

Exhibit 2

Built-in inventory in the supply chain will delay the full impact of halted production.

Expected stockout for companies in EU/US with suppliers in China, by industry, illustrative



Inventory, days of stock (including supply in transit)

	Automotive	Pharmaceuticals	Consumer	Retail (mass)	Retail (fashion)	High tech	Semiconductors
2nd-tier supplier	30–40 (China)	35–70 (China)	20–30 (China)	N/A	N/A	40–60 (China)	N/A
1st-tier supplier	7–17 (EU/US)	120–140 (EU/US)	60–90 (China)	60–90 (China)	15–35 (China)	55–70 (China)	70–110 (China)
Assembly/ packaging	2–12 (EU/US)	55–100 (EU/US)	10–17 (EU/US)	10–17 (EU/US)	15–29 (EU/US)	19–45 (China)	60–90 (Philippines)
RDCs[1]	N/A	80–90 (EU/US)	14 (EU/US)	15–17 (EU/US)	15–23 (EU/US)	N/A	N/A
Market buffer	0–30 (EU/US)	N/A	N/A	7 (EU/US)	21–28 (EU/US)	24–40 (EU/US)	20–30
Total inventory days[2]	40–70	230–320	60–90	70–100	70–110	40–100	130–200

[1] Regional distribution centers.
[2] Figures for total inventory buffer and expected stockout are calculated assuming production stop at latest link based in China.

— *supply currently with customers or dealers*, which should be considered to see if stock could be bought back or transparency could be created for cross-delivery

Assess realistic final-customer demand

A crisis may increase or decrease demand for particular products, making the estimation of realistic final-customer demand harder and more important. Businesses should question whether demand signals they are receiving from their immediate customers, both short and medium term, are realistic and reflect underlying uncertainties in the forecast. The demand-planning team, using its industry experience and available analytical tools, should be able to find a reliable demand signal to determine necessary supply—the result of which should be discussed and agreed upon in the integrated sales- and operations-planning (S&OP) process.

Additionally, direct-to-consumer communication channels, market insights, and internal and external databases can provide invaluable information in assessing the current state of demand among your customers' customers. When data sources are limited, open communication with direct customers can fill in at least some gaps. With these factors in mind, forecasting demand requires a strict process to navigate uncertain and ever-evolving conditions successfully. To prepare for such instances effectively, organizations should take the following actions:

— Develop a demand-forecast strategy, which includes defining the granularity and time horizon for the forecast to make risk-informed decisions in the S&OP process.

— Use advanced statistical forecasting tools to generate a realistic forecast for base demand.

— Integrate market intelligence into product-specific demand-forecasting models.

— Ensure dynamic monitoring of forecasts in order to react quickly to inaccuracies.

With many end customers engaging in shortage buying to ensure that they can claim a higher fraction of whatever is in short supply, businesses can reasonably question whether the demand signals they are receiving from their immediate customers, both short and medium term, are realistic and reflect underlying uncertainties in the forecast. Making orders smaller and more frequent and adding flexibility to contract terms can improve outcomes both for suppliers and their customers by smoothing the peaks and valleys that raise cost and waste. A triaging process that prioritizes customers by strategic importance, margin, and revenue will also help in safeguarding the continuity of commercial relationships.

Optimize production and distribution capacity

Armed with a demand forecast, the S&OP process should next optimize production and distribution capacity. Scenario analysis can be used to test different capacity and production scenarios to understand their financial and operational implications.

Optimizing production begins with ensuring employee safety. This includes sourcing and engaging with crisis-communication teams to communicate clearly with employees about infection-risk concerns and options for remote and home working.

The next step is to conduct scenario planning to project the financial and operational implications of a prolonged shutdown, assessing impact based on available capacity (including inventory already in the system). To plan on how to use available capacity, the S&OP process should determine which products offer the highest strategic value, considering the importance to health and human safety and the earnings potential, both today and during the future recovery. The analysis will draw on a cross-functional team that includes marketing and sales, operations, and strategy staff, including individuals who can tailor updated macroeconomic forecasts to the expected

impact on the business. Where possible, a digital, end-to-end S&OP platform can better match production and supply-chain planning with the expected demand in a variety of circumstances.

Identify and secure logistics capacity
In a time of crisis, understanding current and future logistics capacity by mode—and their associated trade-offs—will be even more essential than usual, as will prioritizing logistics needs in required capacity and time sensitivity of product delivery. Consequently, even as companies look to ramp up production and make up time in their value chains, they should prebook logistics capacity to minimize exposure to potential cost increases. Collaborating with partners can be an effective strategy to gain priority and increase capacity on more favorable terms.

To improve contingency planning under rapidly evolving circumstances, real-time visibility will depend not only on tracking the on-time status of freight in transit but also on monitoring broader changes, such as airport congestion and border closings. Maintaining a nimble approach to logistics management will be imperative in rapidly adapting to any situational or environmental changes.

Manage cash and net working capital
As the crisis takes its course, constrained supply chains, slow sales, and reduced margins will combine to add even more pressure on earnings and liquidity. Businesses have a habit of projecting optimism; now they will need a strong dose of realism so that they can free up cash. Companies will need all available internal forecasting capabilities to stress test their capital requirements on weekly and monthly bases.

As the finance function works on accounts payable and receivable, supply-chain leaders can focus on freeing up cash locked in other parts of the value chain. Reducing finished-goods inventory, with thoughtful, ambitious targets supported by strong governance, can contribute substantial savings. Likewise, improved logistics, such as through smarter fleet management, can allow companies to defer significant capital costs at no impact on customer service. Pressure testing each supplier's purchase order and minimizing or eliminating purchases of nonessential supplies can yield immediate cash infusions. Supply-chain leaders should analyze the root causes of suppliers' nonessential purchases, mitigating them through adherence to consumption-based stock and manufacturing models and through negotiations of supplier contracts to seek more favorable terms.

Building resilience for the future

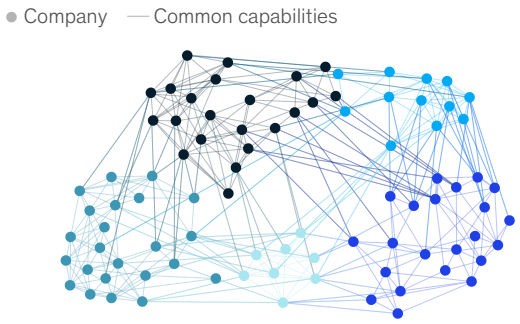
Once the immediate risks to a supply chain have been identified, leaders must then design a resilient supply chain for the future. This begins with establishing a supply-chain-risk function tasked with assessing risk, continually updating risk-impact estimates and remediation strategies, and overseeing risk governance. Processes and tools created during the crisis-management period should be codified into formal documentation, and the nerve center should become a permanent fixture to monitor supply-chain vulnerabilities continuously and reliably. Over time, stronger supplier collaboration can likewise reinforce an entire supplier ecosystem for greater resilience.

During this process, digitizing supply-chain management improves the speed, accuracy, and flexibility of supply-risk management. By building and reinforcing a single source of truth, a digitized supply chain strengthens capabilities in anticipating risk, achieving greater visibility and coordination across the supply chain, and managing issues that arise from growing product complexity. For example, Exhibit 3 shows how a digitally enabled clustering of potential suppliers shows the capabilities they have in common. Estimating a medtech company's degree of connectiveness helped it expand its supplier base by 600 percent, while an industrial-

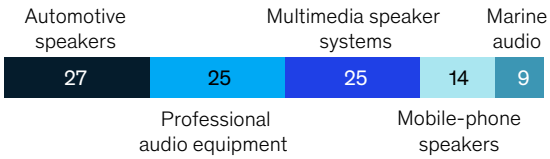
Exhibit 3

Cluster maps reveal alternative sourcing options for all the materials affected.

Cluster map, durable speaker suppliers, illustrative (n = 87 suppliers)



Cluster characteristics, %



tools maker identified request-for-qualifications-ready suppliers for highly complex parts that it had been previously unable to source.

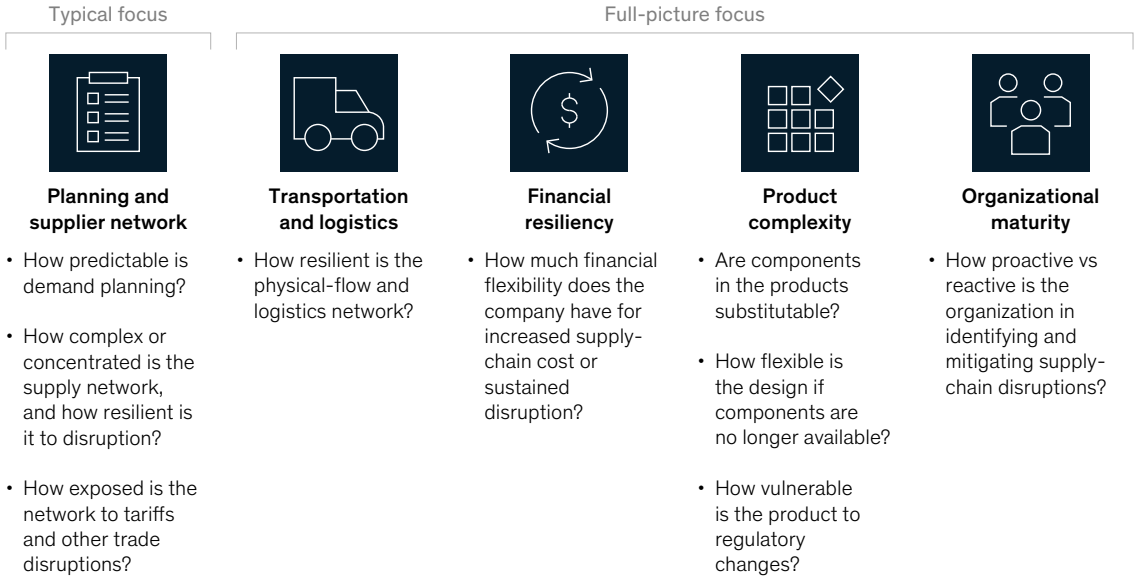
Finally, when coming out of the crisis, companies and governments should take a complete look at their supply-chain vulnerabilities and the shocks that could expose them much as the coronavirus has. Exhibit 4 describes the major sources of vulnerability. The detailed responses can reveal major opportunities. For example, using scenario analyses to review the structural resilience of critical logistics nodes, routes, and transportation modes can reveal weakness even when individual components, such as important airports or rail hubs, may appear resilient.

Organizations should build financial models that size the impact of various shock scenarios and decide how much "insurance" to buy through the mitigation of specific gaps, such as by establishing dual supply sources or relocating production. The analytical underpinnings of this risk analysis are

Exhibit 4

Supply-chain vulnerability occurs across five dimensions.

Drivers of potential vulnerability



well understood in other domains, such as the financial sector—now is the time to apply them to supply chains.

Triaging the human issues facing companies and governments today and addressing them must be the number-one priority, especially for goods that are critical to maintain health and safety during the crisis. As the coronavirus pandemic subsides, the tasks will center on improving and strengthening supply-chain capabilities to prepare for the inevitable next shock. By acting intentionally today and over the next several months, companies and governments can emerge from this crisis better prepared for the next one.

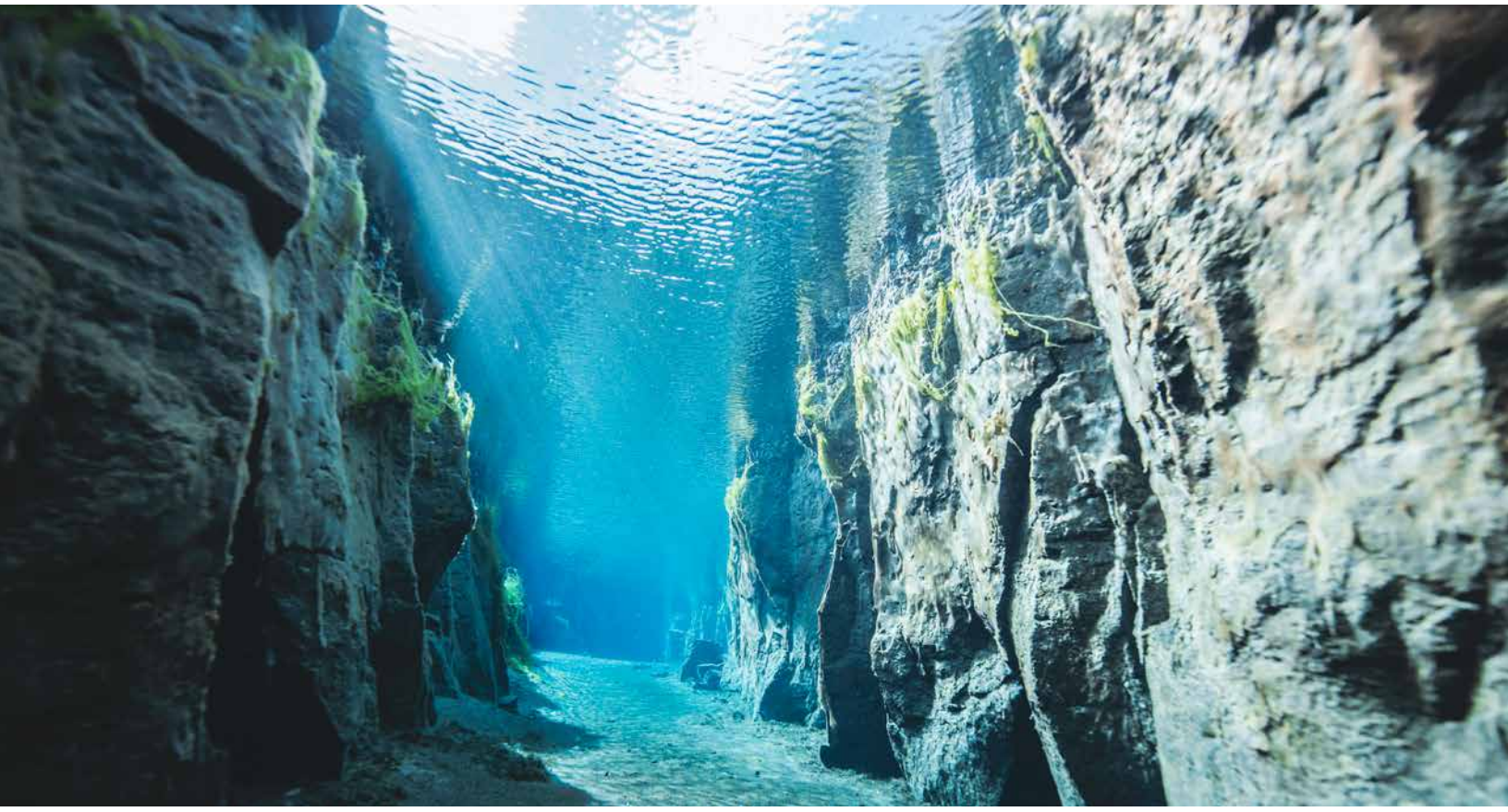
Knut Alicke is a partner in McKinsey's Stuttgart office, **Xavier Azcue** is a consultant in the New Jersey office, and **Edward Barriball** is a partner in the Washington, DC, office.

The authors wish to thank Viktor Bengtsson, Chris Chung, Curt Mueller, Hilary Nguyen, Ed Paranjpe, Anna Strigel, and Faaez Zafar for their contributions to this article.

How banks can ease the pain of negative interest rates

With better governance and data collection, treasurers can stanch the effects of margin erosion.

by Andreas Bohn, Olivier Plantefeve, Thomas Poppensieker, and Sebastian Schneider



By significantly reducing interest rates, central banks in Europe, Japan, and the United States have sought to stimulate economic activity, stabilize banking systems suffering from nonperforming loans, and manage exchange rates. A few have even pushed reference rates toward zero and below, while also undertaking quantitative easing in the form of bond-buying programs, to push down term rates as well. Against this background, central banks are contemplating broader and more intensive implementation of negative rates in case of a severe downturn.

While economies have benefited, low and negative interest rates come with strong side effects for investors and financial institutions. Over time, negative interest rates hurt profitability by eroding banks' net-interest margins. Japanese banks, for example, first saw net-interest margins increase as client rates on deposits were reduced faster than average rates on loans.[1] Soon thereafter, however, net-interest margins steadily declined as yields on loans and bonds acquired declined, pushed down by the Bank of Japan's quantitative-easing program. The increase in balance-sheet volumes did not offset the decline in net-interest margins.

Economists and business analysts expect that the present squeeze on margins is going to last at least five years, and probably more. Eurozone banks could face a margin decline of eight basis points. But there's good news too: treasurers may be able to mitigate most or all of the forecast depletion, through a combination of effective governance, a clear risk-appetite framework for hedging strategies, and IT and data reporting that achieves transaction-level transparency.

Since 2015, most banking sectors subject to negative-interest-rate policies have experienced a decline in net-interest margins (Exhibit 1).[2]

The impact on banks of negative-interest-rate policies varies according to the bank's business model. Smaller banks focused on domestic loans and deposits are often hurt more than larger banks, which tend to be more diversified across currencies and have a larger share of fee business. Banks of all sizes should prepare for the long-term effects of negative interest rates and quantitative easing by adopting a comprehensive program of countermeasures. Treasurers will be instrumental in designing and implementing these measures.

The components of net-interest margins

The main components of net-interest margins are structural elements, margins on assets, and margins on liabilities (which depend on the business model and regional setup) (Exhibit 2). The structural elements include benefits from maturity transformation, modeling and hedging the repricing tenor of the bank's own funds, and liquidity buffer income. They account for 15 to 35 percent of net-interest margin and decline due to flattening interest-rate curves and tighter credit spreads for bonds. The other two components—the margins on assets and liabilities—are more closely linked to client business.

Negative interest rates and quantitative easing create specific challenges for each component:

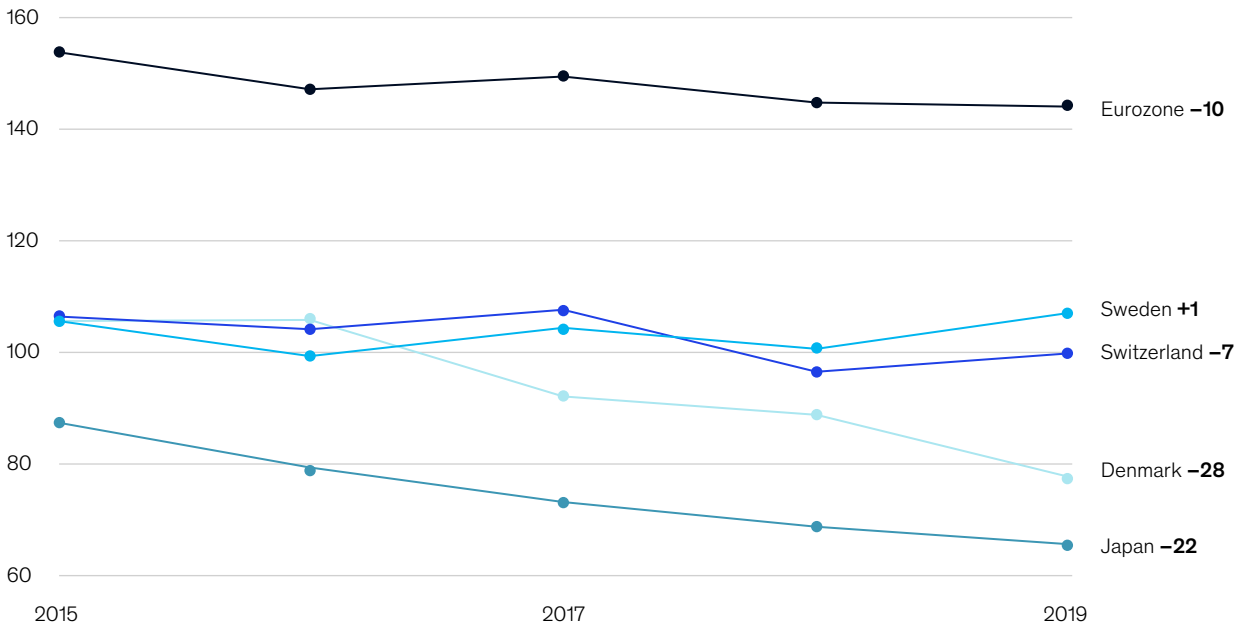
1. Structural elements. Banks have to hold significant amounts of high-quality liquid assets to fulfill requirements set by the liquidity-coverage ratio. These assets predominantly consist of central-bank reserves or government bonds that mostly have negative yields.[3] New regulatory requirements for term funding may extend the duration of liabilities requiring matching asset duration.[4] Furthermore, a flattened yield curve

[1] Christian Weistroffer, "Ultra-low interest rates: How Japanese banks have coped," DB Research, Deutsche Bank, June 10, 2013, dbresearch.com.
[2] The exception is Sweden, which has experienced healthy economic growth since 2014 with a robust mortgage market. Net-interest margins in the banking sector increased in Sweden during this period, and at the end of 2019, the Riksbank decided to lift its key reference rate (seven-day repo rate) back to zero (the rate for daily marginal deposits was set at –0.10 percent). See Qianying Chen, Mitsuru Katagiri, and Jay Surti, *Banking in a steady state of low growth and interest rates,* International Monetary Fund working paper, Number 18/192, August 2018, imf.org; Kerstin Bernoth and Alexander Haas, "Negative interest rates and the signalling channel," European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Monetary Dialogue, September 2018, europarl.europa.eu.
[3] The largest part of central-bank reserves receives negative interest rates although a minimum amount may be exempted. The tiering can be set as a multiple of the minimum reserve requirements or discretionally for an individual bank. Many government bonds, the most suitable alternative to central-bank cash, exhibit negative yields due to quantitative easing.
[4] Examples for regulatory term-funding requirements are the net stable funding ratio and the minimum requirements to issue eligible bail-in debt.

Exhibit 1

Net-interest margins mainly declined in economies subject to negative-interest-rate policies.

Net-interest margins, 2015–19, basis points

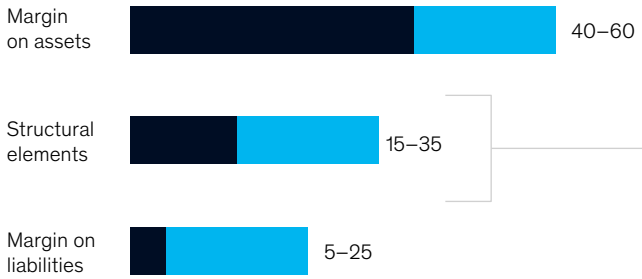


Source: European Banking Authority Risk Dashboard; SNL Financial

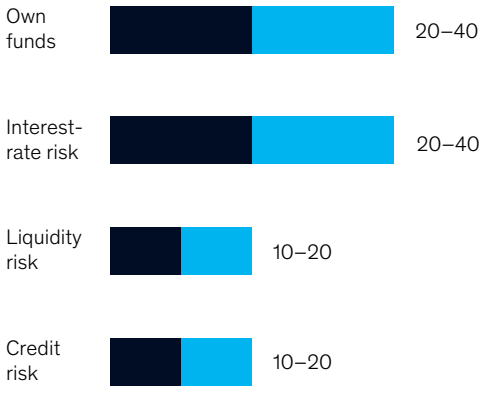
Exhibit 2

The three major components of net-interest margins are structural elements, margin on assets, and margin on liabilities.

3 major components of net-interest margins, %



Breakdown of structural elements, %



Source: Federal Financial Supervisory Authority (BaFin)—Deutsche Bundesbank

diminishes the benefits of maturity transformation. Additionally, the stability of new deposits—and hence their eligibility for maturity transformation—is uncertain.

2. Margin on assets. Banks accumulating excess liquidity from deposits have a particular incentive to increase lending to absorb this liquidity.[5] Some may increase their risk appetite for investments in securities and more risky loans, possibly compromising too much on the margin for term loans.[6]

3. Margin on liabilities. The ability to reprice deposits faster than assets helps at the beginning. While repricing corporate deposits below the zero boundary is feasible to some degree, retail deposits are more difficult to reprice, because deposits would become inferior to cash holdings. In addition, banks tend to experience significant inflows of client deposits.[7]

Even if interest rates remain stable over the next five years, the impact of negative rates will continue to squeeze net-interest margins, especially the structural elements. Consequently, the net-interest margin for banks in the eurozone could decline by another 8 basis points during this period. If the interest-rate curve were to move down another 50 basis points, the net-interest margin would drop by a further 8 basis points—or more—depending on the reaction of banks and clients (Exhibit 3).[8]

The treasurer's role in building resilience

Bank treasurers can play a central role in countering the impact of negative interest rates. They can do this by taking action in the following areas: identify and understand all relevant risks; implement measures to shore up and stabilize the components of net-interest margins, including the structural and client-related elements; and actively cooperate with top management to help steer the business in the negative-interest-rate environment.

Capturing risks

To identify and understand all relevant risks, treasurers need reporting systems that capture, model, and simulate interest-rate, funding, and liquidity risks. The IT and data architecture for reporting should create transaction-level transparency across legal entities. With these systems in place, treasurers can take these important actions:

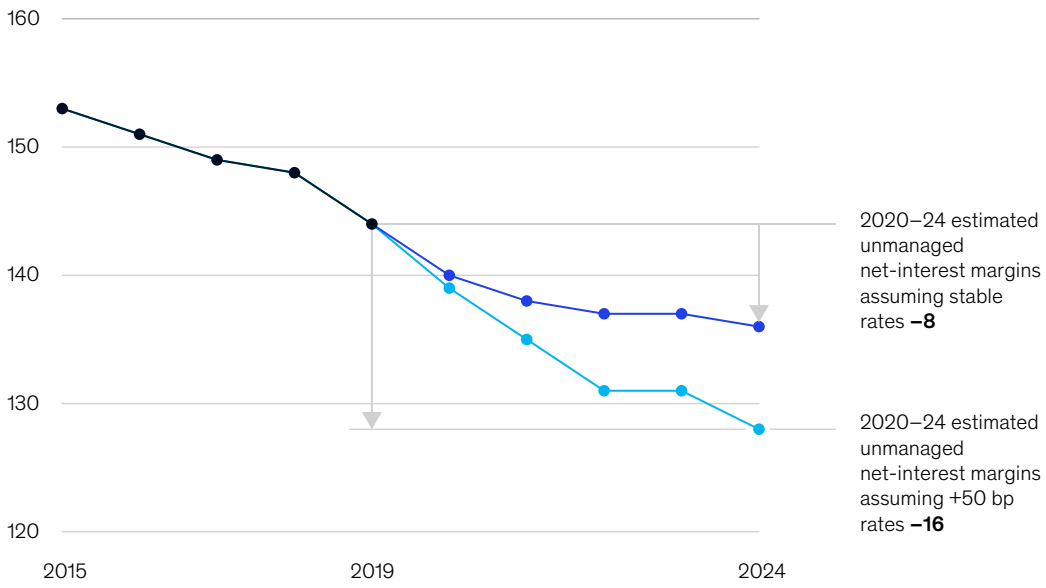
- Choose a sufficiently long time horizon (such as five years) for capturing the impact of negative rates on net-interest margins and the balance sheet.
- Assess the impact of political, legal, or reputational risks, such as the implied zero percent floor for retail deposit and mortgage rates.
- Review the dynamics of pension and insurance risks due to changes in interest rates and the interplay with inflation rates, credit spreads, and longevity.
- Identify the characteristics of implicit and behavioral options, such as prepayment risk in loans and attrition risk in deposits, even if they are not accounted at fair value. Quantify the risk arising from negative convexity in the balance sheet positions (when bond prices move in the same direction as interest rates).

[5] Selva Demiralp, Jens Eisenschmidt, and Thomas Vlassopoulos, *Negative interest rates, excess liquidity and retail deposits: banks' reaction to unconventional monetary policy in the euro area,* European Central Bank working paper 2283, May 2019, ecb.europa.eu.
[6] Florian Heider, Farzad Saidi, and Glenn Schepens, *Life below zero: bank lending under negative policy rates,* European Central Bank working paper 2173, August 2018, ecb.europa.eu.
[7] Carlo Altavilla, Lorenzo Burlon, Mariassunta Giannetti, and Sarah Holton, *Is there a zero lower bound? The effects of negative policy rates on banks and firms,* European Central Bank Working Paper 2289, June 2019, ecb.europa.eu.
[8] For similar results, see "Results of the 2019 LSI stress test," BaFin, September 23, 2019, bafin.de; see also "Sensitivity Analysis of IRRBB – stress test 2017," European Central Bank, February 28, 2017, bankingsupervision.europa.eu.

Exhibit 3

The projection for unmanaged development of net-interest margins over the next five years for banks in the eurozone shows a decline of eight to 16 basis points.

Net-interest margins, basis points (bp)



Source: European Banking Authority Risk Dashboard; SNL Financial

— When calculating scenario analysis for the economic value of equity, also consider the impact on commercial margins. Perform reverse stress tests to identify critical moves in interest rates across different currencies.

Optimizing the risk–return profile of the structural components of net-interest margins

To optimize the risk–return profile of the structural components of net-interest margins, banks need to formulate an effective governance model and a clear risk-appetite framework for hedging strategies. These measures will allow the treasurer and related risk managers to make transparent, informative, and effective proposals. The objective is to obtain clear and timely decisions in the following areas:

— behavioral models for nonmaturing deposit balances feeding into interest-rate risk models and hedging strategies

— adjustments for mismatched maturity profiles of assets and liabilities

— positions with positive convexity (financial instruments which could disproportionally benefit from further declines in interest rates and offset negative-convexity positions)

— assumptions regarding the interest-rate tenor of equity and respective replicating hedge positions

— assumptions on the size, composition, and funding tenor of the liquidity buffer as well as of collateral for payment and clearing and settlement systems

— utilization of liquidity in foreign subsidiaries or branches, which can become trapped on local balance sheets due to legal or regulatory requirements

Stabilizing client-related components

To stabilize the client-related components of net-interest margins (assets and liabilities), treasurers also need a funds-transfer pricing mechanism and limit system that does four things: provide business lines with incentives to generate interest-bearing assets, bring down funding costs, increase the stability of deposits, and minimize liquidity buffer requirements. Treasurers can attain the leverage necessary to accomplish these objectives by taking certain measures:

— providing incentives to increase loan volumes in currencies with positive interest-rate levels

— encouraging new loan products and loan products with digital distribution channels that are scalable and can provide stable margins due to fast processing and positive client experience

— linking mortgages and covered bond issuances more closely with respect to issuance volumes and yields

— adjusting client rates for current accounts, short-term deposits, and savings deposits by offering "account packages" with fixed fees

— introducing tiered pricing for larger deposit balances and reference deposit rates to central-bank rates as appropriate for client group and purpose of deposits

— classifying hurdle rates for client deposits as particularly stable from an internal-risk-management or regulatory perspective

— stimulating the shift of unstable deposits with a zero interest-rate floor into alternative investment products

These actions may include a temporary increase in the loan-to-deposit ratio, reversing the traditional paradigm of targeting a low loan-to-deposit ratio. Denmark, Japan, Sweden, and Switzerland all took this approach from 2014 to 2018 (Exhibit 4).

Our experience and analysis suggest that treasurers may be able to mitigate most or all of the forecast depletion of net-interest margins for the next five years, through a combination of these mitigating measures (Exhibit 5).[9] The degree of mitigation will depend on a bank's business model, its risk appetite, its ability to employ more capital, and the degree to which the specific levers discussed above have already been deployed. The exact shape of the yield curve will also play a role.

Steering the business

To help senior leaders steer the businesses within the negative-interest-rate environment, treasurers must understand each business line's specific business model and criteria for success. To be effective in their consultative capacity, treasurers must help ensure that the roles and responsibilities among treasury, finance, risk, and the business lines are clearly defined and universally understood. The group needs to establish a shared view on balance-sheet planning (including capital, liquidity, and funding needs), legal entities, and strategic planning. Modern technology in fact makes such management overlays relatively easy to create. Establishing organizational units that bridge business lines and treasury departments can help facilitate communication and implement measures.

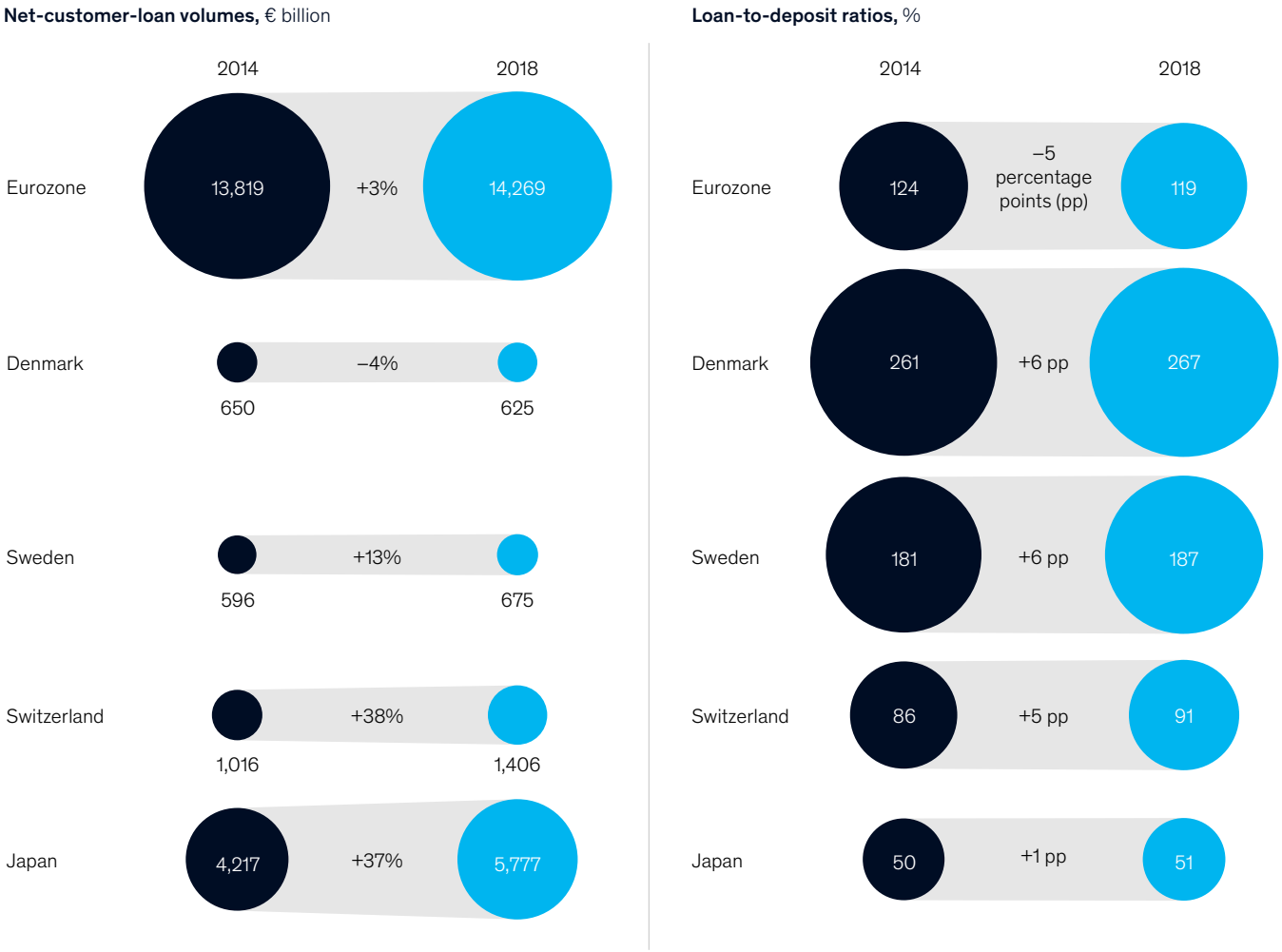
Ongoing strategic management is needed

Simply stabilizing the net-interest margin will not sufficiently drive significant and sustainable income growth. Banks need to take a strategic approach to manage real growth. Treasurers can facilitate that strategy by taking calculated steps in the following areas:

[9] "2020: Europe rising—at the break of dawn," Morgan Stanley, December 2019.

Exhibit 4

To stabilize the client-related components of net-interest margins (assets and liabilities), Denmark, Japan, Sweden, and Switzerland temporarily increased loan-to-deposit ratios.



Source: SNL Financial

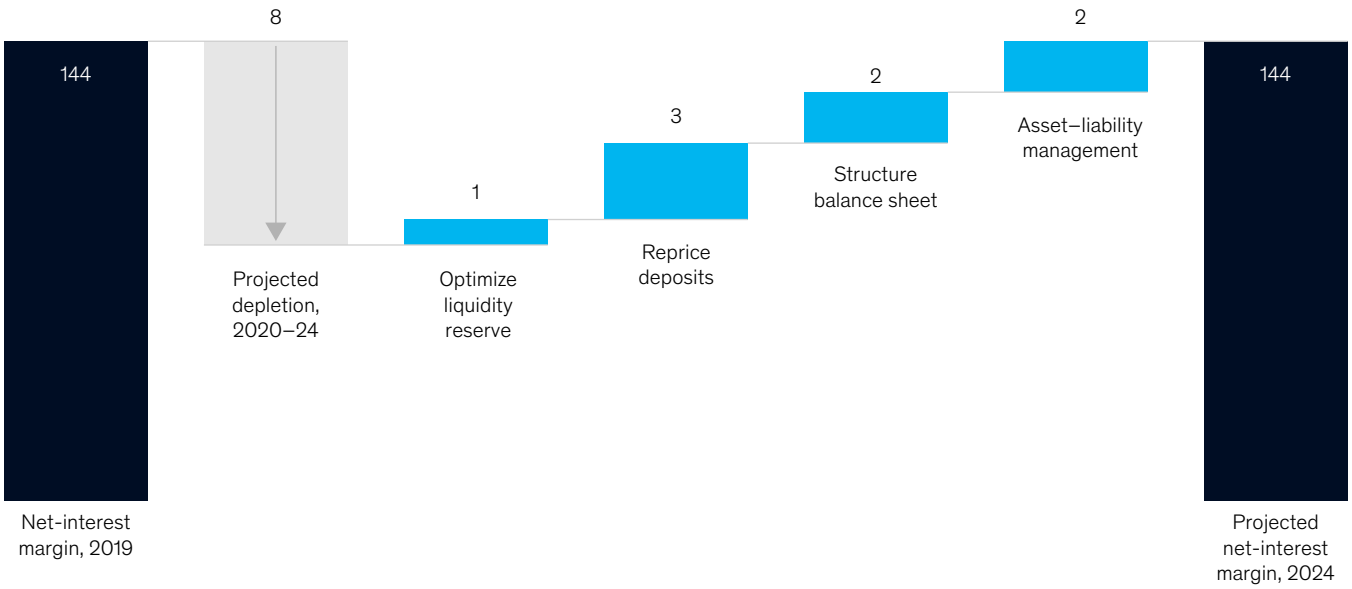
- Expand off-balance-sheet investment solutions, such as deposit platforms, sweeps, fund solutions, cash exchange-traded funds, and insurance-based savings plans.
- Renew emphasis on fee- and commission-based products, such as payments, advisory business, and asset management.
- Use incentives and capital allocation to expand loan volumes in high-margin businesses such as consumer finance and credit cards.

Treasurers can thus increase the efficiency of their own oversight and bring valuable counsel to the executive suite. Depending on the business

Exhibit 5

Treasurers can implement measures to mitigate projected depletion of net-interest margins.

Mitigating measures, basis points



model, the regional setup of the bank, and the deployment of additional capital, a comprehensive program can improve net-interest margins by up to 10 basis points. But timely and decisive action is of essential importance.

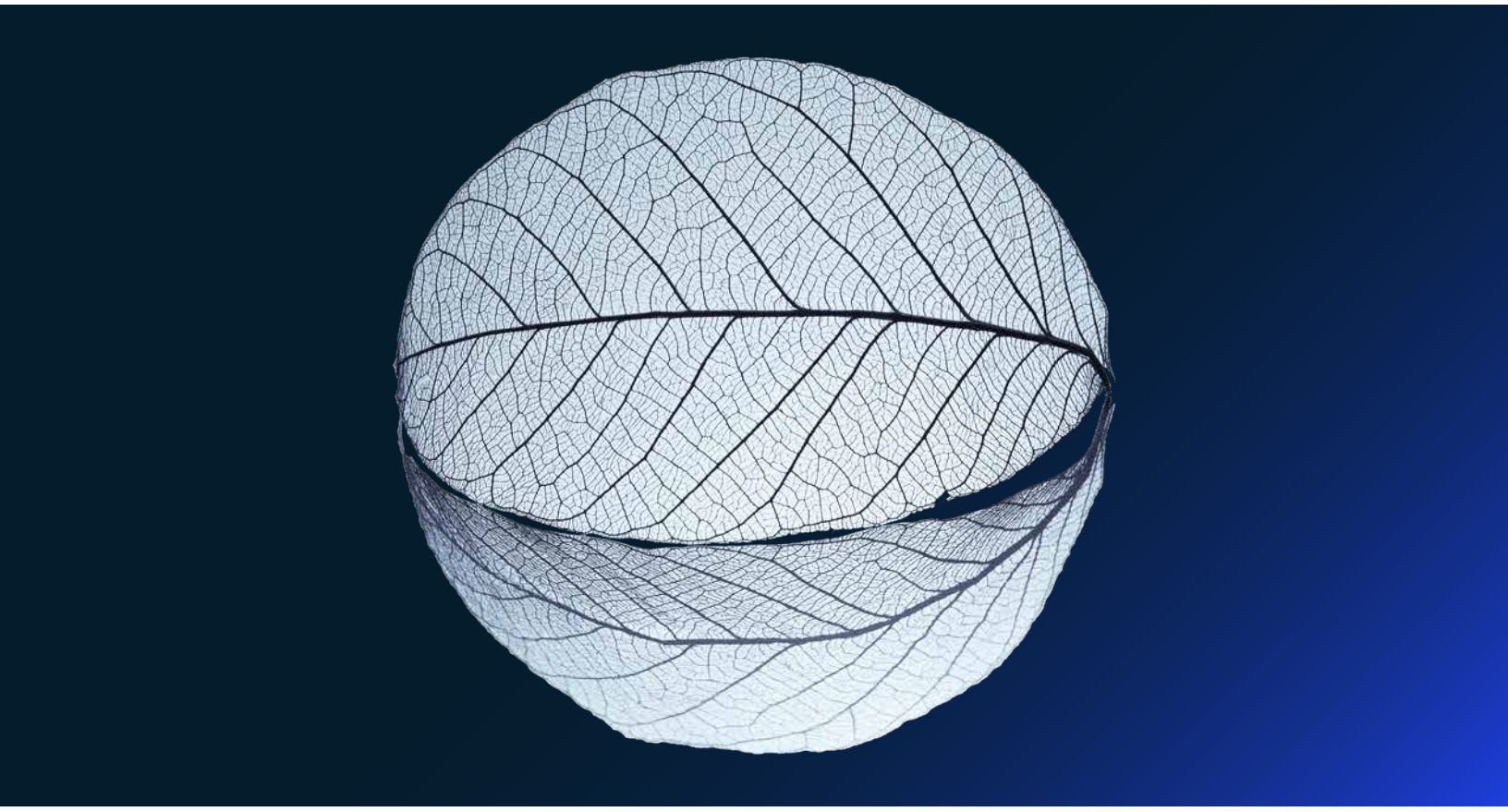
While today's interest-rate environment poses enormous challenges to growth in the banking sector, many of the tools for addressing the challenges are well known to treasurers. By taking a more holistic approach to using these tools, bringing their own considerable expertise to bear, and establishing a joint-management view on strategic planning and balance sheet–capital management, treasurers can play a vital role in their banks' financial success in the next period.

Andreas Bohn is a partner in McKinsey's Frankfurt office, **Olivier Plantefeve** is a partner in the Paris office, and **Thomas Poppensieker** is a senior partner in the Munich office, where **Sebastian Schneider** is a partner.

Banking imperatives for managing climate risk

More than regulatory pressure is driving banks to manage climate risk. Financing a green agenda is also a commercial imperative—but specialized skills are needed to protect balance sheets.

by Joseba Eceiza, Holger Harreis, Daniel Härtl, and Simona Viscardi



The surface temperature of the Earth has risen at a record pace in recent decades, creating risks to life, ecosystems, and economies. Climate science tells us that further warming is unavoidable over the next decade, and probably after that as well. In this uncertain environment, banks must act on two fronts: they need both to manage their own financial exposures and to help finance a green agenda, which will be critical to mitigate the impact of global warming. An imperative in both cases is excellent climate-risk management.

The physical risks of climate change are powerful and pervasive. Warming caused by greenhouse gases could damage livability and workability—for example, through a higher probability of lethal heat waves. Global warming will undermine food systems, physical assets, infrastructure, and natural habitats. The risk of a significant drop in grain yields—of 15 percent or more—and damage to capital stock from flooding will double by 2030. In aggregate, we expect that around a third of the planet's land area will be affected in some way.[1]

Disruptive physical impacts will give rise to transition risks and opportunities in the economy, including shifts in demand, the development of new energy resources, and innovations arising from the need to tackle emissions and manage carbon, as well as necessary reforms in food systems. Sectors that will bear the brunt include oil and gas, real estate, automotive and transport, power generation, and agriculture. In oil and gas, for example, demand could fall by 35 percent over the next decade. The good news is that these changes should also precipitate a sharp decline in emissions.

January 2020 was the warmest January on record. As temperatures rise in this way, it is incumbent on banks to manage the relevant risks and opportunities effectively (Exhibit 1).

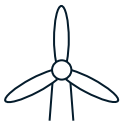
Furthermore, regulation increasingly *requires* banks to manage climate risk. Some have made a start, but many must still formulate strategies, build their capabilities, and create risk-management frameworks. The imperative now is to act decisively

[1] This estimate is based on a higher-emission scenario of RCP (Representative Concentration Pathway) 8.5 CO_2 concentrations (Intergovernmental Panel on Climate Change, a UN body). Lethal heat waves are defined as a wet-bulb temperature of 35° Celsius, at which level the body-core temperatures of healthy, well-hydrated human beings resting in the shade would rise to lethal levels after roughly five hours of exposure. Estimates are subject to uncertainty about aerosol levels and the urban heat-island effect. For further details, see "Climate risk and response: Physical hazards and socioeconomic impacts," McKinsey Global Institute, January 2020, on McKinsey.com.

Exhibit 1

Climate change creates opportunities and challenges for the banking industry.

Opportunity: Financing a green agenda



Transformation of energy production toward renewables

Plant refurbishments to avoid or capture and store carbon emissions

Electrification of transport and automation of mobility

Up to $500 billion in annual adaptation costs[1]

Challenge: Protecting balance sheets from uncertainty

Real-estate market collapse in low-lying areas

Increased risk of major crop failures with implications for meat and dairy producers

Closures of coal-powered power plants before end of useful life

For banks in the European Union, up to 15% of the balance sheet is at risk[2]

[1]Costs until 2050, according to the UN *Adaptation Gap Report* (2018).
[2]Based on analysis of 46 sample EU banks and their portfolio composition in industries and geographies likely affected by physical and transition risks.

The regulatory agenda

Regulatory initiatives that require banks to manage climate risks have gathered pace over the recent period (exhibit).

The United Kingdom's Prudential Regulation Authority was among the first to set out detailed expectations for governance, processes, and risk management. These require banks to identify, measure, quantify, and monitor exposure to climate risk and to ensure that the necessary technology and talent are in place. Germany's BaFin[1] has followed with similar requirements.

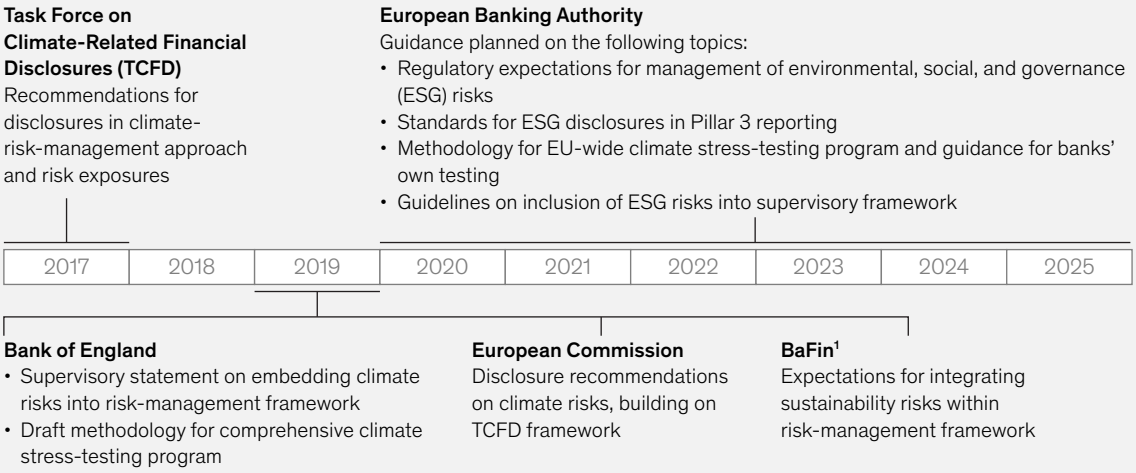
Among upcoming initiatives, the Bank of England plans to devote its 2021 Biennial Exploratory Scenario (BES) to the financial risks of climate change. The BES imposes requirements that will probably force many institutions to ramp up their capabilities, including the collection of data about physical and transition risks, modeling methodologies, risk sizing, understanding challenges to business models, and improvements to risk management. The European Banking Authority (EBA) is establishing regulatory and supervisory standards for environmental, social, and governance (ESG) risks and has published a multiyear sustainable-finance action plan. The EBA may provide a blueprint for authorities in geographies including the United States, Canada, and Hong Kong, which are also considering incorporating climate risk into their supervisory regimes.

[1] Bundesanstalt für Finanzdienstleistungsaufsicht.

Exhibit

Regulation is evolving at high speed.

Regulation timeline



[1]Bundesanstalt für Finanzdienstleistungsaufsicht.

and with conviction, so effective climate-risk management will be an essential skill set in the years ahead.

Regulatory and commercial pressures are increasing

Banks are under rising regulatory and commercial pressure to protect themselves from the impact of climate change and to align with the global sustainability agenda. Banking regulators around the world, now formalizing new rules for climate-risk management, intend to roll out demanding stress tests in the months ahead (see sidebar "The regulatory agenda"). Many investors, responding to their clients' shifting attitudes, already consider environmental, sustainability, and governance (ESG) factors in their investment decisions and are channeling funds to "green" companies.

The commercial imperatives for better climate-risk management are also increasing. In a competitive environment in which banks are often judged on their green credentials, it makes sense to develop sustainable-finance offerings and to incorporate climate factors into capital allocations, loan approvals, portfolio monitoring, and reporting. Some banks have already made significant strategic decisions, ramping up sustainable finance, offering discounts for green lending, and mobilizing new capital for environmental initiatives.

This increased engagement reflects the fact that climate-risk timelines closely align with bank risk profiles. There are material risks on a ten-year horizon (not far beyond the average maturity of loan books), and transition risks are already becoming real, forcing banks, for example, to write off stranded assets. Ratings agencies, meanwhile, are incorporating climate factors into their assessments. Standard & Poor's saw the ratings impact of environmental and climate factors increase by 140 percent over two years amid a high volume of activity in the energy sector.

As climate risk seeps into almost every commercial context, two challenges stand out as drivers of engagement in the short and medium terms.

Protecting the balance sheet from uncertainty

As physical and transition risks materialize, corporates will become increasingly vulnerable to value erosion that could undermine their credit status. Risks may be manifested in such effects as coastal real-estate losses, land redundancy, and forced adaptation of sites or closure. These, in turn, may have direct and indirect negative impact on banks, including an increase in stranded assets, uncertain residual values, and the potential loss of reputation if banks, for example, are not seen to support their customers effectively. Our analysis of portfolios at 46 European banks showed that, at any one time, around 15 percent of them carry increased risk from climate change. The relevant exposure is mostly toward industries (including electricity, gas, mining, water and sewerage, transportation, and construction) with high transition risks.

When we looked at the potential impact of floods on mortgage delinquencies in Florida, for example, we gathered flood-depth forecasts for specific locations and translated them into dollar-value damage levels. The analysis in Exhibit 2 is based on geographic levels associated with specific climate scenarios and probabilities. We then used these factors to generate numbers for depreciation and the probability of default and loss-given default. Based on the analysis, we calculated that more frequent and severe flooding in the Miami–Dade region may lead to an increase in mortgage defaults and loss rates close to those seen at the peak of the financial crisis and higher than those in extreme stress-test projections. Our severe-flooding scenario for 2030 predicts a 2.53 percent loss rate, just a bit lower than the 2.95 percent rate at the peak of the financial crisis. However, in the event of an economic slowdown, the rate could go as high as 7.25 percent.

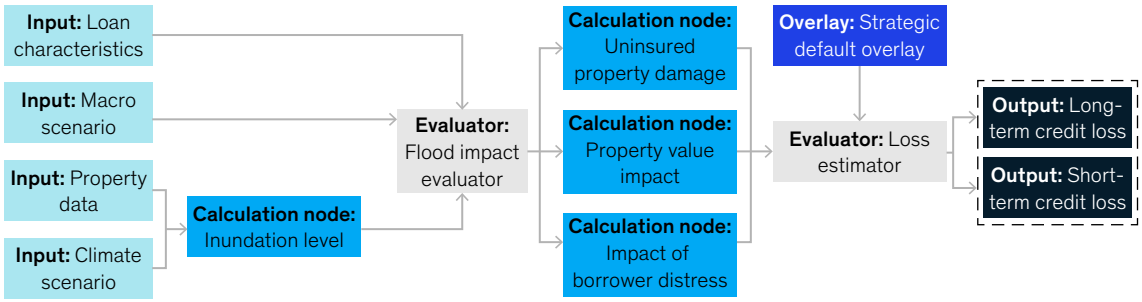
Financing a green agenda

Renewable energy, refurbishing plants, and adaptive technologies all require significant levels of financing. These improvements will cut carbon emissions, capture and store atmospheric carbon, and accelerate the transition away from fossil fuels. Some banks have already acted by redefining their

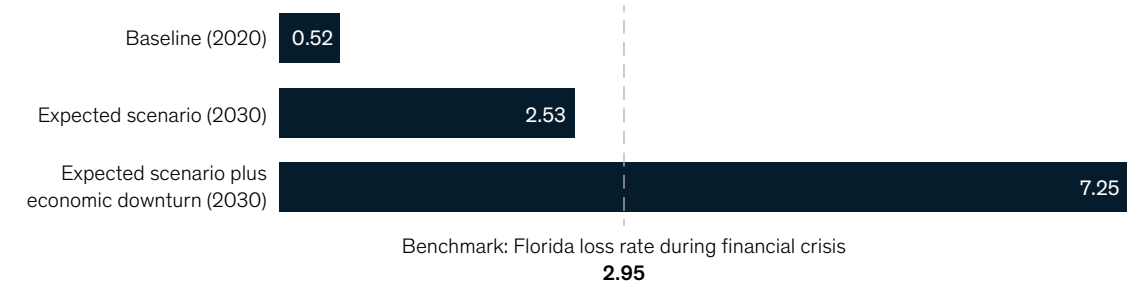
Exhibit 2

This model was developed to measure the impact of flooding on Florida home-loan markets.

Estimation of loss in loan levels



Projected loss rates for Miami mortgage portfolio, %



goals to align their loan portfolios with the aims of the Paris Agreement.[2]

Oil and gas, power generation, real estate, automotive, and agriculture present significant green-investment opportunities. In the United Kingdom, for example, 30 million homes will require sizable expenditure if they are to become low-carbon, low-energy dwellings.[3] In energy, opportunities are present in alternatives, refining, carbon capture, aviation, petrochemicals, and transport. As some clients exit oil and coal, banks have a role in helping them reduce their level of risk in supply contracts or in creating structured finance solutions for power-purchase agreements. In renewables, significant capital investment is needed in energy storage, mobility, and recycling.

A sharper lens: Five principles for climate-risk management

As they seek to become effective managers of climate risk, banks need to quantify climate factors across the business and put in place the tools and processes needed to take advantage of them effectively. At the same time, they must ensure that their operations are aligned with the demands of external stakeholders. Five principles will support this transformation. They should be applied flexibly as the regulatory landscape changes.

[2] The Paris Agreement's central aim is to strengthen the global response to the threat of climate change by keeping any global temperature rise this century well below 2 degrees Celsius above preindustrial levels and to pursue efforts to limit the temperature increase even further to 1.5 degrees Celsius.

[3] Angela Adams, Mary Livingstone, and Jason Palmer, *What does it cost to retrofit homes? Updating the cost assumptions for BEIS's energy efficiency modelling*, UK Department for Business, Energy & Industrial Strategy, April 2017; assets.publishing.service.gov.uk.

Formulate climate-risk governance. It will be of crucial importance for top management to set the tone on climate-risk governance. Banks should nominate a leader responsible for climate risk; chief risk officers (CROs) are often preferred candidates. To ensure that the board can keep an eye on exposures and respond swiftly, banks should institute comprehensive internal-reporting workflows. There is also a cultural imperative: responsibility for climate-risk management must be cascaded throughout the organization.

Tailor business and credit strategy. Climate considerations should be deeply embedded in risk frameworks and capital-allocation processes. Many institutions have decided not to serve certain companies or sectors or have imposed emissions thresholds for financing in some sectors. Boards should regularly identify potential threats to strategic plans and business models.

Align risk processes. To align climate-risk exposure with risk appetite and the business and credit strategy, risk managers should inject climate-risk considerations into all risk-management processes, including capital allocations, loan approvals, portfolio monitoring, and reporting. Some institutions have started to develop methodologies for assessing climate risk at the level of individual counterparties (see sidebar "A leading bank incorporates climate risk into its counterparty ratings").

Counterparty credit scoring requires detailed sectoral and geographic metrics to interpret physical and transition risks as a view of financial vulnerability, taking into account mitigation measures. The resulting risk score can be used to inform credit decisions and to create a portfolio overview. The score can also be embedded in internal and external climate-risk reporting, such as responses to the disclosure recommendations of the Financial Stability Board (Task Force on Climate-Related Financial Disclosures) or the European Banking Authority (Non-Financial Risk Disclosure Framework).

Get up to speed on stress testing. Scenario analyses and stress tests, which are high on business and regulatory agendas, will be critical levers in helping banks assess their resilience. In preparing for tests, they should first identify important climate hazards and primary risk drivers by industry, an analysis they can use to generate physical and transition-risk scenarios. These in turn can help banks estimate the extent of the damage caused by events such as droughts and heat waves. Finally, banks have to quantify the impact by counterparty and in aggregate on a portfolio basis. Risk-management teams should also prepare a range of potential mitigants and put in place systems to translate test results into an overview of the bank's position. Since regulators are prioritizing stress testing for the coming period, acquiring the necessary climate-modeling expertise and climate-hazard and asset-level data is an urgent task.

Focus on enablers. Banks often lack the technical skills required to manage climate risk. They will need to focus on acquiring them and on developing a strategic understanding of how physical and transition risks may affect their activities in certain locations or industry sectors. Banks usually need "quants," for example—the experts required to build climate-focused counterparty- or portfolio-level models. They should therefore budget for increased investment in technology, data, and talent.

Reaching for risk maturity: Three steps

As banks ponder how to incorporate climate-change considerations into their risk-management activities, they will find that it is important to remain pragmatic. The climate issue is emotive. Stakeholders want robust action, and banks feel pressure to respond. Those that make haste, however, increase the risk of missteps. The best strategy is adequate, comprehensive preparation: a bank can create a value-focused road map setting out an agenda fitted to its circumstances and taking into account both the physical and regulatory status quo. Once the road map is in place, banks should adopt a

A leading bank incorporates climate risk into its counterparty ratings

A leading international bank aimed to increase its share of climate markets. To get there, it needed to incorporate climate factors into the risk-management function and to develop tools for assessing climate risks, on the counterparty level, for its entire portfolio.

The bank aimed to assess climate risk for each of its 2,500 counterparties on an annual basis, and its solution had to be sufficiently simple and scalable for individual loan officers to use on counterparties of all sizes. The eventual solution was based on the production of scorecards for physical and transition risks (exhibit).

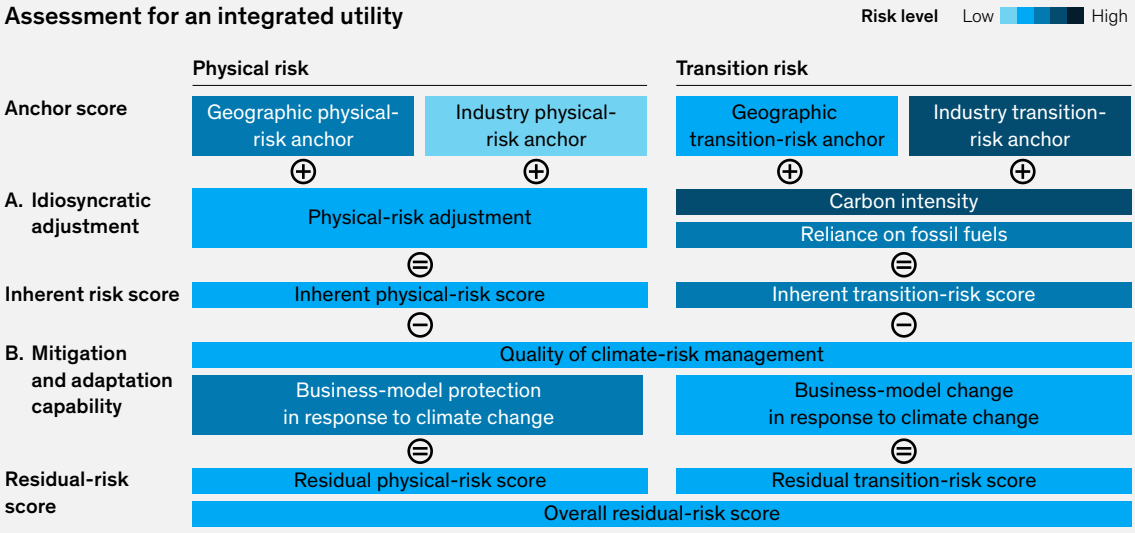
The bank's calculations were predicated on anchor scores that reflected the counterparty's industry and geographic footprint. These were adjusted for idiosyncratic effects to reflect transition risk arising from a company's greenhouse-gas emissions or the reliance of its business model on fossil fuels and related products. Additional parameters helped assess the potential for mitigation and adaptation—including a qualitative assessment of the company's climate-risk management, actions to protect physical assets from future physical hazards, and initiatives to adopt a more sustainable business and operating model. The final output of the calculations was a counterparty rating that incorporated inputs from physical and transition-risk scorecards.

The counterparty model was useful to differentiate the climate risk among companies within sectors. Testing for the bank's utilities subportfolio, for example, showed that electricity providers and multi-utilities fared worse than regulated networks. Companies with a higher proportion of renewables generally fared better.

One concern during model development was the shortage of available climate data and climate-related corporate information. The bank had to strike a balance between model accuracy and feasibility. Finally, it decided to work largely with publicly available data selectively augmented with climate-hazard data. As the bank developed, tested, and rolled out the methodology, cross-functional teams emerged as a success factor. These teams consisted of model developers, analysts, economists, and climate experts.

Exhibit

An international banking group embedded climate risk into counterparty ratings.



modular approach to implementation, ensuring that investments are tied to areas of business value by facilitating finance, offering downside protection, and meeting external expectations.

For developing a comprehensive approach to risk management, we see three key steps, which should be attainable in four to six months.

1. Define and articulate your strategic ambition
Effective climate-risk management should be based on a dedicated strategy. Individual banks must be sure about the role they want to play and identify the client segments and industry sectors where they can add the most value. They should also establish and implement governance frameworks for climate risk—frameworks that include the use of specialized senior personnel, as well as a minimum standard for reporting up and down the business.

Some are already taking action. One financial institution made its CRO the executive accountable for climate change and head of the climate-change working group. Another institution divided these responsibilities among the board of directors, executive management, business areas, group functions, and the sustainable-finance unit. Banks should also factor in adjacencies because lending to some clients in riskier geographies and industries—even to finance climate-related initiatives—is still riskier. This will ensure that banks formulate a structured approach to these dilemmas.

2. Build the foundations
Banks should urgently identify the processes, methodologies, and tools they will need to manage climate risk effectively. This entails embedding climate factors into risk and credit frameworks—for example, through the counterparty-scoring method described above. Scenario analyses and stress tests will be pillars of supervisory frameworks and should be considered essential capabilities. Outcomes should be hardwired into reporting and disclosure frameworks. Finally, banking, like most sectors, does not yet have the climate-risk resources it needs. The industry must therefore accumulate skills and build or buy relevant IT, data, and analytics.

3. Construct a climate-risk-management framework
Banks must aim to embed climate-risk factors into decision making across their front- and back-office activities and for both financial and nonfinancial risks (including operational, legal, compliance, and reputational risks). Data will be a significant hurdle. Data are needed to understand the fundamentals of climate change as well as the impact it will have on activities such as pricing, credit risk, and client-relationship management. However, a paucity of data should not become an impediment to action. As far as possible, banks should measure climate exposures at a number of levels, including by portfolio, subportfolio, and even transaction. This will enable the creation of heat maps and detailed reports of specific situations where necessary. In corporate banking, this kind of measurement and reporting might support a climate-adjusted credit scorecard (covering cash flows, capital, liquidity diversification, and management experience) for individual companies. Banks may then choose to assign specific risk limits. Indeed, some banks have already moved to integrate these types of approaches into their loan books.

As intermediaries and providers of capital, banks play a crucial role in economic development that now includes managing the physical and transition risks of climate change. The task is complex, and the models and assumptions needed to align the business with climate priorities will inevitably be revised and refined over time. However, as temperatures rise, speed is of the essence in managing the transition to a more sustainable global economy.

Joseba Eceiza is a partner in McKinsey's Madrid office, **Holger Harreis** is a senior partner in the Düsseldorf office, **Daniel Härtl** is an associate partner in the Munich office, and **Simona Viscardi** is a partner in the Milan office.

The authors wish to thank Mark Azoulay, Hauke Engel, Hans Helbekkmo, Jan F. Kleine, Olivier Maillet, Daniel Mikkelsen, Arthur Piret, Thomas Poppensieker, and Hamid Samandari for their contributions to this article.

The future of operational-risk management in financial services

By partnering with the business, the operational-risk discipline can create a more secure and profitable institution. Here's what has to happen first.

by Joseba Eceiza, Ida Kristensen, Dmitry Krivin, Hamid Samandari, and Olivia White

New forces are creating new demands for operational-risk management in financial services. Breakthrough technology, increased data availability, and new business models and value chains are transforming the ways banks serve customers, interact with third parties, and operate internally. Operational risk must keep up with this dynamic environment, including the evolving risk landscape.

Legacy processes and controls have to be updated to begin with, but banks can also look upon the imperative to change as an improvement opportunity. The adoption of new technologies and the use of new data can improve operational-risk management itself. Within reach is more targeted risk management, undertaken with greater efficiency, and truly integrated with business decision making.

The advantages for financial-services firms that manage to do this are significant. Already, efforts to address the new challenges are bringing measurable bottom-line impact. For example, one global bank tackled unacceptable false-positive rates in anti–money laundering (AML) detection—which were as high as 96 percent. Using machine learning to identify crucial data flaws, the bank made necessary data-quality improvements and thereby quickly eliminated an estimated 35,000 investigative hours. A North American bank assessed conduct-risk exposures in its retail sales force. Using advanced-analytics models to monitor behavioral patterns among 20,000 employees, the bank identified unwanted anomalies before they became serious problems. The cases for change are in fact diverse and compelling, but transformations can present formidable challenges for functions and their institutions.

The current state

Operational risk is a relatively young field: it became an independent discipline only in the past 20 years. While banks have been aware of risks associated with operations or employee activities for a long while, the Basel Committee on Banking Supervision (BCBS), in a series of papers published between 1999 and 2001, elevated operational risk to a distinct and controllable risk category requiring its own tools and organization.[1] In the first decade of building operational-risk-management capabilities, banks focused on governance, putting in place foundational elements such as loss-event reporting and risk-control self-assessments (RCSAs) and developing operational-risk capital models. The financial crisis precipitated a wave of regulatory fines and enforcement actions on misselling, questionable mortgage-foreclosure practices, financial crimes, London Inter-bank Offered Rate (LIBOR) fixing, and foreign-exchange misconduct. As these events worked their way through the banking system, they highlighted weaknesses of earlier risk practices. Institutions responded by making significant investments in operational-risk capabilities. They developed risk taxonomies beyond the BCBS categories, put in place new risk-identification and risk-assessment processes, and created extensive controls and control-testing processes. While the industry succeeded in reducing industry-wide regulatory fines, losses from operational risk have remained elevated (Exhibit 1).

Intrinsic difficulties

While banks have made good progress, managing operational risk remains intrinsically difficult, for a number of reasons. Compared with financial risk such as credit or market risk, operational risk is more complex, involving dozens of diverse risk types. Second, operational-risk management requires oversight and transparency of almost all organizational processes and business activities. Third, the distinguishing definitions of the roles of the operational-risk function and other oversight groups—especially compliance, financial crime, cyberrisk, and IT risk—have been fluid. Finally, until recently, operational risk was less easily measured and managed through data and recognized limits than financial risk.

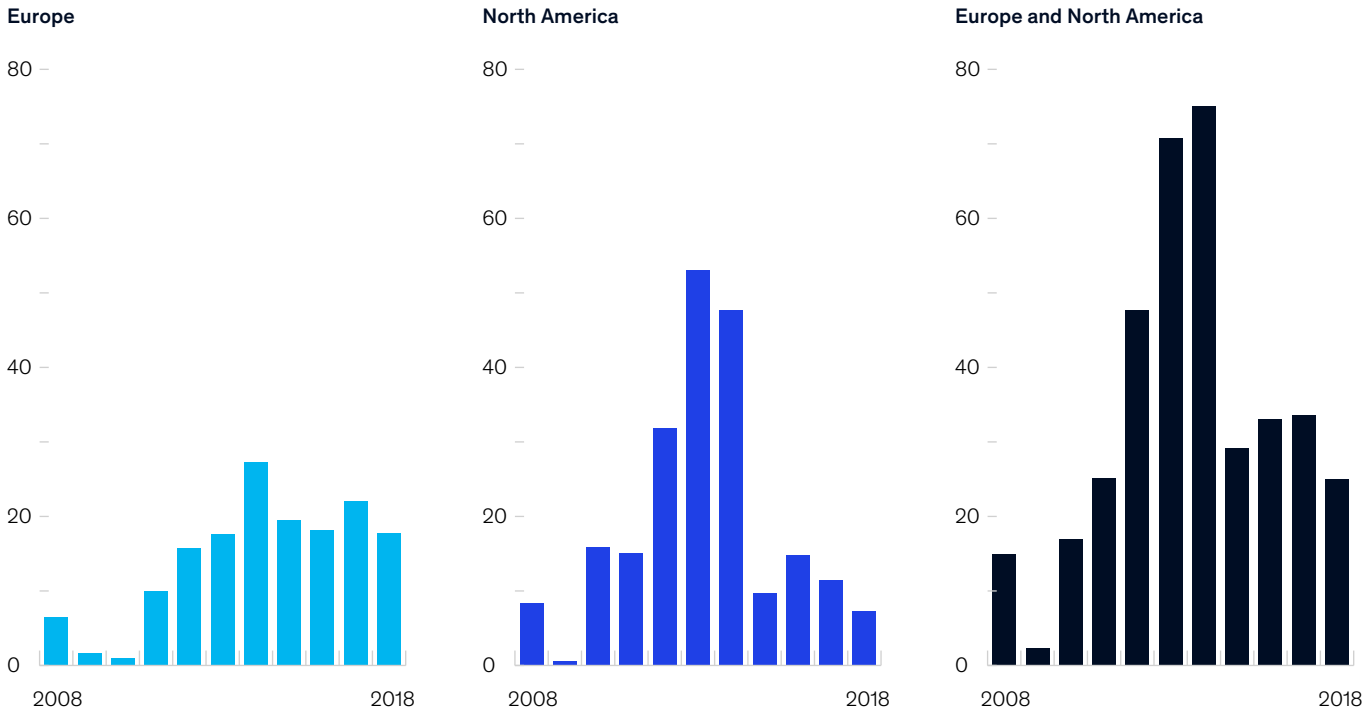
This last constraint has been lifted in recent years: granular data and measurement on operational processes, employee activity, customer feedback,

[1] The standard Basel Committee on Banking Supervision definition of operational (or nonfinancial) risk is "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events." See *Basel Committee on Banking Supervision: Working paper on the regulatory treatment of operational risk,* Bank for International Settlements, September 2001, bis.org.

Exhibit 1

Operational-risk losses increased rapidly after the 2008–9 financial crisis and have remained elevated since.

Banking litigation: costs, fines, and operational losses, $ billion



and other sources of insight are now widely available. Measurement remains difficult, and risk teams still face challenges in bringing together diverse sources of data. Nonetheless, data availability and the potential applications of analytics have created an opportunity to transform operational-risk detection, moving from qualitative, manual controls to data-driven, real-time monitoring.

As for the other challenges, they have, if anything, steepened. Operational complexity has increased. The number and diversity of operational-risk types have enlarged, as important specialized-risk categories become more defined, including unauthorized trading, third-party risk, fraud, questionable sales practices, misconduct, new-product risk, cyberrisk, and operational resilience.

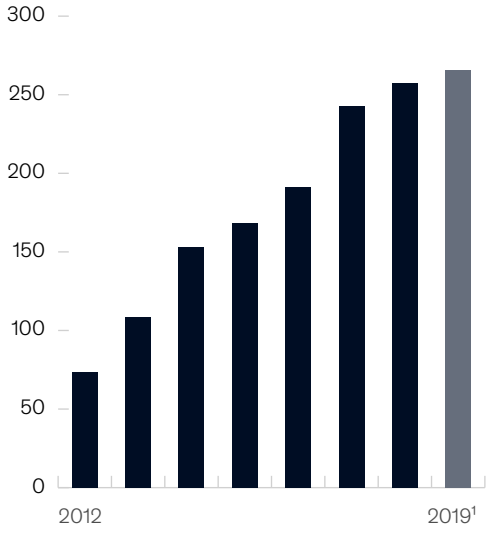
At the same time, digitization and automation have been changing the nature of work, reducing traditional human errors but creating new change-management risks; fintech partnerships create cyberrisks and produce new single points of failure; the application of machine learning and artificial intelligence (AI) raises issues of decision bias and ethical use of customer data. Finally, the lines between the operational-risk-management function and other second-line groups, such as compliance, continue to shift. Banks have invested in harmonizing risk taxonomies and assessments, but most recognize that significant overlap remains. This creates frustration among business units and frontline partners.

Taken together, these factors explain why operational-risk management remains intrinsically difficult and why the effectiveness of the discipline—as measured by consumer complaints, for example—has been disappointing (Exhibit 2).

Exhibit 2

Indicators of operational-risk levels continue to rise.

Complaints filed annually with Consumer Financial Protection Bureau, thousands



[1] 1st half of 2019 annualized.

Source: Consumer Financial Protection Bureau database; McKinsey analysis

Looking ahead

Against these challenges, risk practitioners are seeking to develop better tools, frameworks, and talent. Leading companies are discarding the "rearview mirror" approach, defined by thousands of qualitative controls. For effective operational-risk management, suitable to the new environment, these organizations are refocusing the front line on business resiliency and critical vulnerabilities. They are adopting data-driven risk measurement and shifting detection tools from subjective control assessments to real-time monitoring.

The objective is for operational-risk management to become a valuable partner to the business. Banks need to take specific actions to move the function from reporting and aggregation of first-line controls to providing expertise and thought partnership. The areas where the function will help execute business strategy include operational strengths and vulnerabilities, new-product design, and infrastructure enhancements, as well as other areas that allow the enterprise to operate effectively and prevent undue large-scale risk issues.

Defining next-generation operational-risk management

The operational-risk discipline needs to evolve in four areas: 1) the mandate needs to expand to include second-line oversight, to support operational excellence and business-process resiliency; 2) analytics-driven issue detection and real-time risk reporting have to replace manual risk assessments; 3) talent needs to be realigned as digitization progresses and data and analytics are rolled out: banks will need specialists to manage specific risk types such as cyberrisk, fraud, and conduct risk; and 4) human-factor risks will have to be monitored and assessed—including those that relate to misconduct (such as sexual harassment) and to diversity and inclusion.

The evolution includes the shift to real-time detection and action. This will involve the adoption of more agile ways of working, with greater use of cross-disciplinary teams that can respond quickly to arising issues, near misses, and emerging risks or threats to resilience.

1. Develop second-line oversight to ensure operational excellence and business-process resiliency

The original role of operational-risk management was focused on detecting and reporting nonfinancial risks, such as regulatory, third-party, and process risk. We believe that this mandate should expand so that the second line is an effective partner to the first line, playing a challenge role to support the fundamental resiliency of the operating model and processes. A breakdown in processes is at the core of many nonfinancial risks today, including negative regulatory outcomes, such as missing disclosures, customer and client disruption, and revenue and reputational costs. The operational-risk-management function should help chief risk officers and other senior managers answer several key questions, such as: Have we designed business processes in each area to provide consistent, positive customer outcomes? Do these processes operate well in both normal and stress

conditions? Is our change-management process robust enough to prevent disruptions? Is the operating model designed to limit risk from bad actors?

Untransformed operational-risk-management functions have limited insight into the strength of operational processes or rely on an extensive inventory of controls to ensure quality. Controls, however, are not effective in monitoring process resilience. A transaction-processing system, for example, may have reconciliation controls (such as a line of checkers) that perform well under normal conditions but cannot operate under stress. This is because the controls are fundamentally reliant on manual activities. Similarly, controls on IT infrastructure may not prevent a poorly executed platform transition from leading to large customer disruptions and reputational losses.

New frameworks and tools are therefore needed to properly evaluate the resiliency of business processes, challenge business management as appropriate, and prioritize interventions. These frameworks should support the following types of actions:

- *Map processes, risks, and controls.* Map the processes, along with associated risks and controls, including overall complexity, number of handoffs involved, and automation versus reliance on manual activities (particularly when the danger is high for negative customer outcomes or regulatory mistakes). This work will ideally be done in conjunction with systemic controls embedded in the process; end-to-end process ownership minimizes handoffs and maximizes collaboration.
- *Identify supporting technology.* Identify and understand the points where processes rely on technology.
- *Monitor risks and controls.* Create mechanisms and metrics (such as higher-than-normal volumes) to enable the monitoring of risk levels and control effectiveness, in real time wherever possible.
- *Link resource planning to processes.* Link resource planning to the emergent understanding of processes and associated needs. Be ready to scale capacity up or down according to the results of process monitoring.
- *Reinforce needed behavior.* Ensure reinforcement mechanisms for personal conduct, using communications, training, performance management, and incentives.
- *Enable feedback.* Establish feedback mechanisms for flagging potential issues, undertaking root-cause analysis, and updating or revising processes as needed to address the causes.
- *Establish change management.* Establish systematic, ongoing change management to ensure the right talent is in place, test processes and capacity, and provide guidance, particularly for technology.

2. Transform risk detection with data and real-time analytics

In response to regulatory concerns over sales practices, most banks comprehensively assessed their sales-operating models, including sales processes, product features, incentives, frontline-management routines, and customer-complaint processes. Many of these assessments went beyond the traditional responsibilities of operational-risk management, yet they highlight the type of discipline that will become standard practice. While making advances in some areas, banks still rely on many highly subjective operational-risk detection tools, centered on self-assessment and control reviews. Such tools have been ineffective in detecting cyberrisk, fraud, aspects of conduct risk, and other critical operational-risk categories. Additionally, they miss low-frequency, high-severity events, such as misconduct among a small group of frontline employees. Finally, some traditional detection techniques, such as rules-based cyberrisk and trading alerts, have false-positive rates of more than 90 percent. Many self-assessments in the first and second line consequently require enormous amounts of manual work but still miss major issues.

Operational-risk managers must therefore rethink their approaches to issue detection. Advances in data and analytics can help. Banks can now tap into large repositories of structured and unstructured data to identify risk issues across operational-

risk categories, moving beyond reliance on self-assessments and subjective controls. These emerging detection tools might best be described in two broad categories:

— *Real-time risk indicators* include real-time testing of operational processes and controls and risk metrics that identify areas operating under stress, spikes in transaction volumes, and other determinants of risk levels.

— *Targeted analytics tools* can connect the data dots to detect potential risk issues (see sidebar "Targeted analytics tools"). By mining sales and customer data, banks can detect potentially unauthorized sales. Machine-learning models can detect cyberrisk levels, fraud, and potential money laundering. As long as all privacy measures are respected, institutions can use natural-language processing to analyze calls, emails, surveys, and social-media posts to identify spikes in risk topics raised by customers in real time.

Targeted analytics tools

Advanced analytics has applications in all, or nearly all, areas of operational risk. It is creating significant improvements in detecting operational risks, revealing risks more quickly, and reducing false positives. Whether in information security, data, compliance, technology and systems, process failure, or even personal security and other human-factor risks, the advanced-analytics advantage is becoming increasingly evident. Some applications are described below:

— *Anti–money laundering.* Replacing rules-driven alerts with machine-learning models can reduce false positives and focus resources on cases that actually require investigation.

— *Conduct.* Analytics engines can identify suspicious sales patterns, connecting the dots across sales, product usage, incentives, and customer complaints (for example, increases in nonactivated deposits, accounts sold by a retail banker, or trades triggered by a wealth-management adviser as they approach compensation breakpoints). Trade-monitoring analytics can mine trading and communication patterns for potential markers of conduct risk.

— *Cyberrisk.* Machine learning can analyze sources of signals, identify emerging threats, replace existing rules-based triggers, and reduce false-positive alerts.

— *Fraud.* Machine learning, including unsupervised techniques, can identify fraudulent transactions and reduce false positives; synthetic-ID-fraud analytics use external, third-party data, in accordance with all local regulation, to analyze the depth and consistency in the identity profiles of new customers

— *Process quality and regulatory risks.* Automated call surveillance using natural-language processing can monitor adherence to disclosure requirements. Systemic quality-control touchpoints can check the accuracy of decisions, disclosures, and filings against customer-provided information and regulatory rules (for example, the accuracy of a bankruptcy filing against the system of record information).

— *Third-party risk.* Models can be developed that quantify the reliance on key third parties (including hidden fourth-party exposures) to drive better business-continuity planning and bring a risk-based perspective to vendor assessment and selection.

Exhibit 3 shows how a risk manager using natural-language processing can identify a spike in customer complaints related to the promotion of new accounts. Looking into the underlying complaints and call records, the manager would be able to identify issues in how offers are made to customers.

A number of banks are investing in objective, real-time risk indicators to supplement or replace subjective assessments. These indicators help risk managers track general operational health, such as staffing sufficiency, processing times, and inventories. They also provide early warnings of process risks, such as inaccurate decisions or disclosures, and the results of automated exception reporting and control testing.

Together, analytics and real-time reporting can transform operational-risk detection, enabling banks to move away from qualitative self-assessments to automated real-time risk detection and transparency. The journey is difficult—it requires that institutions overcome challenges in data aggregation and building risk analytics at scale—yet it will result in more effective and efficient risk detection.

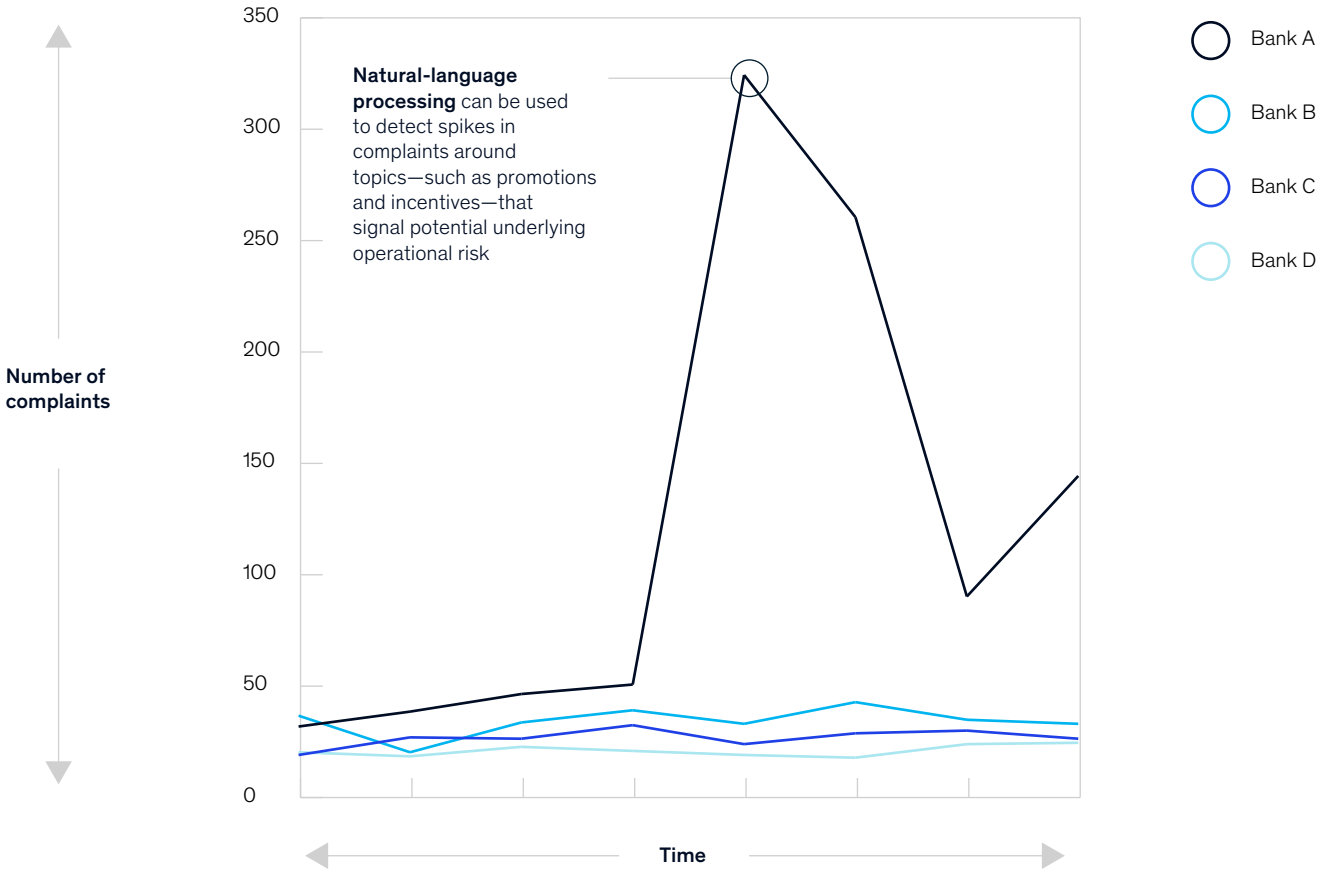
3. Develop talent and the tools to manage specialized risk types

A range of emerging risks, all of which fall under the operational-risk umbrella, present new challenges for banks. To manage these risks—in areas such as technology, data, and financial crime—banks need specialized knowledge and tools. For example,

Exhibit 3

Natural-language processing can help detect operational risk.

Customer complaints over time



managing fraud risk requires a deep understanding of fraud typologies, new and emerging vulnerabilities, and the effectiveness of first-line processes and controls. Similarly, oversight of conduct risks requires up-to-date knowledge about how systems can be "gamed" in each business line. In capital markets, for instance, some products are more susceptible than others to nontransparent communication, misselling, misconduct in products, and manipulation by unscrupulous employees. Operational-risk officers will need to rethink their risk organization and recruit talent to support process-centric risk management and advanced analytics. These changes in talent composition are significant and different from what most banks currently have in place (see sidebar "Examples of specialized expertise").

Examples of specialized expertise

Risk category	Expertise needed for challenge and oversight	Talent profiles
Cyberrisk	— Pathways to vulnerability (such as the impact of a threat like NotPetya) — The bank's most valuable assets (the "crown jewels") — Sources of exposure for a given organization	— Cybersecurity background — Senior status to engage the business and technology organizations
Fraud	— Fraud patterns (for instance, through the dark web) — Technology and cybersecurity — Interdependencies across fraud, cybersecurity, IT, and business-product decisions	— Former senior technology managers — Cybersecurity professionals, ideally with an analytics background
Conduct	— Ways employees can game the system in each business unit (for instance, retail, wealth, and capital markets) — Specific behavioral patterns, such as how traders could harm client interests for their own gain	— Former branch managers and frontline supervisors — Former traders and back-office managers — First-line risk managers with experience in investigating conduct issues

Bank employees drive corporate performance but are also a potential source of operational risk.

With specialized talent in place, banks will then need to integrate the people and work of the operational-risk function as never before. To meet the challenge, organizations have to prepare leaders, business staff, and specialist teams to think and work in new ways. They must help them adapt to process-driven risk management and understand the potential applications of advanced analytics. The overall objective is to create an operational-risk function that embraces agile development, data exploration, and interdisciplinary teamwork.

4. Manage human-factor risks

Bank employees drive corporate performance but are also a potential source of operational risk. In recent years, conduct issues in sales and instances of LIBOR and foreign-exchange manipulation have elevated the human factor in the nonfinancial-risk universe. In the past, HR was mainly responsible for addressing conduct risk, as part of its oversight role in hiring and investigating conduct issues. As the potential for human-factor risks to inflict serious damage has become more apparent, however, banks are recognizing that this oversight must be included in the operational-risk-management function.

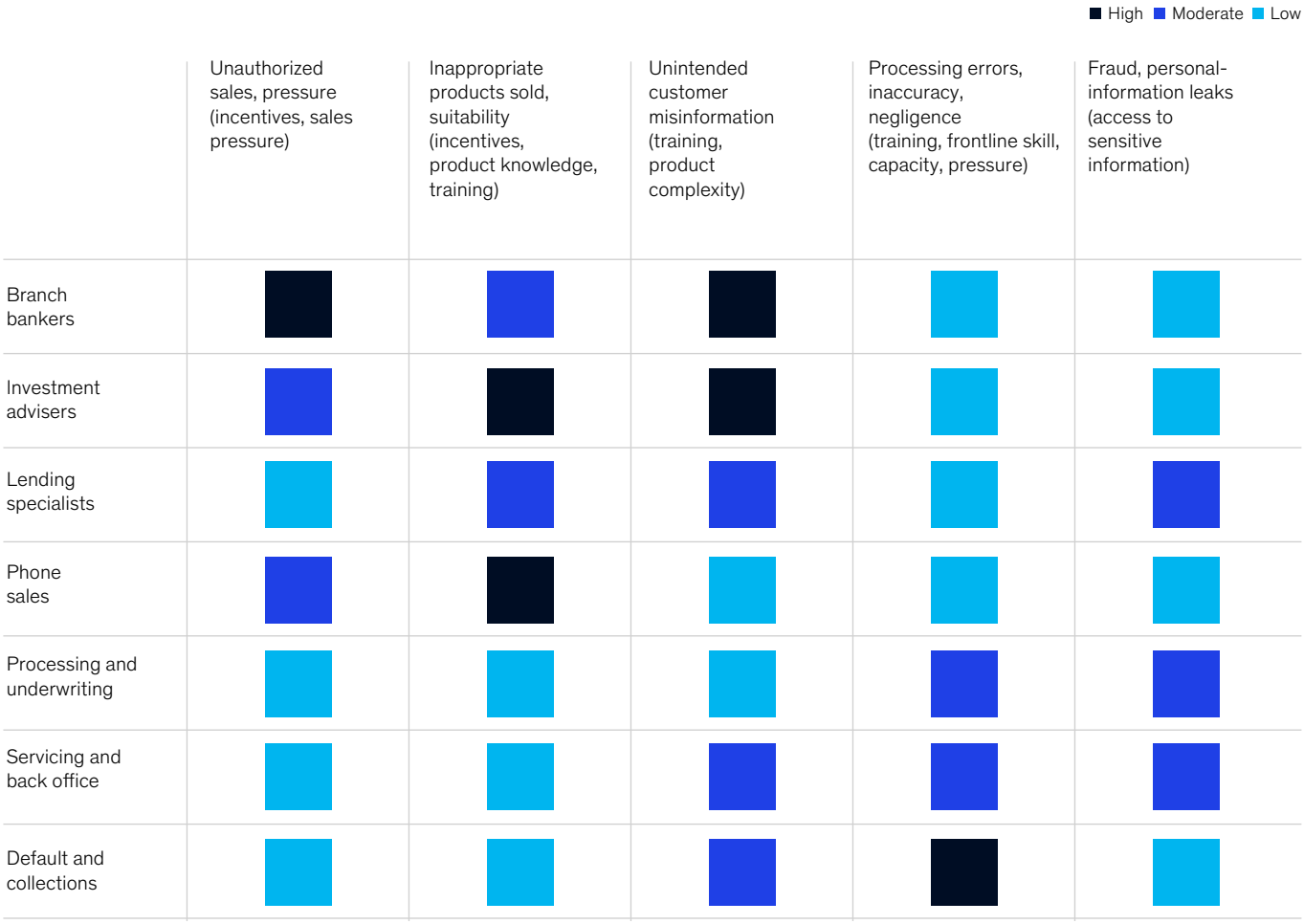
Developing effective risk-oversight frameworks for human-factor risks is not an easy task, as these risks are diverse and differ from many other operational-risk types. Some involve behavioral transgressions among employees; others involve the abuse of insider organizational knowledge and finding ways around static controls. These risks have more to do with culture, personal motives, and incentives, that is, than with operational processes and infrastructure. And they are hard to quantify and prioritize in organizations with many thousands of employees in dozens or even hundreds of functions.

To prioritize areas of oversight and intervention, leading operational-risk executives are taking the following steps. They first determine which groups within the organization present disproportionate human-factor risks, including misconduct, mistakes with heavy regulatory or business consequences, and internal fraud. Analyzing functions within each business unit, operational-risk leaders can then identify those that present the greatest inherent risk exposure. The next step is to prioritize the “failure modes” behind the risks, including malicious intent (traditional conduct risk), inadequate respect for rules, lack of competence or capacity, and the attrition of critical employees. The prioritized framework can be visualized in a heat map (Exhibit 4).

Exhibit 4

A prioritized grid of human-factor risks can help mitigate risks at points of high exposure.

Potential human-factor risks (retail-banking example), by applicability of risk-mitigation measures



The heat map provides risk managers with the basis for partnering with the first line to develop a set of intervention programs tailored to each high-risk group. The effort includes monitoring, oversight, role modeling, and tone setting from the top. Additionally, training, consequence management, a modified incentive structure, and contingency planning for critical employees are indispensable tools for targeting the sources of exposure and appropriate first-line interventions.

A brighter future

Through the four-part transformation we have described, operational-risk functions can proceed to deepen their partnership with the business, joining with executives to derisk underlying processes and infrastructure. Historically, operational-risk management has focused on reporting risk issues, often in specialized forums removed from day-to-day assessment. Many organizations have thus viewed operational-risk

activities as a regulatory necessity and of little business value. The function is accustomed to react to business priorities rather than involve itself in business decision making.

To be effective, operational-risk management needs to change these assumptions. When equipped with objective data and measurement, the function well understands the true level of risk. It is therefore in a unique position to see nonfinancial risks and vulnerabilities across the organization, and it can best prioritize areas for intervention. Together with the business lines, operational-risk management can identify and shape needed investments and initiatives. This would include efforts to digitize operations to remove manual errors, changes in the technology infrastructure, and decisions on product design and business practices. By helping the business meet its objectives while reducing risks of large-scale exposure, operational-risk management will become a creator of tangible value.

The relationship between operational-risk management and the business can also integrate operational-risk reporting and executive and board reporting—including straight-through processing rates, incidents detected, key risk indicators, and insights from complaints and customer calls.

Progress will require time, investment, and management attention, but the transformation of operational-risk management offers institutions compelling opportunities to reduce operational risk while enhancing business value, security, and resilience.

Joseba Eceiza is a partner in McKinsey's Madrid office; **Ida Kristensen** and **Dmitry Krivin** are partners in the New York office, where **Hamid Samandari** is a senior partner; and **Olivia White** is a partner in the San Francisco office.

The investigator-centered approach to financial crime: Doing what matters

The investigator-centered approach to fighting financial crime fosters collaboration among banks, law-enforcement agencies, and regulators for greater effectiveness, efficiency, and social impact.

By Adrian Murphy, Kate Robu, and Matthew Steinert

Over the past ten years, the level of activity in financial-crimes compliance in financial services has expanded significantly, with regulators around the globe taking scores of enforcement actions and levying $36 billion in fines. Many financial institutions have scrambled to implement remediation efforts. Financial-crimes compliance (FCC) was elevated as a function, often reporting to the chief risk or compliance officer. Staffing levels and the organizational seniority of the first and second lines of defense were greatly amplified. The activity generated has cost large institutions hundreds of millions annually and created a dynamic marketplace for consulting services and technological solutions.[1]

Technology in fact now accounts for a significant part of the financial-crimes budget. The demand has generated myriad offerings by incumbent and new vendors, which vie for the chance to alleviate their clients' many pain points. Regulatory-technology start-ups have attracted billions of dollars in investment in recent years, the bulk of it focused on know-your-customer and anti–money laundering (KYC/AML) use cases. Despite this trend, most banks report that manual processes persist. When asked, banks say that as much as 85 percent of FCC and AML activities remain administrative or nonanalytical in character (such as the manual collection of data from some systems to import into others).

The current approach, as expensive as it is, is focused on regulatory compliance. Not surprisingly, it has not been very effective in identifying and intercepting financial crime. Estimates of the volumes of funds moved through the global institutional system in proscribed transactions range from $800 billion to $2 trillion annually. The same estimates indicate, however, that the authorities intercept less than 1 percent of those amounts. The leak of the so-called Panama Papers, the files of a large offshore law firm, is a case in point. The papers showed rich and powerful individuals exploiting offshore tax regimes by funneling their wealth through hundreds of thousands of offshore companies. Not all the activity uncovered in the leak was illegal, but much of it was—*and none of it had been recognized in routine KYC/AML activity.*

To experts, this is not surprising, actually. When asked, most financial-crime AML practitioners will say that their focus is on ticking boxes for regulatory compliance rather than investigating leads and intercepting proscribed movements of funds.

Further evidence of the institutional focus on procedural compliance is the high number of defensive suspicious-activity reports (SARs). Filings have proliferated partly because the tools used for transaction monitoring and due-diligence processes are astoundingly inaccurate. Only one or two transaction-monitoring alerts per hundred is typically acted upon, for example.[2] Another example, from the world of due diligence, is illustrated in Exhibit 1. It presents a typical multifactor customer risk-rating model for the retail business of a large North American universal bank. A manually conducted expert review of the results revealed that for every 100 customers rated high risk, 72 were actually medium to low risk; furthermore, 57 of every 100 customers rated medium to low risk by the model proved on review to have a high-risk profile. To put this into perspective, a credit-risk model with this kind of performance would never be allowed into production.

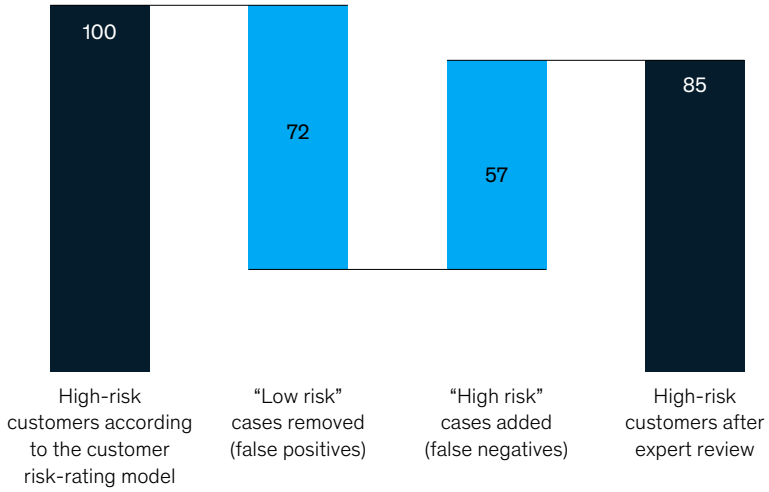
Unfortunately, most of the effort and resources invested in the industry today are focused on optimizing the status quo. These adjustments, such as calibrating thresholds for transaction-monitoring alert scenarios, adding more factors to the existing customer risk-rating models, and automating data feeds throughout the current process, have yielded only incremental improvement. If we were discussing aircraft design, an exorbitantly expensive problem-solving approach that addresses at most

[1] McKinsey Compliance Benchmarking 360 Survey, 2019.
[2] For most banks, more than 90 percent of transaction-monitoring alerts turn out to be false positives. Of those alerts that do result in a suspicious-activity-report filing, 80 to 90 percent are not acted upon.

Exhibit 1

The customer risk-rating models banks employ to detect proscribed transactions under KYC/AML mainly produce false positives and false negatives.

High-risk customers sent to enhanced due-diligence units (disguised real data example), indexed to 100



2 percent of the problem would have been set aside long ago. An increasing number of FCC/AML practitioners believe that the industry needs to go back to the basic premise of combating financial crimes. They want to clarify the mission and define a set of realizable objectives. They want a solution, in other words, that will actually *fly*.

As many industry leaders have pointed out, regulatory reform in FCC/AML is needed to help the industry shift its focus—from reducing the amount of unidentified potentially suspicious activity to increasing the amount of identified actual criminal activity.

While awaiting regulatory reform, institutions can significantly improve efficiency and effectiveness in other ways. They can work with regulators and their own internal audit group to eliminate low-value activities, automate more processes, and implement more advanced analytics. They should also develop investigative capabilities.

Some have already begun to shift their thinking in this direction. Since an investigative approach produces more meaningful results for law enforcement, it also accelerates the momentum for change. Realignment from procedural compliance to an investigator-centered approach will take time, so early movers will have a number of advantages. They will be better positioned to influence regulatory reform by redefining the meaning of effective FCC/AML. Early movers will also save more, as they divert investment away from ineffective solutions toward the technology and data needed to support the new capabilities. As these capabilities demonstrate positive impact in customer experience and overall effectiveness, institutions can begin to reduce structural costs by removing ineffectual activities.

Since the investigator-centered approach is aligned with the spirit of existing regulatory guidelines, financial institutions do not have to wait for formalized regulatory change. If they can prove that their FCC/AML activities are more productive, they

can begin to eliminate the unproductive activities even under the current regime.

From filling out forms to following real leads

The new approach proceeds from a single tenet: follow the investigator. The overwhelming majority of productive alerts—those that lead to enforcement investigations—originate with inquiries from law enforcement or other relevant external partners and "negative news"—publicly available risk-relevant information. Some productive leads also come from targeted analyses of outliers and anomalies. Most important for our discussion, however, is that relatively few investigative cases are *triggered* by automated alerts and the SAR-generating activities associated with them.

In the new approach, banks pursue high-quality leads, including specific requests from law enforcement, names or addresses associated with known transgressions, or known high-risk locations or websites. By focusing organizational FCC/AML resources in this way, banks will dramatically reduce false positives. In the United States, for example, 95 percent of investigations submitted in response to information-sharing requests by the Financial Crimes Enforcement Center (FinCEN) yield positive results. A leading institution that set up an intelligence-based investigations unit reports productive outputs in excess of 80 percent. Without such information sharing or tangible leads of some kind, less than 2 percent of alerts achieve productive results.

One argument in favor of the current SAR filing process is that it is the primary means financial institutions use to pass on information to law enforcement. FinCEN reported that law-enforcement agencies consult the SAR database 30,000 times per day, estimating a total of 7.4 million queries in 2019.[3] Our research suggests, however, that the searches are often performed to support existing cases or follow leads. Given that pattern of usage, the database could become a more comprehensive and efficient tool were banks to provide it as primary data on an automated basis. Accordingly, law enforcement would be given more access to searchable bank data, as long as all applicable privacy laws and protections were respected (such as safe-harbor provisions). At the very least the process and tools for information exchange between financial institutions and law-enforcement agencies could be significantly improved, thus eliminating the need for massive (and often unnecessary) SAR writing and filing.

Another issue with SARs is that most of the information banks recover from them amounts to fragmentary evidence of past activities. While they are useful for building prosecution cases, the delayed and incomplete bits are of less use to banks for the prevention of financial crimes than a more up-to-date and holistic view would be.

In contrast, the new approach puts investigative teams at the center of efforts against financial crime. Teams begin with seemingly small pieces of high-quality information, developing leads through intelligent follow-ups and probing. The objective is to intercept proscribed transactions and bad actors quickly. Investigators are encouraged to be proactive, connecting financial transactions and other information (such as travel or shipping itineraries, tax filings, trade invoices, and predicate crimes), using advanced analytics and new data sources. Over time, by connecting the dots in this way, institutions build a better understanding of customer behavior and the sources of risk.

Banks could object to an approach requiring them to develop investigative capabilities, countering with a traditional view that investigating financial crime is law enforcement's job. The role of banks, in this view, is limited to identifying and reporting

[3] "Prepared remarks of FinCEN Director Kenneth A. Blanco," delivered at the American Bankers Association /American Bar Association Financial Crimes Enforcement Conference, December 2019, Financial Crimes Enforcement Network, December 10, 2019, fincen.gov.

The best way for financial institutions to allocate FCC/AML resources is to set investigators to work on cases based on some kernel or snippet of information that points to unlawful activity.

unusual, suspicious, or potentially unlawful activity. Increased investigative efforts by banks would not only add to FCC/AML costs but also heighten regulatory expectations for the level of assistance banks provide to law enforcement. There is logic in this view, but the reality is that it has led to a status quo few financial institutions would deem efficient or effective. The new approach promises both improved FCC/AML results and lower costs.

A good working relationship between financial institutions and law enforcement, particularly at local-office level, makes this lead-based, clue-driven investigative approach possible. It helps banks gain visibility into emerging risks and bolsters public trust. The approach does, however, signify a shift in mindset compared with the current regulatory-driven approach. How should institutions proceed? We see five constituent actions.

1. Focus on sources of productive leads

This is the heart of the investigator-centered approach. The best way for financial institutions to allocate FCC/AML resources is to set investigators to work on cases based on some kernel or snippet of information that points to unlawful activity. As previously mentioned, the leads come from inquiries from law-enforcement or other external partners, negative news, and, to a lesser extent, analysis of abnormal activity. Collaboration with external partners, including law enforcement, is discussed in action four, below. Analysis of abnormal activity (also known as anomaly detection and outlier analysis) can become a much-improved source of productive leads with the use of modern analytical techniques. (It is a topic to which we will dedicate a technically focused article in the near future.)

Negative-news screening (also known as adverse-media screening) has been recommended by regulatory authorities in high-risk situations for some time, as part of enhanced due-diligence procedures. These do not often require continuous monitoring of negative news, but examiners have lately been expressing concern over the effectiveness of the monitoring process. This suggests that the bar may be rising, and institutions might eventually be required to apply negative-news screening in more situations and to more categories of customers.

Many financial institutions still use manual approaches for negative-news screening. With many third-party solutions available, however, they can automate this process. Investments in artificial intelligence (AI) and digital tools can dramatically improve the reach of the screening and the quality of insights it will surface. Available solutions produce potential leads but also sets of insights to help analysts assess and prioritize information in the broader context of the case. When selecting among vendors of these solutions, banks will want to consider the negative-news sources they offer;

their coverage by country, language, and customer; and the array of technical features listed, including the following features:

— data acquisition by keyword search to retrieve articles

— natural-language processing to analyze language usage and extract a set of features (such as related people and mixed-case names)

— association model to relate searched entities and articles (from unassociated to highly associated)

— event-classification model to organize by article topic (known as "event type")

— grouping of articles by subject or incident within each event type

— auto-adjudication to highlight potential false positives

— workflow functionality, including audit traceability, visualization, and integration with other tools

2. Assemble agile cross-functional investigative teams

The financial-crime investigator of the future will not be an individual but a cross-functional team. It will include former law-enforcement agents; business, fraud, and cyber experts; product specialists; data scientists; and financial analysts. The team will thus be well positioned to connect the dots in a case. In rapid development cycles, the team takes in leads, substantiates cases, probes for real material risk, and stops where evidence is limited or material risk is low. The work is centrally coordinated and strictly prioritized based on the probability of a successful outcome for law enforcement. Institutions will solicit feedback from law-enforcement agencies to ensure that their lead generation, priorities, and processes are continuously improved. Exhibit 2 illustrates how agile investigative teams operate.

Some financial institutions have already created special investigative units to work on leads from law enforcement, negative news, and high-probability internal alerts. They report success rates of 80 percent and more, taking cases with high risk exposure and the likelihood of a successful outcome. The success of these units presents a stark contrast with existing industry approaches, which mainly produce false negatives and false positives. The challenge is to make this approach scalable. That requires banks to develop a scalable operating model and invest in the necessary investigative tools and data.

3. Enhance investigative tools

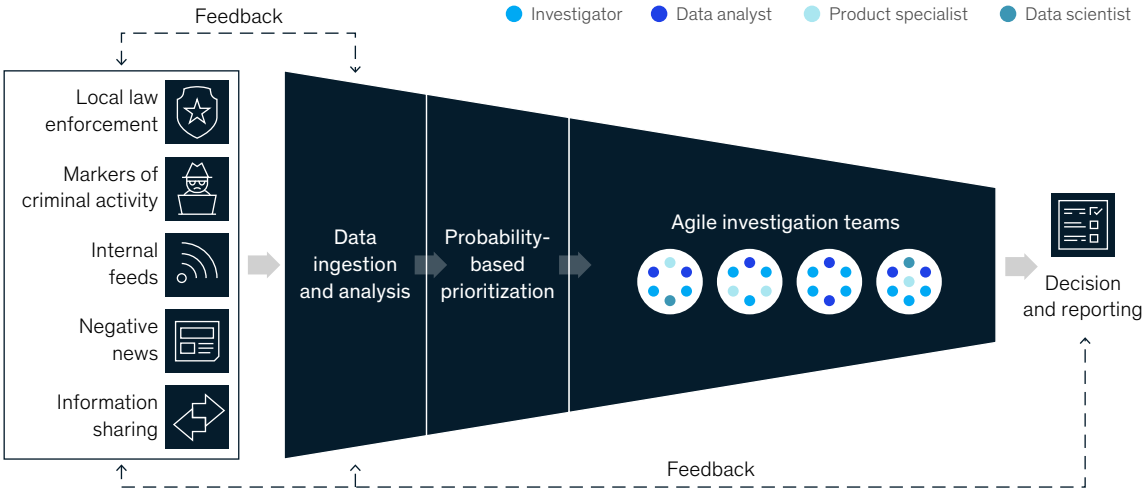
To put the investigative team at the center of financial-crimes risk management, banks must enable team members to spend the vast majority of their time investigating. Most investment in FCC/AML technology has been in internal data, models, and scenarios. Investigators have been offered little technical help, beyond workflow tools that mostly serve as task trackers and systems of record. These are rarely integrated with data sources relevant for the investigation and produce few useful insights. Investigators spend much of their time shuffling among different applications and performing a fair amount of manual data entry to create formal paper trails around cases (even for false positives).

The solution lies in deploying the data, analytics, and technology needed to free human investigators to produce better results in the highest-risk cases. The technology-aided investigation can improve outcomes dramatically, providing investigators with a more complete view of the parties and transactions involved, drawn from more diverse data sources. We will publish a dedicated article on these tools and how they work in the coming months. Here are some of the more promising enhancements:

— improved design and data visualization to inform investigators of the reason for an alert and potential courses of action (Exhibit 3 presents an example of an investigator dashboard)

Exhibit 2

The agile, cross-functional investigative team is focused on following qualified leads to identify proscribed activity.



— improved entity and network resolution to provide more clarity on high-risk connections and beneficial ownership, by using more automated data and intelligence sharing from public and private sources

— intelligent search function tailored to FCC/AML needs to produce more relevant, prioritized results

— "point and click" metrics and analysis to help investigators assess cases and determine actions

— automated prepopulation of key data items and AI-enabled text generation to support investigators in report production

— automated quality control of the output, subject to human review

— improved information storage and retrieval

4. Build a network of external partnerships

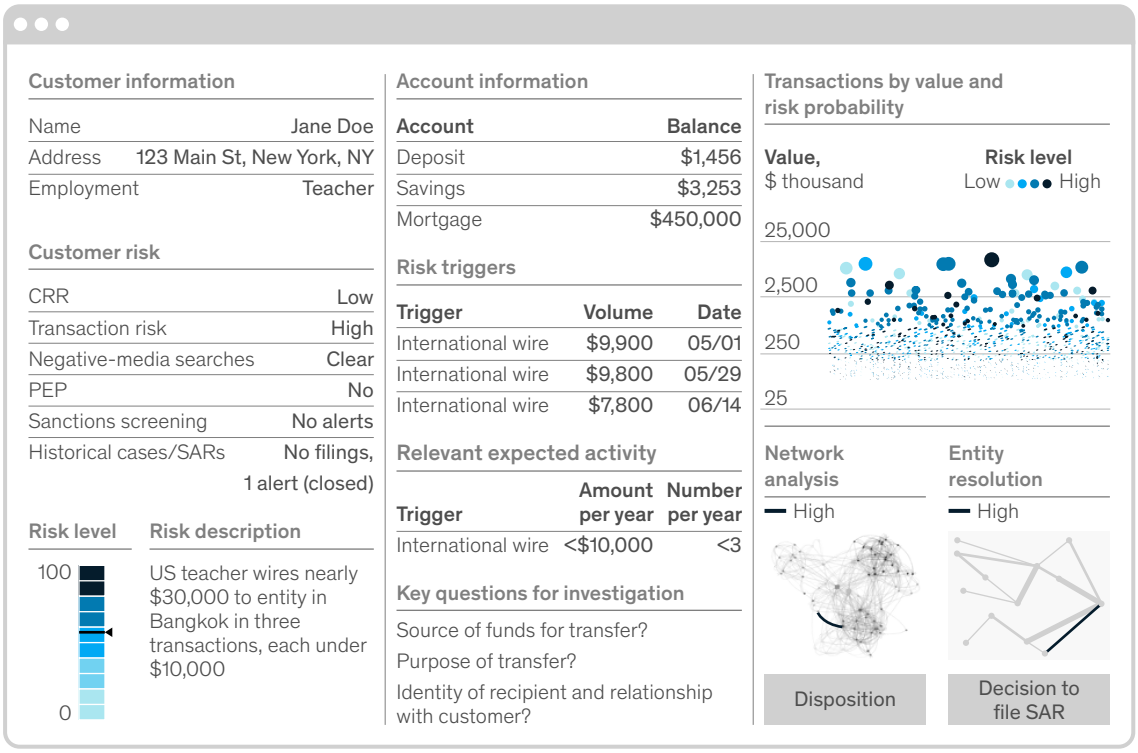
Shared intelligence is critically important for successful investigations. Collaborators include local law enforcement (for criminal trafficking), other financial institutions, tax-collection agencies, shipping companies, airlines, social-media companies, and nonprofits. In the United States, more than 100 interagency joint money-laundering task forces already exist at the federal level, and even more than that at the state level.

Collaborative networks of institutions and shared information enable more rigorous investigations. Some financial institutions have shared information with Polaris, for example, an organization that fights human trafficking. Leads and investigative insights may come in the form of potential sanctions violations, information on planned shipping routes, and retail and payments data on any number of dubious activities. With the right platform, the data

Exhibit 3

Improved dashboard design and data visualization inform investigators of the reason for an alert and potential courses of action.

Example dashboard, illustrative



Note: CRR = credit-risk rating; PEP = politically exposed person; SARs = suspicious-activity reports.

can be processed and filtered through advanced machine-learning algorithms to help investigators understand institutional exposures to the parties directly involved in the proscribed actions as well as to related parties. Investigative teams will make the connections among the flagged transactions, across all banking products and services.

Close collaboration with law enforcement is paramount, particularly at the local-office level. To build an effective operating model for this joint work, banks should bring former law-enforcement officers and specialists onto their investigative teams. Their expertise and their relationships help the institution investigate leads and better understand arising threats and local priorities. Relationships with active officers will also be instrumental in helping institutions understand the local authorities, including their processes and their people.

Financial institutions and enforcement agencies can also create public–private partnerships to improve the information flow and intercept prohibited activities. An example of such a partnership is the Joint Money-Laundering Intelligence Taskforce (JMLIT) in the United Kingdom (involving more than 40 financial institutions), the Financial Conduct Authority (FCA), Cifas (the nonprofit fraud-prevention

organization), and five law-enforcement agencies. JMLIT utilizes information from the real economy—logistics companies, airlines, retailers, hotels, and so forth. The sharing of information among industries located at different points along the chain of proscribed activities reveals a more complete picture of the nature and patterns of these activities.

5. Realign activities and platforms

While the path forward is exciting, financial institutions remain burdened by their current FCC/AML infrastructures. This limits their ability to make needed investments and allocate talent and management resources toward a more progressive solution. More important, the sheer volume of current activity and controls is deeply distracting, reducing the organization's ability to act on real risks. The "signal-to-noise ratio in the AML space," as a chief risk officer at a North American bank remarked, "is unbelievably low."

In the current absence of structural regulatory reform in this space, financial institutions should begin streamlining current FCC/AML operations to make them much more efficient and effective, while freeing up substantial resources for redirection to more valuable activities. At many institutions, FCC/AML operations were developed in reaction to intense regulatory scrutiny. Much was done quickly and under great pressure. Many banks relied heavily on industry-standard and manual solutions to save time and effort. These conditions led, unsurprisingly, to inefficient and ineffective operations, unsustainable in size and cost.

There are a few practical things financial institutions can do to substantially realign the current AML infrastructure and increase the signal-to-noise ratio.

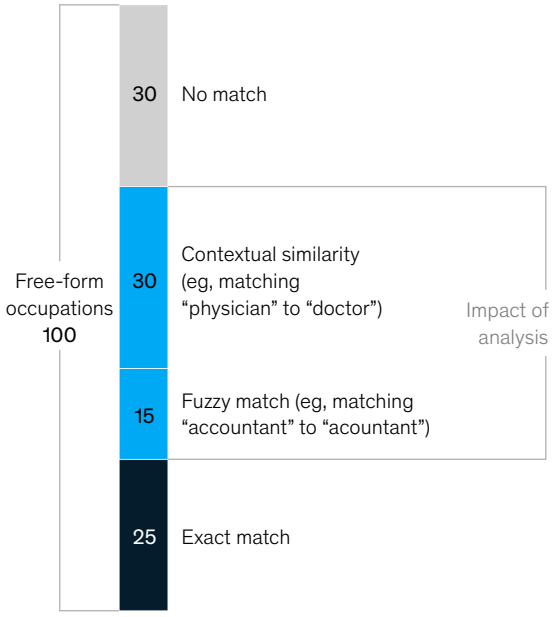
First, banks can review all FCC/AML activities and stop doing anything that is not required by regulations or beneficial to law enforcement. In our experience, institutions introduce many activities as tactical repairs but keep doing them even after they're no longer needed. Over time, layers of redundant controls and processes pile up. These should be cleared away, but with care so that the overall soundness of financial-crimes risk management is not compromised. Before removing activities that are not contributing to the effectiveness of the program, banks should of course discuss their intentions with the regulators.

Second, banks should add more intelligence to decision making, across organizational silos, databases, and systems. As an example, one North American bank used a combination of tools, including fuzzy logic and Google Dictionary, to take out 45 percent of the cases in its enhanced due-diligence pipeline. It came down to a matter of fixing data-quality issues with the occupation-code data field (Exhibit 4).

Exhibit 4

One bank significantly reduced 'noise' in its due-diligence pipeline by improving data quality.

Use of text analytics to eliminate backlogs in due diligence (disguised real data example), indexed to 100



By automating manual tasks, particularly in information and documentation management, banks can significantly reduce the strain on resources (see sidebar, "Streamlining existing FCC/AML operations: Example actions").

Particular initiatives will improve the effectiveness and efficiency of FCC/AML activities, by freeing up resources for redeployment to the actions that are truly consequential in fighting financial misdeeds. The aggregate effect of sets of initiatives can be significant. At large banks, the effects of streamlining in this way can add up to hundreds of millions of dollars (Exhibit 5).

Benefits

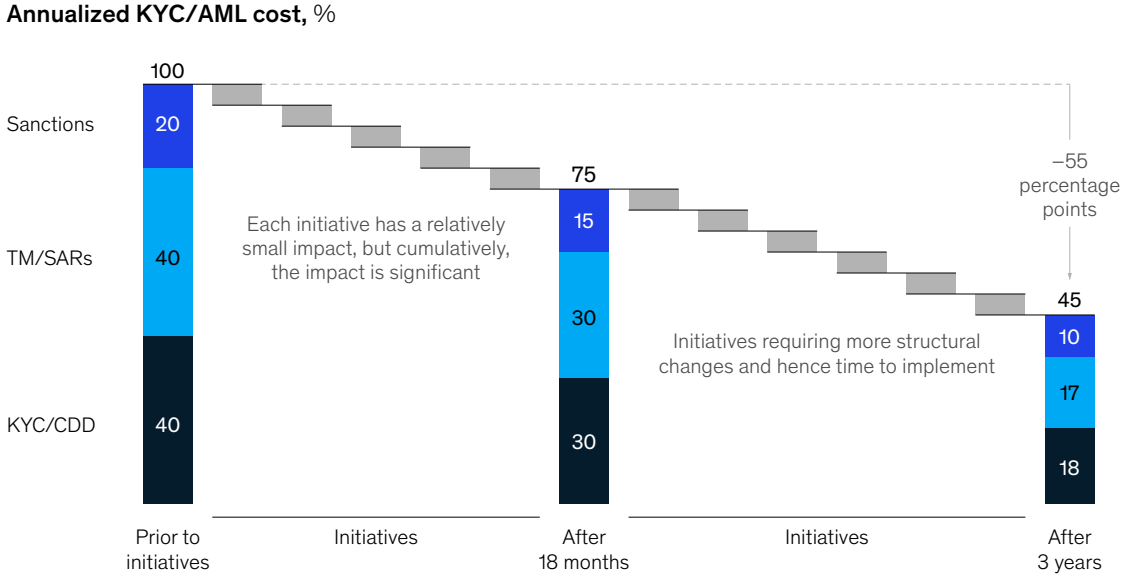
The benefits of the investigator-led approach to FCC/AML consist first of all in dramatically improved effectiveness. Activities today typically result in false-positive rates of 90 percent or more. The great majority of the work is not really useful in identifying and mitigating financial crime and proscribed transactions. The investigator-led approach is designed to reverse these proportions. It will increase the signal-to-noise ratio of current due-diligence and monitoring processes, helping to refocus efforts on the most valuable actions. Banks will be able to process far more proscribed activities.

A second benefit will be in reduced strain on organizational resources. The gains achieved from the substantial improvement of current processes and tools could be reinvested in special investigative teams that serve as much better partners to law-enforcement agencies in the investigation of crimes.

A third benefit is that the approach can elevate the profile of financial institutions as socially responsible actors in society and build public confidence in banks and the financial system. By improving detection and reducing financial crime, banks will be helping to reduce instances of money laundering, drug smuggling, human trafficking,

Exhibit 5

Financial institutions can unlock organizational resources in financial crime–related activities with a series of incrementally effective initiatives.



Note: KYC = know your customer; AML = anti–money laundering; TM = transaction monitoring; SARs = suspicious-activity reports; CDD = customer due diligence.

Streamlining existing FCC/AML operations: Example actions

Eliminate unnecessary activities. Introduce event-based review cycles for low-risk customers, ensure that the due diligence performed is commensurate with risk and regulatory requirements, remove redundant checks and excess quality assurance and control (QA/QC), reduce defensive suspicious-activity reports (SARs).

Introduce more intelligence into decision making. Improve links and optimize processes across silos to elevate performance; use behavioral information to improve client risk-rating models; maximize use of know-your-customer (KYC) information to tailor transaction monitoring; dramatically reduce false positives with machine learning–based detection models; use machine learning to improve sanctions-screening and filtering algorithms to reduce "noise" and false negatives; and use smarter search algorithms, improved entity resolution, and better data visualization and management to improve investigation productivity and outcomes.

Streamline and automate processes. Automate data collection and document handling for KYC and customer-due-diligence (CDD) procedures; automate data collection and case-file assembly sourcing from internal and external sources; improve differentiation in investigative processes by improving skills and better aligning these processes with risk objectives and business value; introduce automated data-quality checks and quality assurance and control (QC/QA).

corruption, and embezzlement. Customers and society as a whole will see the results of these investigations as highly worthwhile. Research has shown that companies with improved environmental, social, and corporate-governance profiles enjoy higher shareholder value, higher equity returns, and a reduction in downside risk.

Finally, the new approach will foster deeper regulatory engagement—and that's a good thing. To improve detection, banks will need to share more information and create public–private partnerships. They cannot do all this on their own. Regulatory incentives are needed both to encourage banks along this path and to provide them with a safe harbor for testing innovative solutions as new types of previously unnoticed proscribed transactions are discovered. Some regulators have indicated their openness to innovative approaches, and financial institutions should take up this invitation. They must ensure not only bilateral senior-level involvement but also cooperation on the ground—where the innovations meet the road, so to speak.

Institutions devote a massive amount of resources to financial-crime compliance and anti–money laundering, mostly on procedure-driven activities, the effectiveness of which is rather limited. We believe the clock has run out on refining the existing model. The field is open for an intelligence-driven, investigator-centered approach that focuses on intercepting the proscribed activities of highest risk to the organization.

Adrian Murphy is a partner in McKinsey's New York office, **Kate Robu** is a partner in the Chicago office, and **Matthew Steinert** is an associate partner in the Toronto office.

The consumer-data opportunity and the privacy imperative

As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage.

by Venky Anant, Lisa Donchak, James M. Kaplan, and Henning Soller

As consumers increasingly adopt digital technology, the data they generate create both an opportunity for enterprises to improve their consumer engagement and a responsibility to keep consumer data safe. These data, including location-tracking and other kinds of personally identifiable information, are immensely valuable to companies: many organizations, for example, use data to better understand the consumer's pain points and unmet needs. These insights help to develop new products and services, as well as to personalize advertising and marketing (the total global value of digital advertising is now estimated at $300 billion).

Consumer data are clearly transforming business, and companies are responsible for managing the data they collect. To find out what consumers think about the privacy and collection of data, McKinsey conducted a survey of 1,000 North American consumers. To determine their views on data collection, hacks and breaches, regulations, communications, and particular industries, we asked them pointed questions about their trust in the businesses they patronize.

The responses reveal that consumers are becoming increasingly intentional about what types of data they share—and with whom. They are far more likely to share personal data that are a necessary part of their interactions with organizations. By industry, consumers are most comfortable sharing data with providers in healthcare and financial services, though no industry reached a trust rating of 50 percent for data protection.

That lack of trust is understandable given the recent history of high-profile consumer-data breaches. Respondents were aware of such breaches, which informed their survey answers about trust. The scale of consumer data exposed in the most catastrophic breaches is staggering. In two breaches at one large corporation, more than 3.5 billion records were made public. Breaches at several others exposed hundreds of millions of records. The stakes are high for companies handling consumer data: even consumers who were not directly affected by these breaches paid attention to the way companies responded to them.

Proliferating breaches and the demand of consumers for privacy and control of their own data have led governments to adopt new regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in that US state. Many others are following suit.

The breaches have also promoted the increased use of tools that give people more control over their data. One in ten internet users around the world (and three in ten US users) deploy ad-blocking software that can prevent companies from tracking online activity. The great majority of respondents—87 percent—said they would not do business with a company if they had concerns about its security practices. Seventy-one percent said they would stop doing business with a company if it gave away sensitive data without permission.

Because the stakes are so high—and awareness of these issues is growing—the way companies handle consumer data and privacy can become a point of differentiation and even a source of competitive business advantage. The main findings of our research are presented below. We then offer prescriptive steps for data mapping, operations, and infrastructure, as well as customer-facing best practices. These can help companies position themselves to win that competitive advantage.

A matter of trust—or a lack thereof

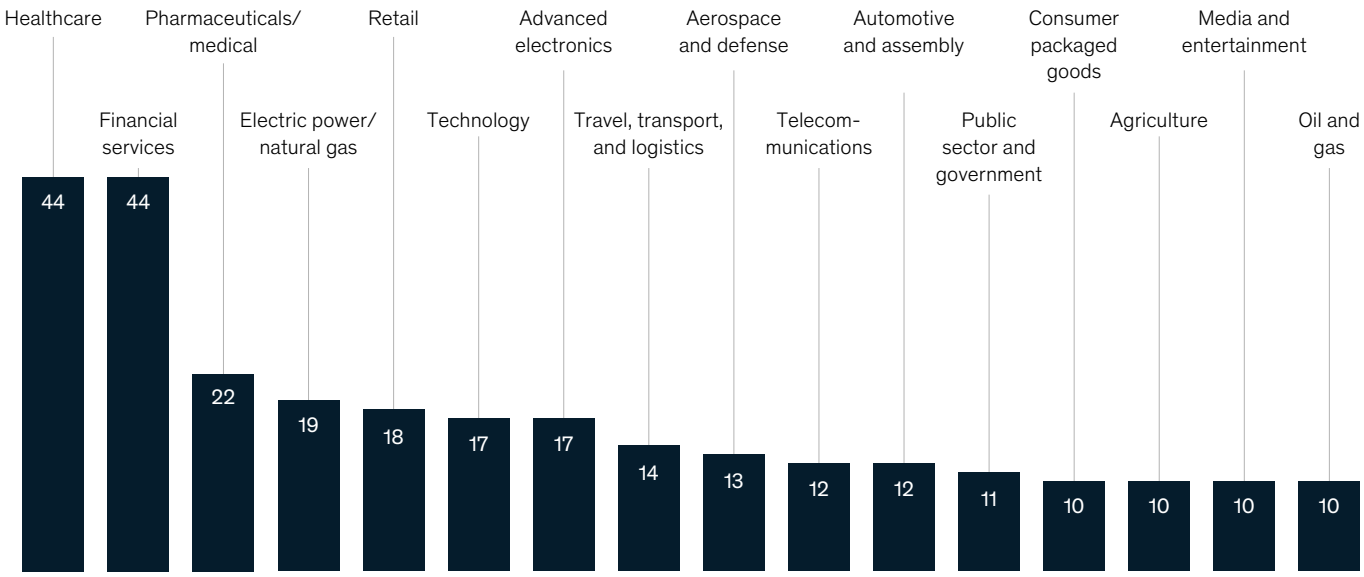
Consumer responses to our survey led to a number of important insights about data management and privacy. First, consumer-trust levels are low overall but vary by industry. Two sectors—healthcare and financial services—achieved the highest score for trust: 44 percent. Notably, customer interactions in these sectors involve the use of personal and highly sensitive data. Trust levels are far lower for other industries. Only about 10 percent of consumer respondents said that they trust consumer-packaged-goods or media and entertainment companies, for example (Exhibit 1).

About two-thirds of internet users in the United States say it is "very important" that the content

Exhibit 1

Consumers view healthcare and financial-services businesses as the most trustworthy.

Respondents choosing a particular industry as most trusted in protecting of privacy and data, % (n = 1,000)



Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

of their email should remain accessible only to those whom they authorize and that the names and identities of their email correspondents remain private (Exhibit 2).

About half of the consumer respondents said they are more likely to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested. These markers apparently signal to consumers that a company is taking a thoughtful approach to data management.

Half of our consumer respondents are also more likely to trust companies that react quickly to hacks and breaches or actively disclose such incidents to the public. These practices have become increasingly important both for companies and consumers as the impact of breaches grows and more regulations govern the timeline for data-breach disclosures.

Other issues are of lesser importance in gaining the consumer's trust, according to the survey: the level of regulation in a particular industry, whether a company has its headquarters in a country with a trustworthy government, or whether a company proactively shares cyber practices on websites or in advertisements (Exhibit 3).

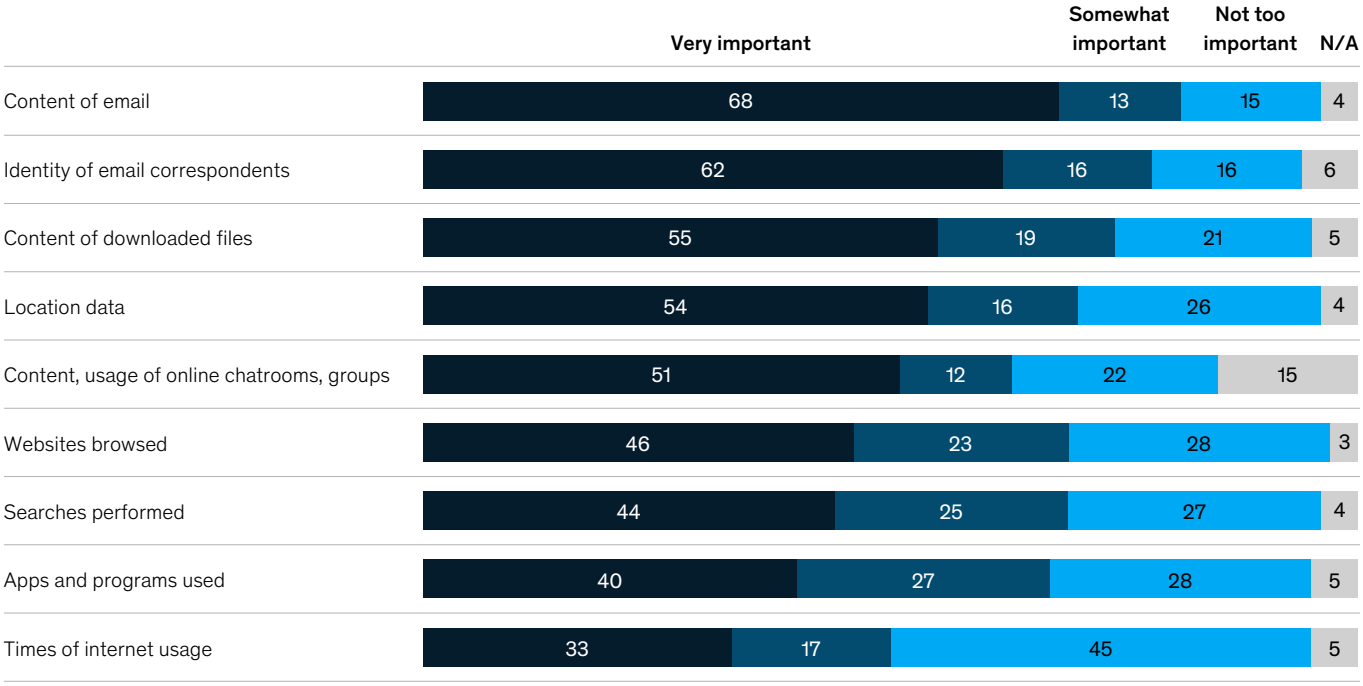
Consumer empowerment and actions

Given the low overall levels of trust, it is not surprising that consumers often want to restrict the types of data that they share with businesses. Consumers have greater control over their personal information as a result of the many privacy tools now available, including web browsers with built-in cookie blockers, ad-blocking software (used on more than 600 million devices around the world), and incognito browsers (used by more than 40 percent of internet users globally). However, if a product or service offering—for example, healthcare or money management—is

Exhibit 2

Consumer privacy and protection concerns vary by type of digital data.

Relative importance by data type, % of respondents (n = 792)



Source: Internet & American Life Project, Pew Research Center

critically important to consumers, many are willing to set aside their privacy concerns.

Consumers are not willing to share data for transactions they view as less important. They may even "vote with their feet" and walk away from doing business with companies whose data-privacy practices they don't trust, don't agree with, or don't understand. In addition, while overall knowledge of consumer privacy is on the rise, many consumers still don't know how to protect themselves: for example, only 14 percent of internet users encrypt their online communications, and only a third change their passwords regularly (Exhibit 4).

Evolving regulations

Privacy regulations are evolving, with a marked shift toward protecting consumers: the GDPR, for example, implemented in Europe in May 2018, gives consumers more choices and protections about how their data are used. The GDPR gives consumers easier access to data that companies hold about them and makes it easier for them to ask companies to delete their data.

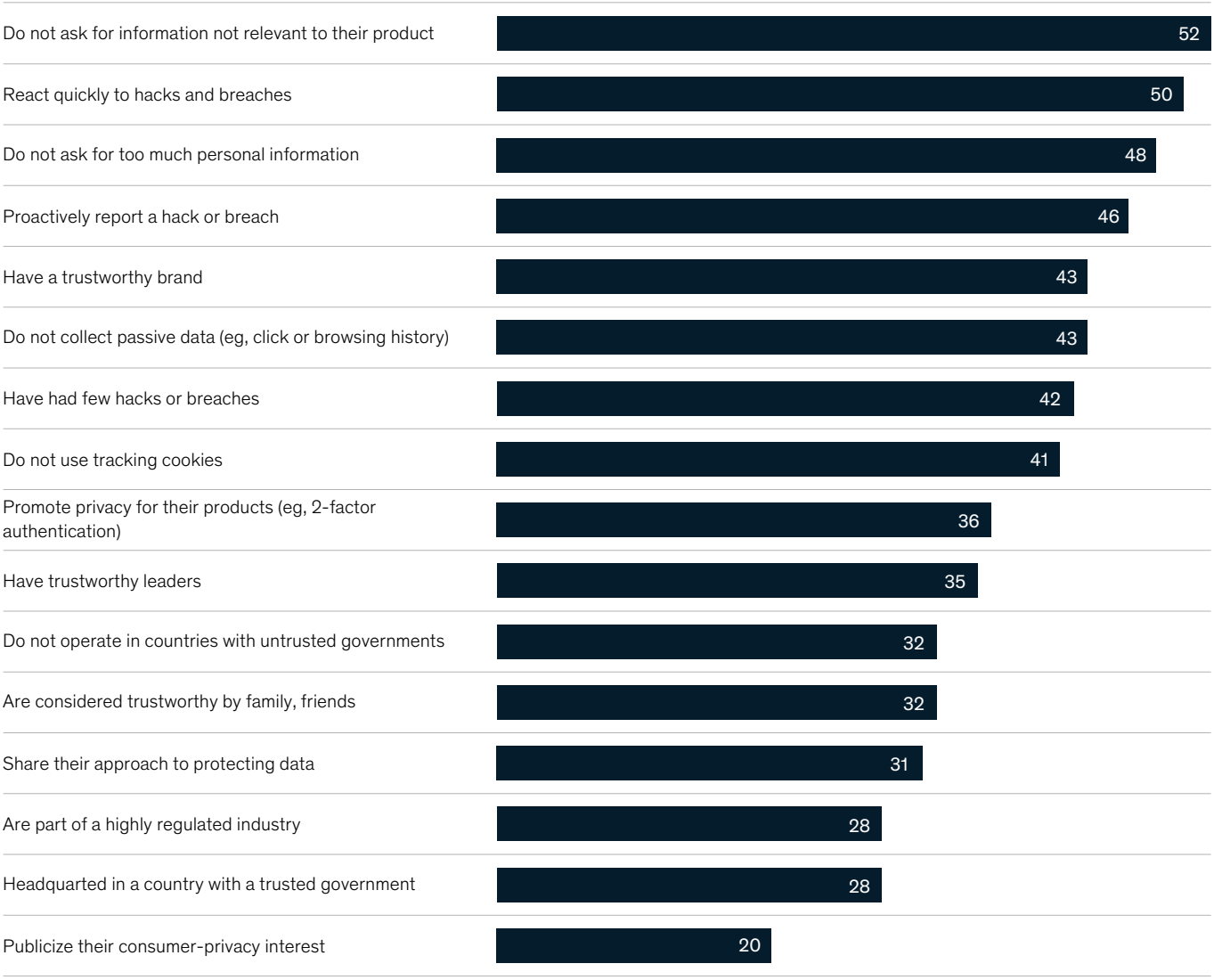
For companies, the GDPR requires meaningful changes in the way they collect, store, share, and delete data. Failure to comply could result in steep fines, potentially costing a company up to 4 percent of its global revenue. One company incurred a fine of $180 million for a data breach that included log-in and payment information for nearly 400,000 people.[1] Another was fined $57 million for failure to comply with GDPR. A side effect of this regulation is an increased awareness among consumers of their data-privacy rights and protections. About six in ten consumers in Europe now realize that rules regulate the use of their data

[1] The fine was imposed by the Information Commissions Office, the British data regulator, and is currently under regulatory process review.

Exhibit 3

Consumers trust companies that limit the use of personal data and respond quickly to hacks and breaches.

Respondent trust by practices, % (n = 1,000)

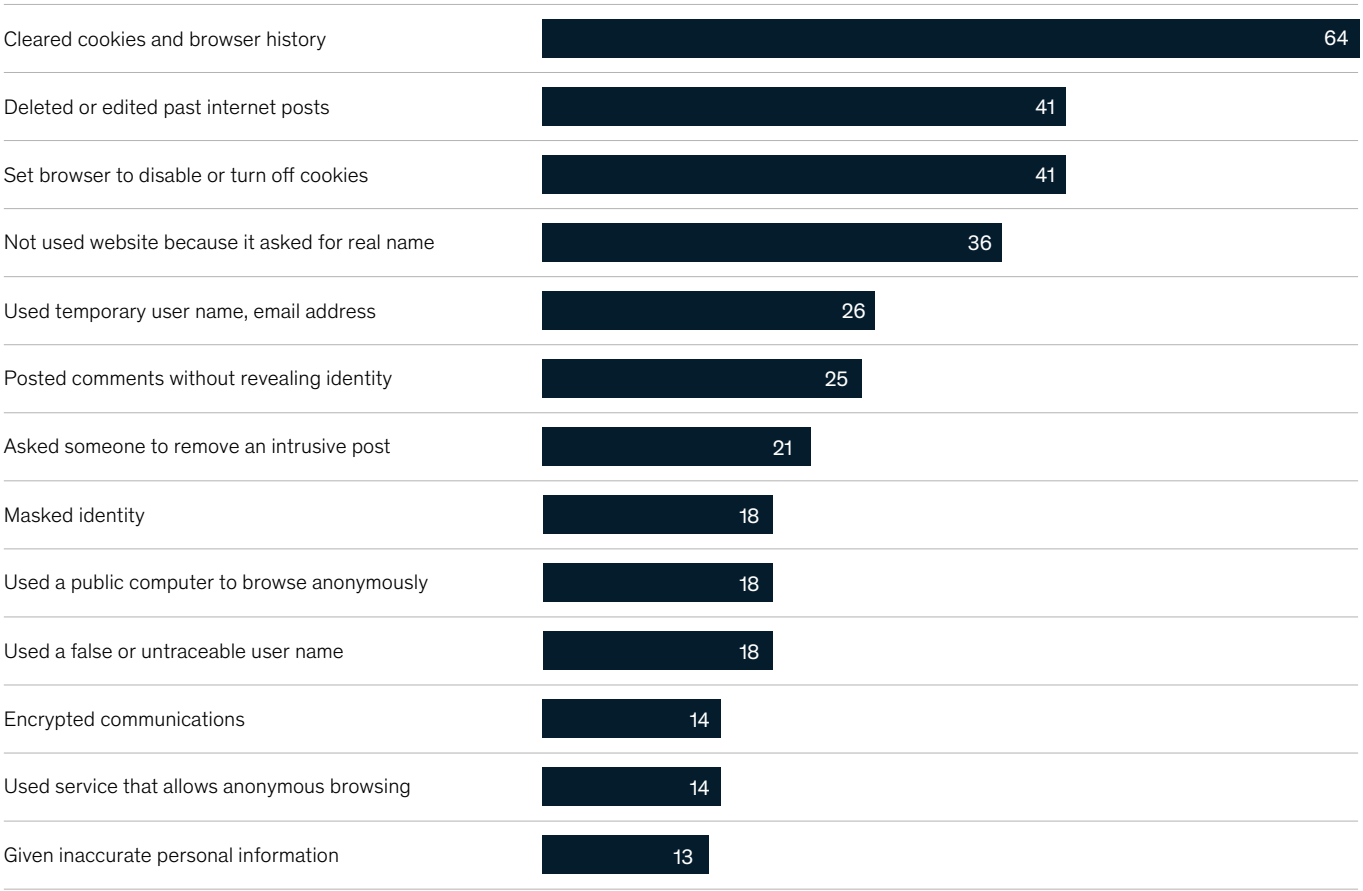


Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Exhibit 4

Consumer concerns over data collection and privacy are mounting, but few take adequate protective precautions.

Respondents taking action, % (n = 792)



Source: Internet & American Life Project, Pew Research Center

within their own countries, an increase from only four in ten in 2015.

The GDPR has been considered a bellwether for data-privacy regulation. Even in Europe, policy makers are seeking to enact additional consumer-privacy measures, including the ePrivacy regulation (an extension of GDPR), which focuses on privacy protection for data transmitted electronically. Its status as a regulation (rather than a directive) means that it could be enforced uniformly across EU member states. The ePrivacy regulation is likely to be enacted in 2020.

Beyond Europe

Governments outside Europe have also begun to enact data-privacy regulations. In Brazil, for example, the Lei Geral de Proteção de Dados, or LGPD (General Data Protection Law) will go into effect in August 2020. Brazil's previous data-protection regulations were sector based. The LGPD is an overarching, nationwide law centralizing and codifying rules governing the collection, use, processing, and storage of personal data. While the fines are less steep than the GDPR's, they are still formidable: failing to

comply with the LGPD could cost companies up to 2 percent of their Brazilian revenues.

In the United States, the California Consumer Privacy Act (CCPA) went into effect in the state in January 2020. It gives residents the right to know which data are collected about them and to prevent the sale of their data. CCPA is a broad measure, applying to for-profit organizations that do business in California and meet one of the following criteria: earning more than half of their annual revenues from selling consumers' personal information; earning gross revenues of more than $50 million; or holding personal information on more than 100,000 consumers, households, or devices.

The CCPA is the strictest consumer-privacy regulation in the United States, which as yet has no national data-privacy law. The largest fine for mishandling data was, however, issued by the US Federal Trade Commission (FTC).

Compliance investments

Companies are investing hefty sums to ensure that they are compliant with these new regulations. In total, Fortune Global 500 companies had spent $7.8 billion by 2018 preparing for GDPR, according to an estimate by the International Association of Privacy Professionals. Companies have hired data-protection officers, a newly defined corporate position mandated by the GDPR for all companies handling large amounts of personal data. Despite these measures, few companies feel fully compliant, and many are still working on scalable solutions.

A central challenge—particularly for companies that operate internationally—is the patchwork nature of regulation. Requirements are very different from one jurisdiction or market to another. To address regulatory diversity and anticipate future regulations, many companies have begun systematizing their approach to compliance. Some have begun creating regulatory roles and responsibilities within their organizations. Many are trying to implement future-proof solutions. Rather than meeting CCPA requirements only in California, Microsoft is applying them to all US citizens, though other states do not yet have policies as restrictive as the CCPA. This practice will probably become more common, as many companies are using the most restrictive legal requirements as their own standard. For most companies in the United States, this means following CCPA's guidelines.

Another difficult aspect of privacy regulation has to do with the deletion and porting of data: regulations allow consumers to request that their data be deleted or that enterprises provide user data to individual consumers or other services. For many companies, these tasks are technically challenging. Corporate data sets are often fragmented across varied IT infrastructure, making it difficult to recover all information on individual consumers. Some data, furthermore, may be located outside the enterprise, in affiliate or third-party networks. For these reasons, companies can struggle to identify all data from all sources for transfer or deletion.

Proactive steps for companies

Several effective actions have emerged for companies that seek to address enhanced consumer-privacy and data-protection requirements. These span the life cycle of enterprise data, and include steps in operations, infrastructure, and customer-facing practices, and are enabled by data mapping.

Data mapping

Leading companies have created data maps or registers to categorize the types of data they collect from customers. The solution is best designed to accommodate increases in the volume and range of such data that will surely come. Existing data-cataloging and data-flow-mapping tools can support the process.

Companies need to know which data they actually require to serve customers. Many of the data collected are not used for analytics and will not be needed in the future. Companies will mitigate risk by collecting only the data they will probably need. Another necessary step is to write or revise data-

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data.

storage and -security policies. The best approaches account for the different categories of data, which can require different storage policies.

Of further importance is the growing appetite for applied analytics. Today, leading companies need robust analytics policies. Given the proliferation of advanced machine-learning tools, many organizations will seek to analyze the high volumes of data they collect, especially by experimenting with unsupervised algorithms. But unless companies have advanced model-validation approaches and thoughtfully purposed consumer data, they should proceed with extreme caution, probably by focusing specifically on supervised-learning algorithms to minimize risk.

Operations

Leading organizations have developed identity- and access-management practices for individuals according to their roles, with security-access levels determined for different data categories. About one-third of the breaches in recent years have been attributed to insider threats. This risk can be mitigated by ensuring that data sets are accessible only to those who need them and that no one has access to all available data. Even the most robust practices for identity and access management can fail—some breaches can be caused by individuals with approved access—so additional activity monitoring can be helpful.

To act quickly when breaches do occur, organizations will want to pressure-test their crisis-response processes in advance. People who will be involved in the response must be identified and a strong communications strategy developed. One of the highest predictors of consumer trust is the speed of company reporting and response when breaches occur. Indeed, most new regulations require companies to disclose breaches very quickly; the GDPR, for example, mandates the announcement of a breach within 72 hours of its discovery.

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data. These should ensure expedited compliance with regulations and cover consumer requests for the identification, removal, and transfer of data. The processes should support data discovery in all pertinent infrastructure environments within a company and across its affiliates. Most companies today use manual processes, which creates an opportunity for streamlining and automating them to save time and resources. This approach also prepares infrastructure environments for future process developments.

Working closely with third parties, affiliates, and vendors, companies can gain an understanding of how and where their data are stored. This knowledge is especially important when third parties are supporting the development of products and features and need access to consumer data. Some companies are considering establishing review boards to support decisions about sharing data with third parties.

Infrastructure

Organizations are working to create infrastructure environments that can readily accommodate the increasing volumes of data collected, as well as attending technological innovations. Best practice is to store data in a limited number of systems,

depending on data type or classification. A smaller systems footprint reduces the chance of breaches.

Customer-facing best practices

Leading companies are building "privacy by design" into consumer-facing applications, with such features as automatic timed log-outs and requirements for strong passwords. Security and privacy become default options for consumers, while features strike a balance with the user experience.

It is important for organizations to communicate transparently: customers should know when and why their data are being collected. Many companies are adding consumer privacy to their value propositions and carefully crafting the messages in their privacy policies and cookie notices to align with the overall brand.

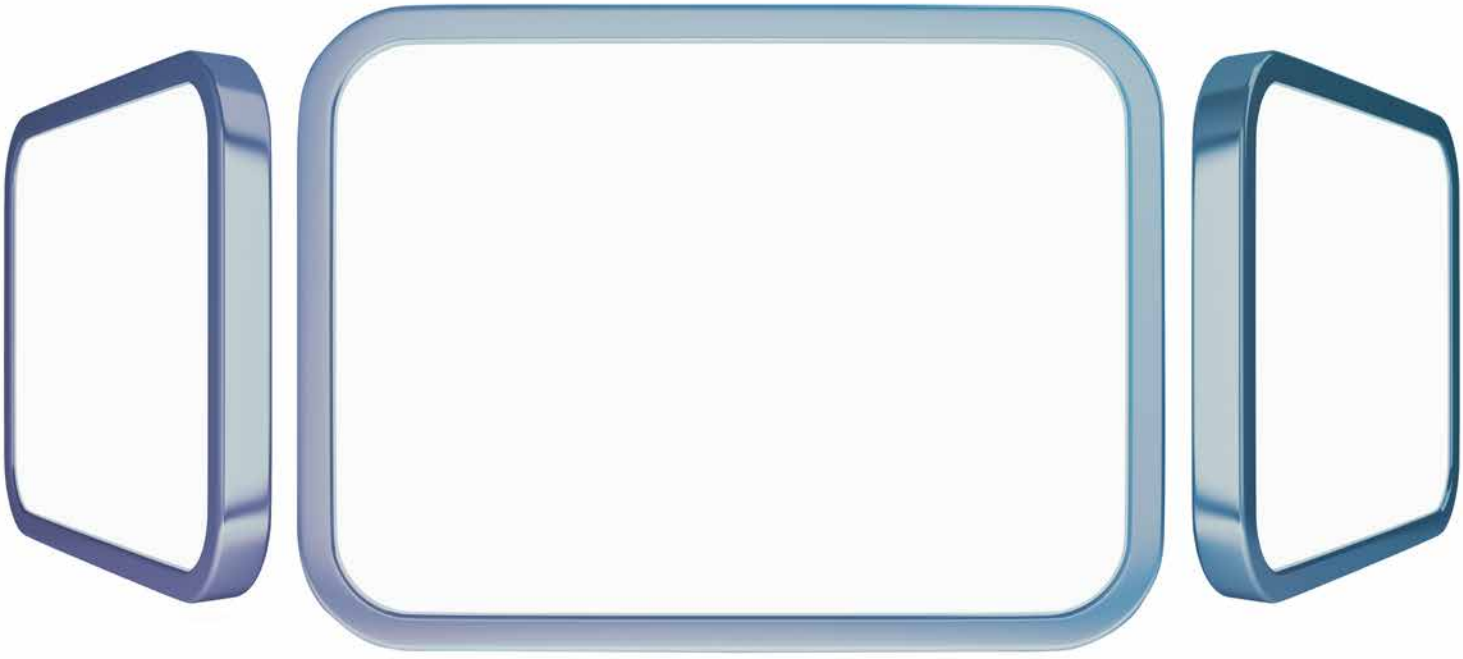
Our research revealed that our sample of consumers simply do not trust companies to handle their data and protect their privacy. Companies can therefore differentiate themselves by taking deliberate, positive measures in this domain. In our experience, consumers respond to companies that treat personal data as carefully as consumers treat their own.

Venky Anant is a partner in McKinsey's Silicon Valley office, where **Lisa Donchak** is a consultant; **James Kaplan** is a partner in the New York office; and **Henning Soller** is a partner in the Frankfurt office.

Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity

New cyberrisk management information systems provide executives with the risk transparency they need to transform organizational cyberresilience.

by Jim Boehm, James M. Kaplan, Peter Merrath, Thomas Poppensieker, and Tobias Stähle



Executives in all sectors have deepened their understanding of the dangers cyberrisk poses to their business. As hacks, cyberattacks, and data leaks proliferate in industry after industry, a holistic, enterprise-wide approach to cybersecurity has become a priority on board agendas. Companies are strengthening protections around their business models, core processes, and sensitive data. Regulators are applying their own pressures, and privacy demands are sharpening.

We asked executives at financial institutions in Europe and North America about their actual experiences with cyberrisk management and reporting. What they told us was instructive. They said cyberrisk management can be effective only when the information it is based on is accurate. Yet cyberrisk reporting at many companies is inadequate, failing to provide executives with the facts they need to make informed decisions about countermeasures. Because of the information gaps, managers often apply a standard set of controls to all company assets. As a result, low-priority assets can be overprotected, while critical assets remain dangerously exposed.

Fortunately, some leading organizations are pioneering an effective, efficient approach to cyberrisk reporting that helps executives increase corporate resilience—one that also provides transparency on cyberrisk and allows companies to integrate cyberrisk reporting with legacy systems.

Risk managers are flying blind

Many companies rely on a patchwork of reports from different sources to manage cyberrisk. Executives at these companies are unable to assess the return from their cybersecurity investments. They lack needed information about cyberrisk levels, the effectiveness of countermeasures, and the status of protection for key assets. Available data are incomplete, inconsistent, and not reliable as a basis for decision making. Executives also question the complexity of their cyberrisk-management tools, finding them overly complicated and their results incomprehensible.

Risk decision makers reserve particular criticism for governance-risk-compliance (GRC) systems. These complex software solutions can take years to implement and rarely produce a satisfying result. Like many risk-management systems, GRC software was created by technicians, and specialized expertise is required to make sense of the output. In one survey, more than half of executive respondents said cybersecurity reporting was too technical for their purposes.[1] In fact, GRC does not even focus on cyberrisk but rather covers a wide range of risk types,

[1] *How boards of directors really feel about cyber security reports*, Bay Dynamics, June 2016, baydynamics.com.

> **"We need to bring rigor to the risks related to data and protect our top assets effectively."**
>
> **—Advanced industries CIO**

> **"The current situation is a mess. We do not have the facts to decide on actions. This paralysis puts our business at risk."**
>
> **—Financial-services chief information-security officer**

including financial, legal, natural, and regulatory risks. It therefore cannot create the overview of cybersecurity that board members and regulators need. In effect, many cyberrisk managers are flying blind.

At a leading European financial institution, executives were dissatisfied with the existing cyberrisk-reporting regime. In attempting to improve it, they first assessed their experience:

— Cyberrisk reports were compiled by IT specialists for other IT specialists. As a result, the reports were very technical in nature and provided little to no guidance for executive decision making. Executives found that the reports did not help them interpret how cyberrisk is related to other risks the institution faces, such as legal or financial risks.

— At the same time, the reporting had many gaps: almost no information was provided on top risks, key assets, recent incidents, counter-risk measures, implementation accountability, the institution's resilience in the face of cyberthreats, or the return on investments in cybersecurity.

— The reporting was structured by systems, servers, and applications rather than by business units, business processes, functions, countries, or legal entities. Most reports were compiled as stand-alone documents, with no integrated view of cyberrisk across the group .

The executives had no clear sense of the overall magnitude of the risk from cyberattacks, malware, and data leaks. Neither did they know what was needed to improve protection of their key assets against the biggest threats. Several mitigating initiatives were in progress, but the reporting did not make clear what contributions if any these actions made to reducing risk. Cyberrisk managers found it difficult to decide on the areas of focus for cybersecurity investments or to justify their ultimate decisions to the board. For want of reliable reporting, the entire cybersecurity strategy was undifferentiated: all controls were being applied to all assets.

The chief information-security officer (CISO) did not know whom to contact about a given issue. Regulators reproached the institution for incomplete information. For example, the institution did not compile data on the share of employees that had completed mandatory cybersecurity training in any one location. Within the undifferentiated group-level data, high attendance in one country could easily mask low attendance in another. The training gap could be contributing to unacceptable levels of cyberrisk exposure in that country, which, however, would be invisible.

The objectives of effective cyberrisk reporting

State-of-the-art cyberrisk management requires an information system that consolidates all relevant information in one place. The most important risk metrics—key risk indicators (KRIs)—present a consistent evaluation across assets to enable the tailored application of cyberrisk controls. A given asset can be protected with the controls appropriate to its importance and the threat levels to which it is exposed.

To ready their companies for the challenges of the evolving cyberrisk-threat landscape, executives need to upgrade their approach to cyberrisk reporting and management. To address the magnitude and the complexity of the threat, companies should build a high-performing cyberrisk management information system (MIS) with three fundamental objectives.[2]

— *Transparency on cyberrisk.* Make the cyberrisk status of the institution's most valuable assets fully transparent, with data on the most dangerous threats and most important defenses assembled in a way that's accessible and comprehensible for nonspecialists.

— *Risk-based enterprise overview.* Provide decision makers with a risk-based overview of the institution so they can focus their cybersecurity investments on protecting the most valuable assets from the most dangerous threats.

— *Return on cyber investments.* Ensure the efficiency of counterrisk measures by requiring a high return on investment.

A dedicated cyberrisk MIS is not a substitute for GRC systems but rather a reporting solution addressing cyberrisk. It must be compatible with legacy systems and serve decision makers rather than specialists. It is designed to provide the information that executives need to prioritize threats and devise effective controls; it enables informed board discussions on cyberrisk strategy and helps optimize the allocation of funds.

The cyberrisk MIS should not become a burden on executives, reduced to yet another software system they must learn. Rather, it should be integrated into the existing business-intelligence system, drawing initially on existing data sources. A good cyberrisk MIS should also aspire to be future-proof, adaptable to new technologies, and able to integrate more granular data sources and more sophisticated algorithms for risk assessment as they become available.

For optimal performance, the cyberrisk MIS should be tailored to the needs of a given company. However, even a basic setup can create substantial impact. This is because a cyberrisk MIS acts as a catalyst for better, more informed decision making. Even the process of setting it up forces executives to come to a common understanding of the level of cyberrisk the company is willing to tolerate.

A strong analytical backbone

Analytics is the backbone of the cyberrisk MIS; having a strong, smart analytical system in place enables users to integrate data from different sources across a network and aggregate risks as needed. Ideally, the cyberrisk MIS should have a pyramid structure, with risk data organized hierarchically. The starting point is a simple overview, with the most important data at the highest level of aggregation. These data would describe, for example, the top global risks, differentiated by potential loss and probability. More detailed information can be added as needed, including KRIs and countermeasures for individual divisions, countries, assets, processes, and even buildings. The contact details of the people responsible for implementing the specific countermeasures can also be included.

[2] See also Thomas Poppensieker and Rolf Riemenschnitter, "A new posture for cybersecurity in a networked world," *McKinsey on Risk*, March 2018, McKinsey.com.

As shown in Exhibit 1, a top-down approach for risk-data aggregation typically involves the use of qualitative risk assessments based on scenarios. Top down is a good way to begin: it requires the least amount of data and provides significant insight in a short time. Eventually, enough risk data will become available to introduce a bottom-up approach.

The movement from top down to bottom up helps achieve cyberrisk MIS objectives quicker—by clarifying definitions of the elements of cyberrisk, providing executives with the information they need to make strategic decisions, and enhancing transparency on risk exposure and the efficacy of risk-mitigation initiatives.

Exhibit 1

The cyberrisk management information system begins with top-down risk aggregation and proceeds to a bottom-up approach.

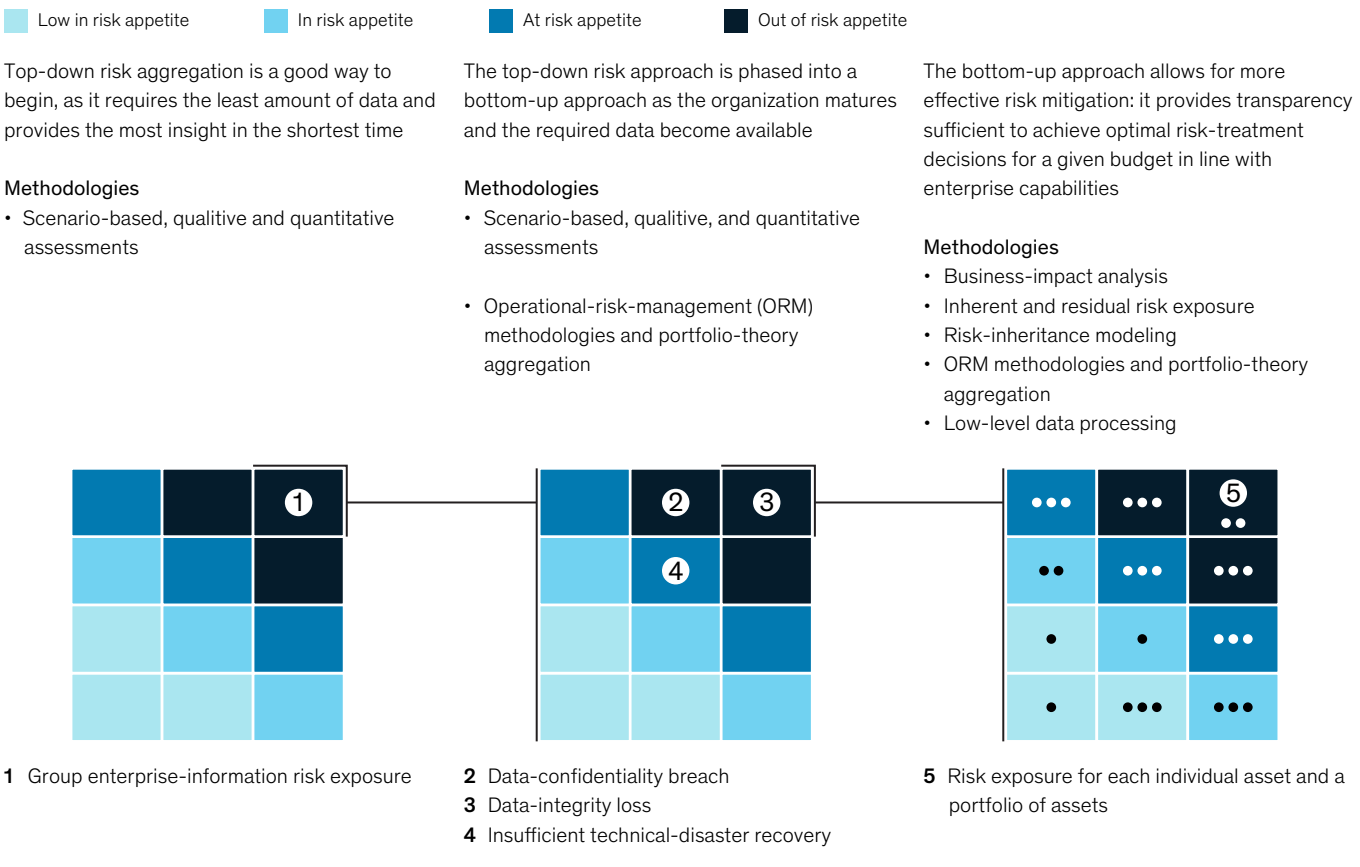


Exhibit 2 presents the "path to green": the risk-mitigation initiatives enabled by the mature bottom-up approach that bring risk indicators within the risk appetite.

A high-performing cyberrisk MIS is much more than a reporting tool. It is an integrated decision-support system, creating visibility on all relevant assets—end-user devices, applications, infrastructure, networks, and buildings. It gives decision makers access to detailed information on organizational units, regions, and legal entities. It embodies the principles of good cyberrisk governance, from definition and detection to treatment and measurement.

Implementation of the cyberrisk MIS is as critically important as its design. Even the finest aggregated scorecard or the most granular breakdown of KRIs will be useless if executives do not rely on the output for decision making. This is why a good cyberrisk MIS should be customized, reflecting the specific needs of decision makers at levels one and two of a company's hierarchy.

Catalyzing a cybersecurity transformation

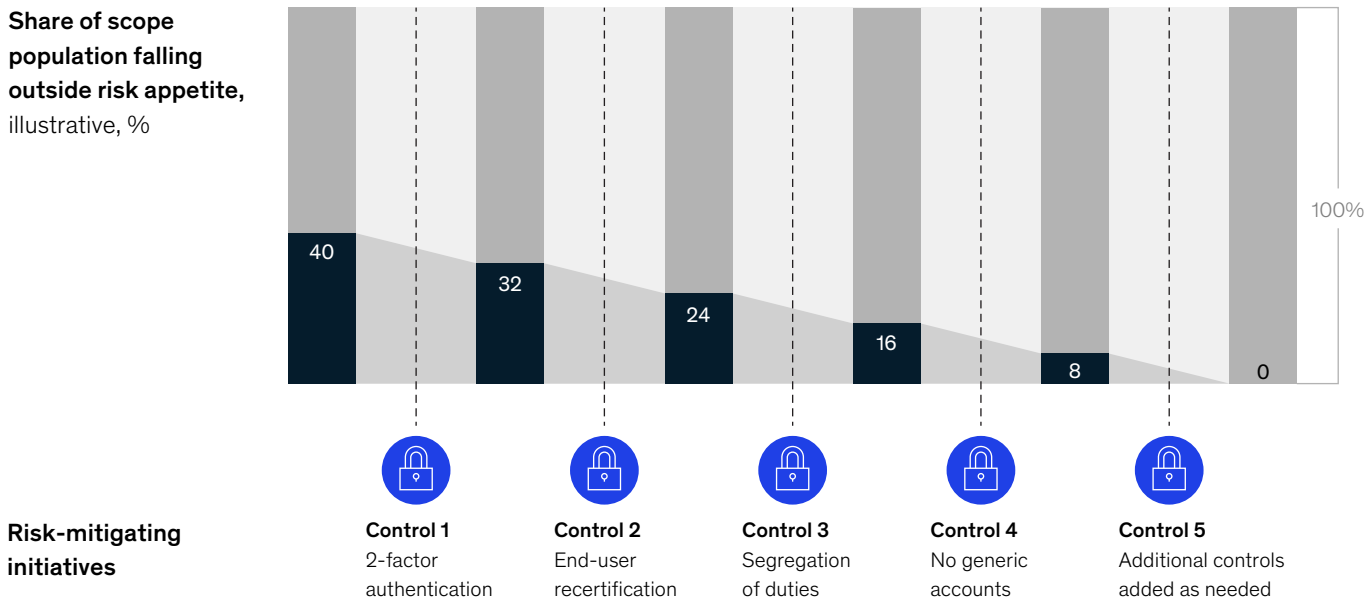
The cyberrisk MIS can catalyze a comprehensive cybersecurity transformation. This happens in the MIS implementation, which in itself is an opportunity to transform the ways companies gather information about cyberrisk and make decisions about countermeasures.

The description of a successful cyberrisk MIS implementation is remarkably congruent with that of a cybersecurity transformation. The steps are as follows:

— *Define the scope and objectives.* Leaders work up front to define objectives and deliverables. They begin by taking stock of how cyberrisk information is gathered and how executives decide on countermeasures. Cybersecurity governance and organization should be established across the whole company, with common standards and best-in-class reporting for systematic risk identification and prioritization.

Exhibit 2

Risk-mitigation initiatives indicated by the bottom-up aggregation approach provide the 'path to green.'



> "We don't want to reinvent the wheel. We need a cyberrisk management information system that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today."
>
> —Financial-services chief information-security officer

— *Avoid patchwork solutions.* The cyberrisk MIS must not be regarded as another patch. It should be comprehensive and more accessible than the previous assemblage of stand-alone reports. A good cyberrisk MIS can accommodate different degrees of maturity in different business units. For example, a module can be included that enables managers to upload static reports until dynamic data become available for automatic updates. Generally, the MIS should supply decision makers with the most pertinent information available at any given time.

— *Enhance consistency.* With improved transparency comes improved consistency. As the transformation proceeds, executives should calibrate their understanding of cyberrisk and cybersecurity. They should ask, "As an institution, how much risk are we willing to accept? What are our biggest threats? What level of protection renders a given asset safe?" Even a seemingly trivial risk topic can initiate fruitful discussions. For example, in defining cyberrisk-warning thresholds, executives can arrive at a common understanding of risk appetite, asset relevance, regulatory requirements, and the return on investments in cybersecurity.

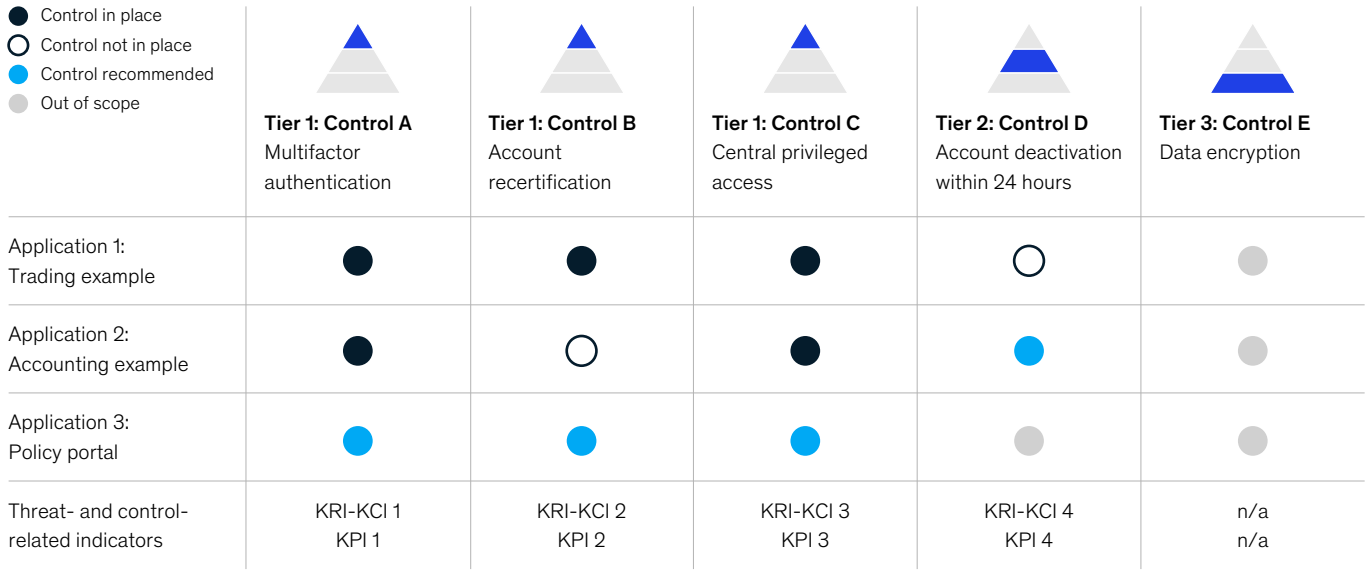
— *Shift to a risk-based approach.* One of the most powerful benefits of a good cyberrisk MIS is the risk-based approach to controls (Exhibit 3), which replaces the undifferentiated "all controls for all assets" approach. The risk-based approach focuses on the most important assets and the biggest, most probable threats. Decision makers can then allocate investments accordingly. Resilience is thereby improved without an increased cybersecurity budget. In many cases, a state-of-the-art cyberrisk MIS allows reductions in operating expenditure as well.

One company used the fact base it created in implementing its cyberrisk MIS to introduce a tiered

Exhibit 3

The cybersecurity transformation enabled through a cyberrisk management information system includes more effective, less costly differentiated controls.

Cyberrisk management information system, example



Effective information-security risk management is based on asset-centric indicators, including key risk indicators (KRIs), key compliance indicators (KCIs), and key performance indicators (KPIs), revealing compliance issues as well as current and forecasted residual risk exposure.

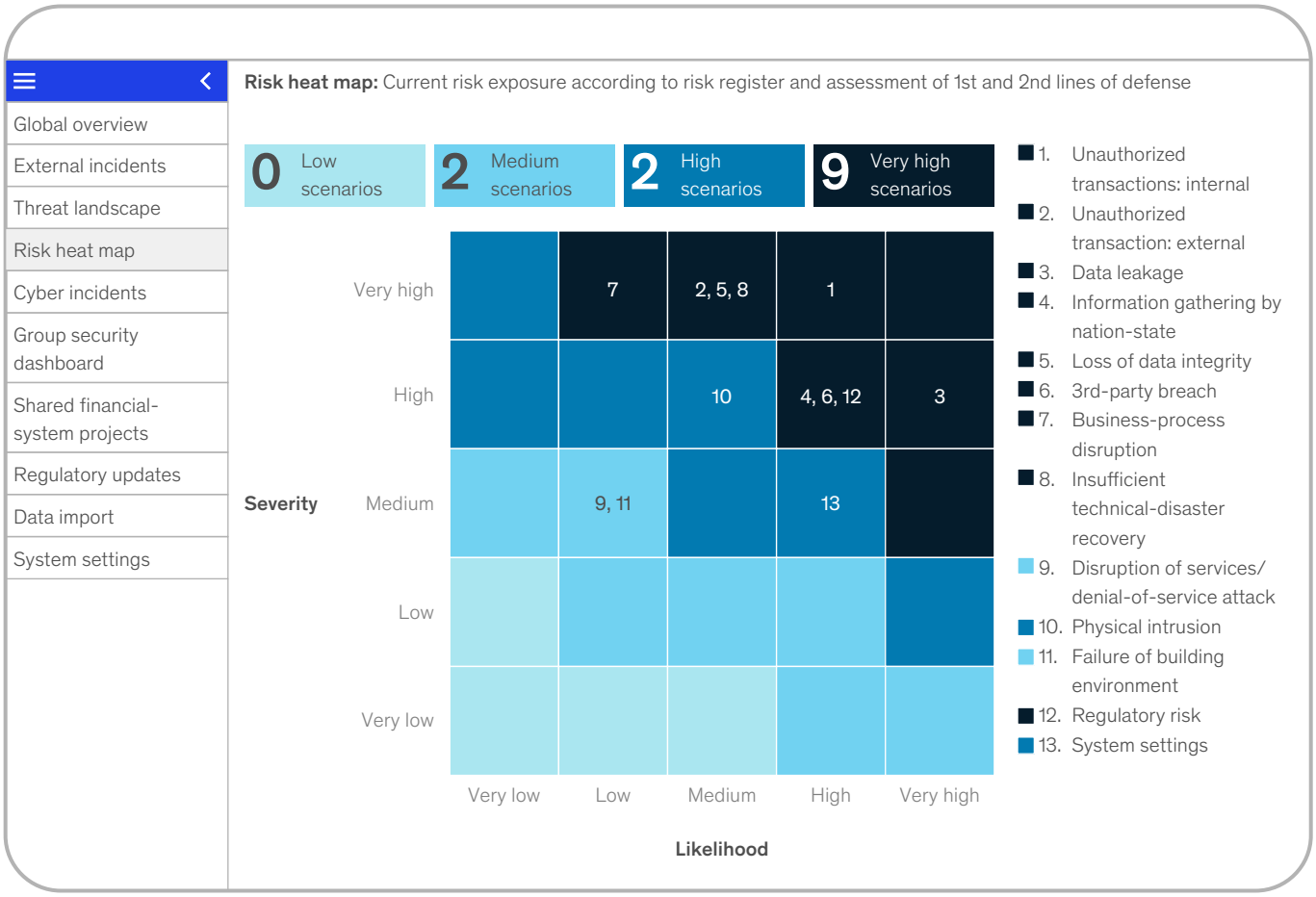
control regime. The company subjected only its most critical, most vulnerable assets (class one) to the full arsenal of controls—from multifactor user authentication to deleting, after 24 hours, the accounts of anyone who left the company. By contrast, it applied only basic controls to the least critical assets (Exhibit 3). As a result of this tiered approach, the company was able to improve compliance with relevant regulatory requirements while reducing the residual risk level. At the same time, it also reduced costs: both direct costs (such as for software licenses) and indirect costs (such as those incurred through the use of cumbersome, undifferentiated controls, even those for low-level applications).

With the right approach, a cyberrisk MIS cybersecurity transformation will provide board-level executives with a concise and easily digestible overview of top cyberrisks. Exhibit 4 shows an MIS cyberrisk dashboard, with the risk heat-map tab open. Other tabs provide the chief risk officer and the chief information officer with the KRIs, KPIs, controls, and progress reports for different functions, organizational levels, and applications. The transformation will foster the use of a common language and a fact-based approach to cyberrisk across the entire institution. Over time, the institution will accrue the benefits of greater cyberrisk transparency, improved cybersecurity efficiency, and greater cyberresilience.

Exhibit 4

The cyberrisk dashboard includes a risk heat map.

Cyberrisk dashboard, example



The fast track to impact

The modular design of the recommended cyberrisk MIS makes it possible to implement a viable version in parts over a period of three to six months, depending on an organization's needs and complexity. For many companies, the most important components—the underlying data structure, the analytical backbone, and the visualization interface—are already in place. In all likelihood, the initial version of a next-generation cyberrisk MIS will not be fully customized to the needs of a given company, but it will be a real working product, not a dummy.

The implementation journey begins with a project team, experts, risk managers, data owners, IT, and other stakeholders jointly determining specific requirements, relevant processes, and data availability. In the building stage, live trial sessions are held to give executives a chance to provide

> **"Step by step, we made the cyberrisk MIS our own. The whole process took less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the-shelf solution."**
>
> **—Cyberrisk MIS user**

feedback on MIS utility. After needed adjustments, the scope is widened and the system is deployed to the entire organization.

Leading institutions that have implemented state-of-the-art cyberrisk management information systems have seen significant improvement in the efficacy of cyberrisk detection and remediation. The platform links operational data with groupwide enterprise-risk-management information accurately and consistently. These cyberrisk systems can become the basis for a comprehensive cybersecurity transformation and part of a holistic risk-based approach to cybersecurity, reducing risk, raising resilience, and controlling costs.

Jim Boehm is an associate partner in McKinsey's New York office, where **James M. Kaplan** is a partner; **Peter Merrath** is an associate partner in the Frankfurt office, where **Tobias Stähle** is a senior expert; and **Thomas Poppensieker** is a senior partner in the Munich office.

The authors wish to thank Rolf Riemenschnitter for his contributions to this article.

Risk Practice leadership

Cindy Levy
Global
Cindy_Levy@McKinsey.com

Fritz Nauck
Americas
Frederic_Nauck@McKinsey.com

Philipp Härle
Europe
Philipp_Haerle@McKinsey.com

Gabriel Vigo
Asia
Gabriel_Vigo@McKinsey.com

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

Kevin Buehler
Risk Dynamics, Cyberrisk
Kevin_Buehler@McKinsey.com

Marco Piccitto
Risk People
Marco_Piccitto@McKinsey.com

Holger Harreis, Olivia White
Risk Knowledge
Holger_Harreis@McKinsey.com
Olivia_White@McKinsey.com

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

In this issue

Responding to the coronavirus: The minimum viable nerve center
Supply-chain recovery in coronavirus times: Plan for now and in the future
How banks can ease the pain of negative interest rates
Banking imperatives for managing climate risk
The future of operational-risk management in financial services
The investigator-centered approach to financial crime: Doing what matters
The consumer-data opportunity and the privacy imperative
Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity

This McKinsey Practice Publication meets the Forest Stewardship Council® (FSC®) chain-of-custody standards. The paper used in this publication is certified as being produced in an environmentally responsible, socially beneficial, and economically viable way.

Printed in the United States of America

June 2020
Designed by Global Editorial Services

McKinsey.com