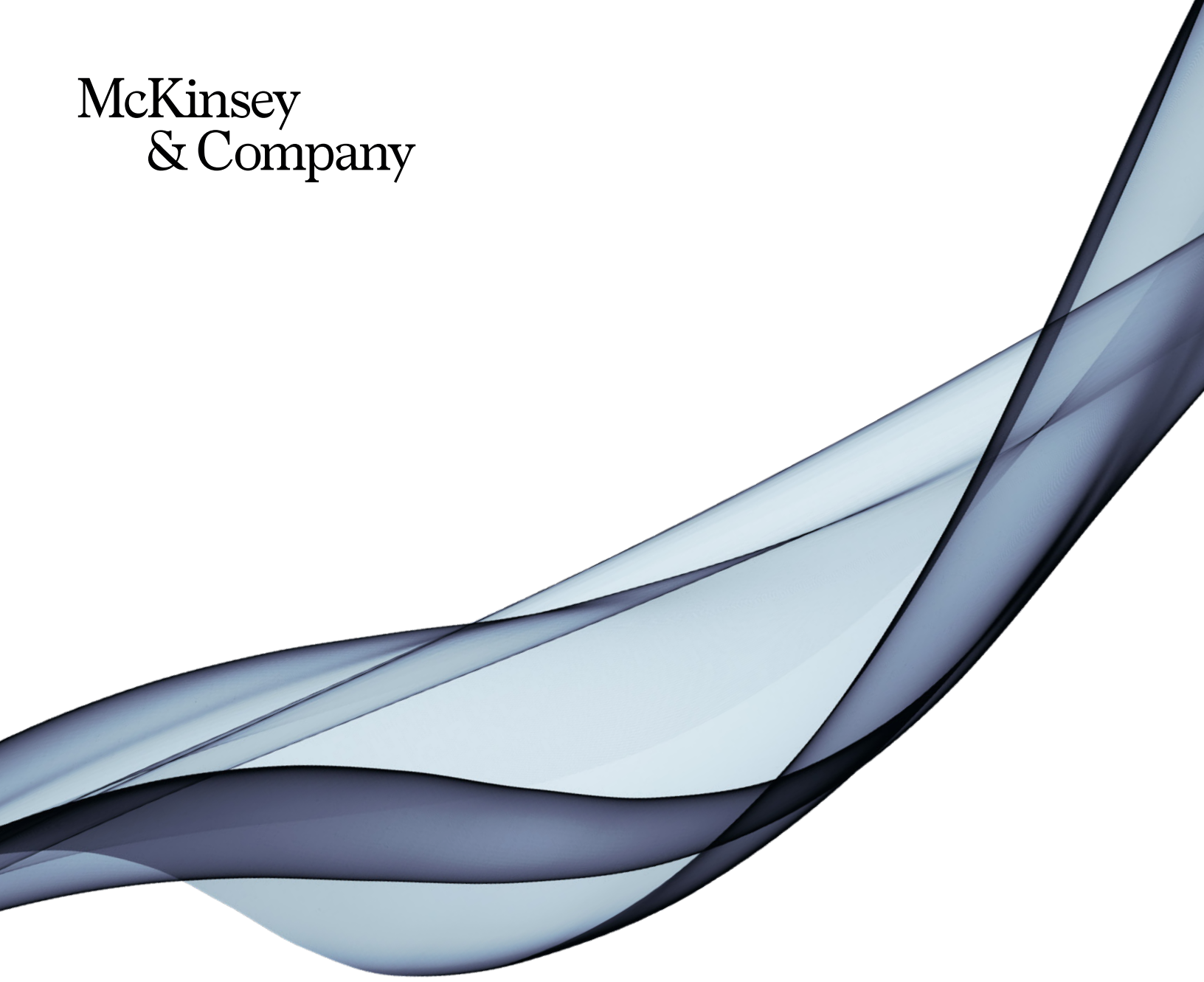
McKinsey & Company



McKinsey on Risk

Strengthening institutional resilience has never been more important

Number 11, August 2021

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

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

Cover image:
© oxygen/Getty Images

Table of contents

Introduction

In January 2021, when we last issued *McKinsey on Risk*, the world was coming to grips with the prospect of a second pandemic year. The number of recorded cases of COVID-19 had climbed to new heights through the final months of 2020 and into the new year. Both developed and developing nations continued to struggle with the 21st century's worst human tragedy. Since then, epidemiological uncertainty has deepened as another, even more powerful pandemic wave swept the globe. In the more developed nations, its effects were at last mitigated by the arrival and widespread distribution of vaccines. In lower-income economies, however, the fight against the spread of the virus—and the struggle to acquire vaccines—continues.

Coincident with the health crisis is an unusually strong, if uneven, economic revival. The global economy has been restarted by governments voluntarily lifting restrictions on the production and delivery of goods and services. The process has resulted in unusual effects, including strong expressions of pent-up demand colliding with supply-chain discontinuities. Inflation has reappeared in a financial environment defined during this period—especially in Europe and the United States—by low interest rates, fiscal accommodation, and significant stimulus spending.

Steep business challenges were present before the arrival of COVID-19. The pandemic, the resulting economic crisis, and the uneven recovery have complicated the risk environment. Uncertainty is unfolding across this environment in nonlinear patterns. Threats become more severe and occur with greater frequency. As companies adjust to changing risk parameters in several dimensions while keeping an eye on the balance sheet, how should they think about profitability and growth? Our lead article, "The resilience imperative: Succeeding in uncertain times," emphasizes that to thrive in the 2020s, companies and institutions need to become *resilient*—able to withstand diverse and unpredictable threats and emerge stronger in the changed business landscape.

Gearing up for life beyond the crisis, companies face an array of intersecting stresses in addition to tightening market competition. These include the demands of digitization and automation, whose transformative force shows no signs of weakening. Cyberthreats, partly stoked by rising geopolitical tensions and ransomware, increasingly endanger corporate functions, data security, and productive operations.

Here you will find articles that reflect McKinsey's latest thinking on risk and offer concrete, experience-based steps toward solving the most compelling risk problems. Cutting through signal-to-noise distortion, our risk authors discuss best practices for the returning credit cycle and for driving a model-risk transformation to correct for pandemic discontinuity. All leading organizations will find worthwhile considerations for managing the broad enterprise cybersecurity environment.

As we stress in "The resilience imperative: Succeeding in uncertain times," companies cannot afford to be either inflexible or imprudent. Without taking on sufficient risk, they will be unable to respond or innovate to meet changing circumstances. But those too focused on financials, growth, or expansion may take on risk that prevents long-term success. Our overarching objective is to help organizations navigate those straits and grow stronger in the coming decade.

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

Thomas Poppensieker
Chair, Risk & Resilience Editorial Board

The resilience imperative: Succeeding in uncertain times

Strengthening institutional resilience has never been more important.

by Fritz Nauck, Luca Pancaldi, Thomas Poppensieker, and Olivia White

2020 was a wake-up call. To thrive in the coming decade, companies must develop resilience—the ability to withstand unpredictable threat or change and then to emerge stronger.

This perspective piece introduces our approach to resilience. "Develop resilience" is easy to say but hard to define, and yet harder to do. In this article, we reiterate the imperative, define the components of resilience, and introduce the approaches companies can take to become more resilient. In the coming months, we will publish a series of more detailed articles on the topic, focused on the actions that institutions of different types can take to measure and improve their resilience.

The resilience imperative

The world is undergoing increasingly rapid, unpredictable, and unprecedented change. But across industries, most companies have remained persistently focused on near- and medium-term earnings, typically assuming ongoing smooth business conditions. The COVID-19 pandemic heralds the need for a new approach.

Catastrophic events will grow more frequent but less predictable. They will unfold faster but in more varied ways. The digital and technology revolution, climate change, and geopolitical uncertainty will all play major roles (exhibit).

The digital revolution has increased the availability of data, the degree of connectivity, and the speed at which decisions are made. This offers transformational promise but also comes with potential for large-scale failure and security breaches, together with rapid cascading of consequences. It also increases the speed at which a company's reputation can change in the eyes of consumers and employees.

The changing climate presents structural shifts to companies' risk–return profiles, which will accelerate nonlinearly. Companies need to navigate concerns for their immediate bottom line together with pressures from governments, investors, and society at large. All this, while natural disasters are growing more frequent and severe.

An uncertain geopolitical future provides the backdrop. The world is more interconnected than ever before, from supply chains to travel to the flow of information. But these ties are under threat, and most companies have not designed their role in the global system for robustness to keep functioning smoothly even if connections are abruptly cut.

In a world where the future is uncertain and change comes fast, companies need to look beyond short-term performance and basic organizational health. They must be able not only to withstand unpredictable threat or change but to emerge stronger. In short, they need to be resilient.

Broad-based resilience: Beyond financials

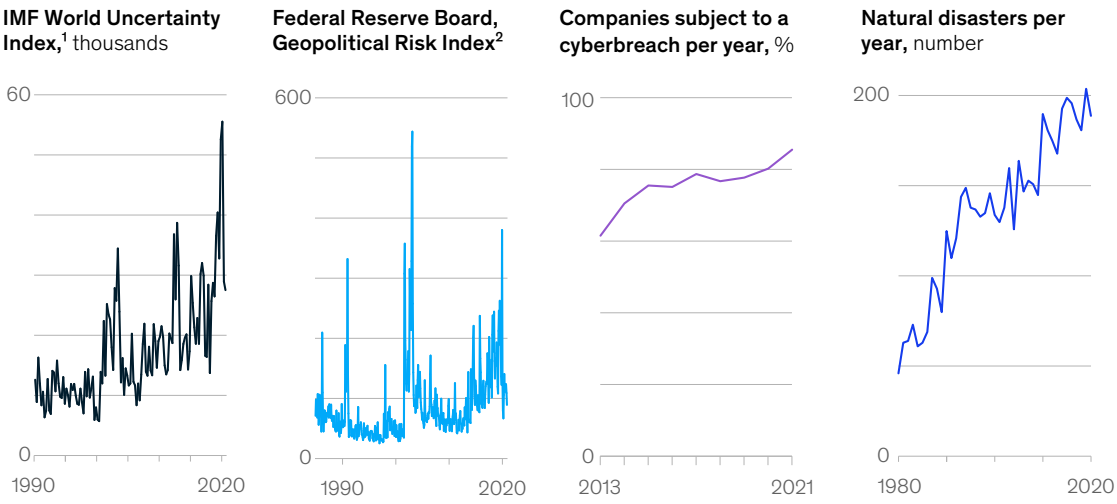
Organizations cannot afford to be either inflexible or imprudent. Those unwilling to take sufficient risk will not respond or innovate to meet changing circumstances. But at the same time, those too focused on financials, growth, or expansion may take on risk that kills their long-term success. Industries have developed specific resilience capabilities, but when disruptions occur, "surprise gaps" become visible (see sidebar, "Resilience capabilities and 'surprise gaps' in select industries").

Many companies have thought about such risk–return trade-offs in financial terms, making sure they have the financial reserves needed to withstand some uncertainty around a single planning scenario.

But today's world demands more than financial resilience. As an example, take climate change. Severe climate hazards will threaten the sourcing, production, and distribution of products and services and can come from both nearby and afar in the era of global supply chains. Moreover, companies must take a stance on the role they want to play in reducing emissions, accounting for expectations from governments, employees, customers, shareholders, and society at large. Such climate adaption and mitigation, together with technology change, will shift business mix and business models, and companies will need the flexibility to respond.

Exhibit

Disruption is becoming more frequent and more severe.



[1]IMF = International Monetary Fund. Based on the percentage of the word "uncertain" (or its variant) in the Economist Intelligence Unit country reports.
[2]Automated text-search results from the electronic archives of 11 newspapers: *Boston Globe*, *Chicago Tribune*, *Daily Telegraph*, *Financial Times*, *Globe and Mail*, *Guardian*, *Los Angeles Times*, *New York Times*, *Times*, *Wall Street Journal*, and *Washington Post*. Index was calculated by counting the number of articles related to geopolitical risk in each newspaper for each month (as a share of the total number of news articles).
Source: CyberEdge; Swiss Re

Internally driven change also requires a broad view of resilience. Consider a company-wide digital and analytics transformation addressing both internal processes and product and service delivery to customers. While efficiency and the art of the possible expand, so does the potential for broadscale technological failure or massive cyberincursion. Employees need to develop new skills and different ways of working together. Analytics offers new horizons but also can embed bias in decision making.

We believe that true resilience requires balanced focus on six dimensions: financials, operations, technology, organization, reputation, and business model.

Financial resilience

Institutions must balance short- and longer-term financial aims. A solid capital position and sufficient liquidity enables organizations to weather rapid drops in revenue, increased cost, or credit issues. Most companies must protect themselves against the deterioration of markets and reduced access to capital, debt, or equity or, for financial institutions, decreases in net interest income and credit loss.

Operational resilience

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

Technological resilience

Resilient organizations invest in strong, secure, and flexible infrastructure, including to manage cyberthreats and to avoid technology breakdown. They maintain and make use of high-quality data in a way that respects privacy and avoids bias, compliant with all regulatory requirements. At the same time, they implement IT projects both large and small—at high quality, on time, in budget, and without breakdown—to keep pace with customer needs, competitive demands, and regulatory requirements. In case something does go wrong, they maintain

Resilience capabilities and 'surprise gaps' in select industries

Industry	Resilience capabilities	'Surprise gaps'
Advanced electronics	Technological-innovation strengths; standardization, flexibility, and regionalized production and supply chains; product compliance, especially to international standards, regulatory regimes, and customer specifications	Business-model innovation around software, change in system architecture, and disruptive shift in customer demands; environmental regulations, including recycling and European Green Deal; safeguarding crucial supplies (eg, chips, semiconductors); cash preservation and cost management against revenue loss
Airlines	Flight-network resilience in response to local or temporary disruptions due to extreme weather or local emergencies (eg, pandemics)	Climate change and environmental regulations; behavioral changes; potential regulations limiting short-distance flights
Banking	Regulatory and capital-market compliance minimizing financial crimes, insider trading, and market manipulation	Business continuity after COVID-19 crisis to enable work from home while maintaining flexible working model in accordance with banking secrecy and confidentiality of data
Pharmaceuticals	Portfolio management across R&D pipeline and product life cycle	Cluster risk in the supply of active pharmaceutical ingredients due to the concentration of contract manufacturing and organizations in China and India
Telecommunications	Network resilience; prevention of network failure	Shift of competitive positions toward new competitors, given convergence of telecommunications and media

robust business continuity and disaster-recovery capability, avoiding service disruptions for customers and internal operations.

Organizational resilience

Resilient institutions foster a diverse workforce in which everyone feels included and can perform at their best. They deliberately recruit the best talent, develop that talent equitably, upskill or reskill employees flexibly and fast, implement strong people processes that are free of bias, and maintain robust succession plans throughout the organization. Culture and desired behaviors are mutually reinforcing, supported by thoughtfully developed rules and standards to which adherence is enforced while also promoting fast and agile decision making.

Reputational resilience

You are what you do. Resilient institutions align their values with their actions, with their words. A wide range of stakeholders—from employees to customers to regulators to investors to society at large—increasingly looks to hold organizations accountable in a range of ways, spanning from their brand promise to their stance on environmental,

social, and governance (ESG) issues. Resilience demands a strong sense of self—enshrined in mission, values, and purpose—which guides actions. It also requires flexibility and openness in listening to and communicating with stakeholders, anticipating and addressing societal expectations, and responding to criticism of organization behavior.

Business-model resilience
Resilient organizations maintain business models that can adapt to significant shifts in customer demand, the competitive landscape, technology, and the regulatory terrain. This involves maintaining an innovation portfolio and valuing entrepreneurship. Particularly during times of crisis, resilient organizations will place strategic bets to evolve their business models.

Anticipating and responding

Institutions with the capabilities to prepare for and respond to disruption dynamically are more resilient across the six dimensions.

Anticipation
Developing the understanding and fact base to anticipate relevant future scenarios enables organizations to pressure test their resilience and to anticipate some types of disruption. By examining specific significant potential disruptions, institutions will learn more about gaps in their resilience across the six dimensions. Specific, hypothetical supply-chain disruptions, for example, probe a part of operational resilience; cyberattack scenarios are most relevant to technological resilience; and physical climate-risk events require several types of resilience. At the same time, institutions can systematically identify potential industry-wide disruption stemming from a range of sources: from technical change to macroeconomic downturns, or from geopolitical disruption to major regulatory shift. Not all such disruptions can be anticipated. But some can, at least in part, and early anticipation can provide significant advantage, as demonstrated through numerous examples during the COVID-19 pandemic.

Response
Institutions cannot anticipate or prepare for all disruptions. The capability to respond rapidly and effectively after something happens can make a determinative difference in company success. In the face of company-specific crises, a poor and indecisive response can drive as much as half of the lost shareholder value. On the flip side, companies that respond well stand to gain. Organizations that respond early to industry disruption or economic downturn can create competitive advantage that drives superior performance through the next industry cycle. For example, as measured through total returns to shareholders, top-quintile performance through the global financial crisis (2007–11) outperformed other companies in 2017 by more than 150 percentage points.

Embedding resilience

Traditionally, to stave off disaster, institutions have put in place business-continuity plans to respond to a list of potential threats—hurricanes, server outages, cyberincursion, and so on. They have tended to include a dose of conservativism in a single-scenario planning approach. This approach is outdated.

The capability to respond rapidly and effectively after something happens can make a determinative difference in company success.

Organizations should strive as much as possible to embed resilience in the way they work, in a way that makes them better in normal times, not just in the face of unpredictable threat or change. We delineate three approaches institutions can take to increase resilience:

— *Add on.* Boxes of supplies, emergency generators, backup servers, and redundant pathways all fall in this category. This is the domain of the traditional business-continuity plan and is certainly necessary in some cases. This approach to buffering against threat is isolated and easy to understand and does not get in the way of core operations or business models. On the other hand, in practice, this approach is almost never as reliable as one wants—for example, emergency supplies expire, and generators might not work. Add-ons also tend to increase complexity and can lead to unpredictable knock-on effects. So relying entirely on add-ons is ill advised.

— *Trade off.* Capital buffers, stocks of goods, and overstaffed call centers all fall in this category. These are considered explicit trade-offs between resilience and other parts of the system, often returns or productivity. Leveraging trade-offs requires transparency, true understanding of the desired risk–return balance, and practical ability to retune the system fast. Financial resiliency is perhaps most easily suited to this approach. Systems with physical constraints (such as production facilities) and networks (such as shipping networks) present greater challenge for making quick shifts.

— *'Bake in.'* This is the happy convergence between what is best for resilience and what is best for other business aims. Organizational resilience is where the baked-in approach is most in its element and springs from diversity of skills and experience, fostering of innovation and creative problem solving, and the basic psychological safety that enables peak performance. These characteristics are helpful in good times and indispensable when quick, collaborative adaptation is needed for an institution to thrive.

Add-on resilience is necessary, but it is not the full answer. Backups can fail, they add complexity, and they typically do not help companies emerge from change stronger. Some trade-offs are also required. But companies should look to maximize the amount of baked-in resiliency they can create. This helps better target add-on redundancy, reduce the degree of needed trade-offs, and at the same time improve institutional ability to emerge stronger from change or threat.

The path forward

To get started in building resilience for the years ahead, companies can take three steps:

— *Describe how resilient you are today.* How resilient are you currently—overall and across each of the six dimensions of resilience? Do you have well-developed capabilities to anticipate and respond to disruption or crisis? What are you doing to promote resilience? In particular, to what degree and where do you rely on add-ons or trade-offs, and in what ways do you bake resilience into the way you operate in normal times? Systematic diagnostic tools enable quick but comprehensive understanding of the current state.

— *Determine the degree and nature of resilience you need for the future.* What types of threats or potential change matter most to your institution? Where do you have gaps across each of the resilience dimensions? This analysis should consider each company-led change (for example, a digital transformation), industry-specific dynamics (for instance, rapidly changing levels of regulatory scrutiny), and global dynamics (for example, climate change) that may pose the greatest threat to the institution.

— *Design your approach to building and maintaining the resilience you need.* Where do you most need to shift or supplement your current approach? Ongoing resilience requires embedding related considerations into day-to-day decision making as well as into strategy setting. Institutions should link this business-focused approach toward resilience to any existing enterprise-risk-management processes and should consider investment in anticipation and response capabilities. An ideal design will maximize practices that make you stronger in normal times and better ready to withstand and adapt to threats, but it will also accommodate add-ons and trade-offs where needed.

Companies that understand the resilience they need for the future can implement sensible change. In case of vulnerabilities, this may mean transforming in ways big or small to enhance resilience directly. But, as importantly, organizations should look to build resilience into any transformation they undertake, regardless of the primary goals—from digital to growth to cost. This yields more robust change and helps you bake in resilience from the outset.

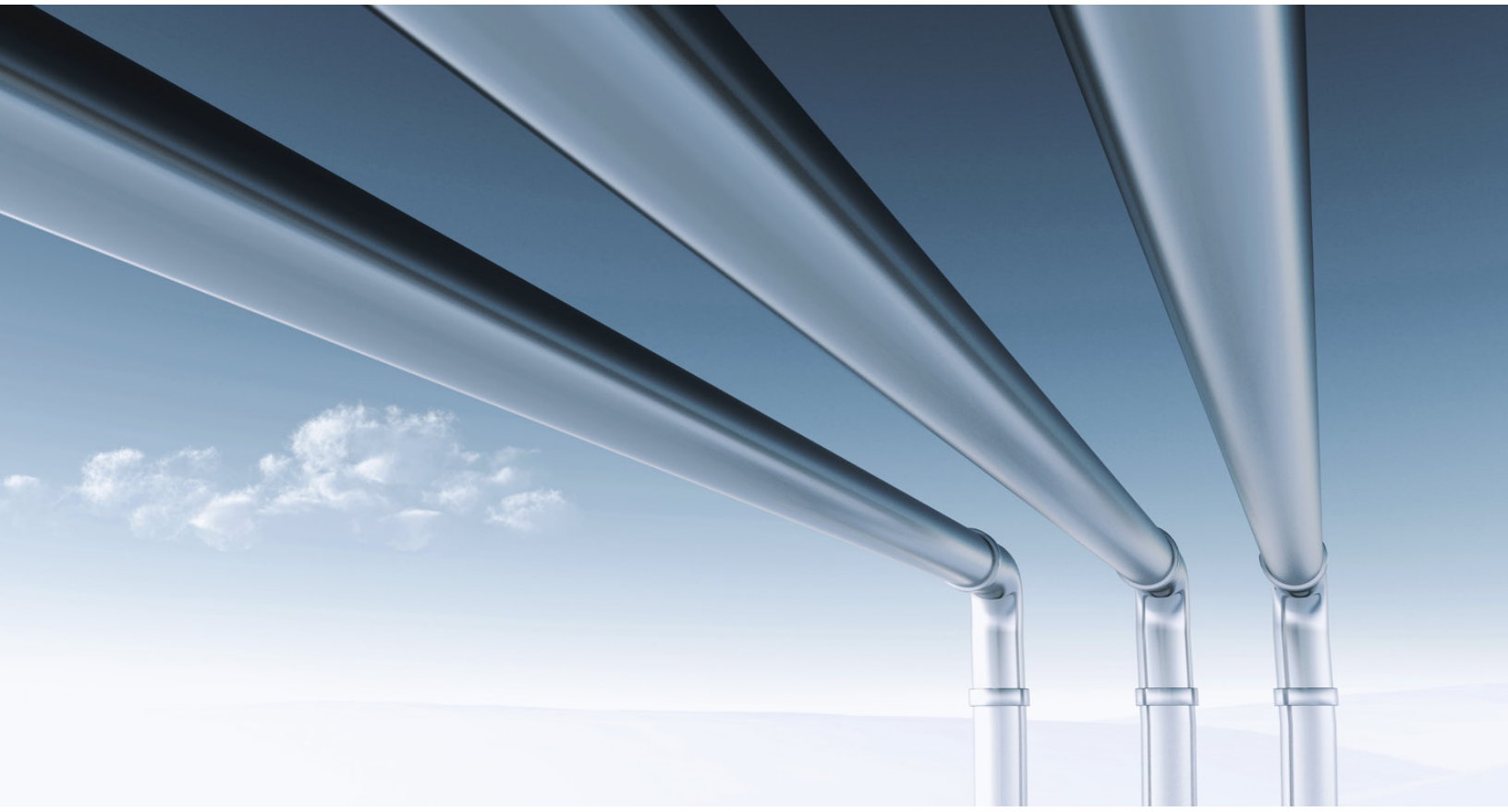
Fritz Nauck is a senior partner in McKinsey's Charlotte office, **Luca Pancaldi** is a partner in the Milan office, **Thomas Poppensieker** is a senior partner in the Munich office, and **Olivia White** is a senior partner in the San Francisco office.

The authors wish to thank Gabriela Hernandez, Graciana Petersen, Michael Thun, and Joseph Truesdale for their contributions to this article.

Building cyber resilience in national critical infrastructure

Recent cyberattacks focus attention on the vulnerabilities of operations technology to web-based threats.

by Rich Isenberg, Ida Kristensen, Mihir Mysore, and David Weinstein



The rising danger posed by cyberattacks on critical national infrastructure was evident again in May 2021, when a small group of hackers launched a ransomware attack on Colonial Pipeline, the United States' largest pipeline network for delivery of refined petroleum products. Colonial Pipeline shut down its main lines for five days, disrupting nearly half the fuel supply for the eastern part of the country. Worried drivers drained supplies in gas stations in the Southeast, airlines rerouted flights to airports with available fuel, traders were rocked by unexpected price volatility, and logistics companies scrambled to locate new sources of fuel.[1]

The attackers seem to have initiated the havoc through "spear phishing"—the sending of fraudulent emails from apparently familiar and trusted sources. Expected user response opened the way for the attackers to launch executable ransomware. This, in turn, enabled lateral movement deeper into the system and the compromising of credentials as the attack progressed. Colonial Pipeline shut down affected systems, which protected it from broader damage. The company also paid a ransom to the attackers to enable a reopening of operations.[2]

One unusual aspect of the attack is that the attackers attempted to apologize for it. On the group's site on the dark web, it issued a statement that its sole motive was financial and that in the future it would choose its targets more carefully. Future investigations may tell us more, but whatever the details, the attack is unsettling. A small group of hackers temporarily, and inadvertently, cut off energy flows to an important economic center, triggering real-world impact.

The Colonial Pipeline hack reveals that societies and economies are vulnerable to serious disruption, and physical harm, from accidental overreach by criminals. Ransomware exists to make money, usually through extortion from the private sector (or, sometimes, government agencies). When, as now, criminals launch unusually ambitious attacks on targets whose managers do not know exactly how their own systems work, things can go wrong in dangerous ways.

The threat to critical infrastructure posed by ransomware attacks has only recently risen to an existential level. Past attacks of this type did not implicate the security of operations technology (OT); rather, OT security developed in response to threats by nation-state actors. The Colonial Pipeline attack, however, demonstrates that the picture has changed. Assurances about the separation of IT and OT systems are no longer tenable. If a relatively unsophisticated ransomware attack can take out infrastructure by disrupting the enterprise network, then more organized attackers will be emboldened.

The threats we face

Not long ago, cyberthreats on critical infrastructure were believed to be acts that could be carried out only by nation-states. Specialists assumed that only states possessed the diverse skills and resources required to develop such threats. The targeted assets usually relied on analog OT and were relatively isolated from the internet. Gaining and maintaining access to such assets requires specialized tools, similar OT, reconnaissance capabilities, and even physical access to the site itself.

In recent years, however, business demands for remote visibility into industrial operations have led to the convergence of IT and OT systems. The digital transformations that enabled sought-after business advantages, including remote access and predictive maintenance, created new vulnerabilities to cyberattacks. Now, less sophisticated attackers could prey on infrastructure assets.

In a recent attack on a water-treatment facility in Florida, for example, sodium hydroxide added to the water supply was raised to poisonous levels (an operator noticed the anomaly and took countervailing action in time). The attacker exploited

[1] Niraj Chokshi, Clifford Krauss, and David E. Sanger, "Gas pipeline hack leads to panic buying in the Southeast," *New York Times*, May 11, 2021, nyt.com.

[2] Collin Eaton and Dustin Volz, "Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom," *Wall Street Journal*, May 19, 2021, wsj.com; Jason Fuller, Mary Louise Kelly, and Justine Kenin, "The Colonial Pipeline CEO explains the decision to pay hackers a $4.4 million ransom," *All Things Considered*, NPR, June 3, 2021, npr.org.

a dormant, password-controlled, remote-access software platform, compromising user credentials, gaining entry into the internet-facing system, and then moving laterally across the operational network. While the source of this attack has not been discovered, experts agree that the level of sophistication needed to carry it out is not particularly high.[3]

The attack on Colonial Pipeline was narrowly aimed to interrupt operations until the ransom was paid. For the target company, however, the attack led to uncertainty about the security of its OT systems, given the absence of proper network segmentation and security controls. In process-control environments, this kind of collateral damage disrupts availability and can also compromise the safety of personnel and citizens.

Web-based tactics, techniques, and procedures used against IT systems now put OT systems at risk. Barriers to entry are being breached with increasing frequency, making crystal clear that a new organization-wide approach to cyber resilience is needed—one that integrates IT and OT security.

How should organizations prepare?

Recent high-profile attacks and breaches have elevated awareness levels, and companies in the United States and in many other countries can expect regulations on resilience and cybersecurity to tighten over time. In particular, the Colonial Pipeline attack has expanded the focus on ransomware beyond experts to the mainstream. In the United States, pressure is mounting against a response in which ransom is quietly paid. In a direct response to the Colonial Pipeline attack, for example, the US Transportation Security Administration, which oversees the cybersecurity of pipelines, made it a requirement that companies report cyberattacks to the federal government within 12 hours of becoming aware of them.[4]

Companies will have to improve their knowledge of their own systems. Knowledge of operations, vulnerabilities, and remedies will be the starting point for building resilience. It will also enable companies to communicate effectively—to governments, regulators, customers, and the media—to build trust in the event of an incident.

The new threat to critical infrastructure is now out in the open, and it shows that a step change in both cyber defenses and our capabilities to absorb and navigate operational attacks is urgently needed. The following principles can guide critical-infrastructure companies in their operational and technical actions to build organization-wide cyber resilience.

Visibility, zero-trust architecture, and resilience

Organizations need to establish visibility into their business-technology assets and their OT systems. Here the watchword might be, "You can't protect what you can't see"—words that are highly relevant to critical-infrastructure networks ranging from manufacturing plants to natural-gas pipelines.

The journey begins with gaining and maintaining real-time visibility into the assets on these industrial networks—but that is not where it ends. Effective visibility demands that organizations take a posture that affords them access to more details. Owners and operators of these critical systems can establish high-fidelity baselines for the devices on the network so they are able to detect subtle anomalies in behavior. Such slight changes can indicate threats and lead to unsafe conditions.

The recent ransomware attack against Colonial Pipeline was likely not targeted against the pipeline itself. Rather, the company's IT systems were attacked. The lack of visibility into the interconnection between the IT and OT systems contributed to the decision to stop operations. The operator could not be confident that the malware had been isolated. The necessity of such a decision might have been confirmed or disproved had operations visibility been established.

Second, owners and operators must move to a zero-trust mindset and architecture. Most of the OT systems controlling America's critical infrastructure

[3] Andy Greenberg, "A hacker tried to poison a Florida city's water supply, officials say," *Wired*, February 8, 2021, wired.com.
[4] Brian Naylor, "In wake of Colonial attack, pipelines now must report cybersecurity breaches," NPR, May 27, 2021, npr.org.

were designed at a time when industrial networks were far less connected than they are today. In the digital age, however, IT and OT systems are converging at a rapid pace. To address the changing picture, organizations can move from a "trust but verify" mindset to a "verify first" approach. Sophisticated actors are increasingly capable of exploiting trust-based approaches. They manipulate the native functionality of control systems while maintaining the appearance of a normal state. Proactive threat hunting and defense-in-depth controls can help ensure not only swift detection of threats but also containment to prevent lateral movement, and therefore mitigate the impact of a compromising attack.

Finally, the Colonial Pipeline attack can be viewed as a case study in the importance of building resilience. Events like this one are extremely difficult, if not impossible, to predict, but a lot can be done to prepare for them. Organizations need to improve their systems' ability to respond, establish control, and spring back quickly. Scenario planning and threat mapping can help organizations define primary- and second-order effects. These capabilities can identify in advance the actions to take in response to a large disruptive event. Thinking in advance about targeted ways to build in redundancy at critical points or capabilities to expand capacity at critical moments can make all the difference. Time is of the essence in a crisis. Organizations have to know what to do, develop the capabilities to do it, and then rehearse their crisis-response actions—all in advance of the incident.

Actions for critical-infrastructure organizations

To best prepare for ransomware and similar disruptive cyberattacks, critical-infrastructure companies can take preemptive action by developing a comprehensive plan with steps to be taken within one, three, and 30 days. In the US government's response to the attack on Colonial Pipeline and a subsequent high-profile cyberattack on JBS Foods, the world's largest meat-processing company, it took specific note of the shift in ransomware targeting: from data theft to the disruption of operations. In no uncertain terms, the government told companies that they must ensure the separation of business functions and production operations so that attacks on corporate activities do not disrupt production and supply.

These preparations require advanced levels of cybersecurity capabilities. Depending on the status of their security environment, organizations will have to accelerate their journeys from maturity-based cybersecurity to an advanced, proactive cybersecurity posture. Foundational capabilities are only the starting point. The journey then moves to a risk-based approach, focusing on the risks that matter to reduce enterprise risk, and then to holistic resilience, embedding security by design into next-generation processes, services, and technologies and incorporating customers, partners, third parties, and regulators into enterprise resilience management.

Preemptive activities include the following:

— *Mapping IT–OT interdependencies.* Organizations need to obtain a true understanding of the inter-dependencies of the network environment, including core systems and applications, and to discover the intentional and unintentional connections and overlap of the IT and OT environments. This mapping will enable organizations to grasp quickly the full implications of a ransomware attack against any one part of the organization.

— *Conducting simulations.* Organizations can continue to rehearse and improve cyber crisis-response scenarios, including for ransomware attacks. Simulations are usually most effective when they include third parties such as law enforcement, public-sector industry groups, and critical customers and suppliers. The simulations should include further core decisions, especially ones such as when to isolate or shut down parts of the network and whether to engage with the attackers.

— *Making the changes needed to achieve cyber resilience.* Mapping and simulations can help organizations improve their operating model and governance structure. Both activities will aid in identifying and implementing the necessary refinements to attain cyber maturity across the

integrated IT and OT architecture. In addition to cyber maturity, the organization can gain greater clarity on the roles, responsibilities, and decision making that will form the core of its response in the event of an actual ransomware event or other cyberattack.

Evidence suggests that the ransomware attack on Colonial Pipeline was not a particularly sophisticated cyberattack—and yet it managed to paralyze a significant part of the fuel supply of the world's largest economy. Good could come of this disturbing event if it acts as a call to action for nations and organizations. Critical infrastructure is vital to a nation's economy and security. The investments needed to truly protect it can no longer be delayed.

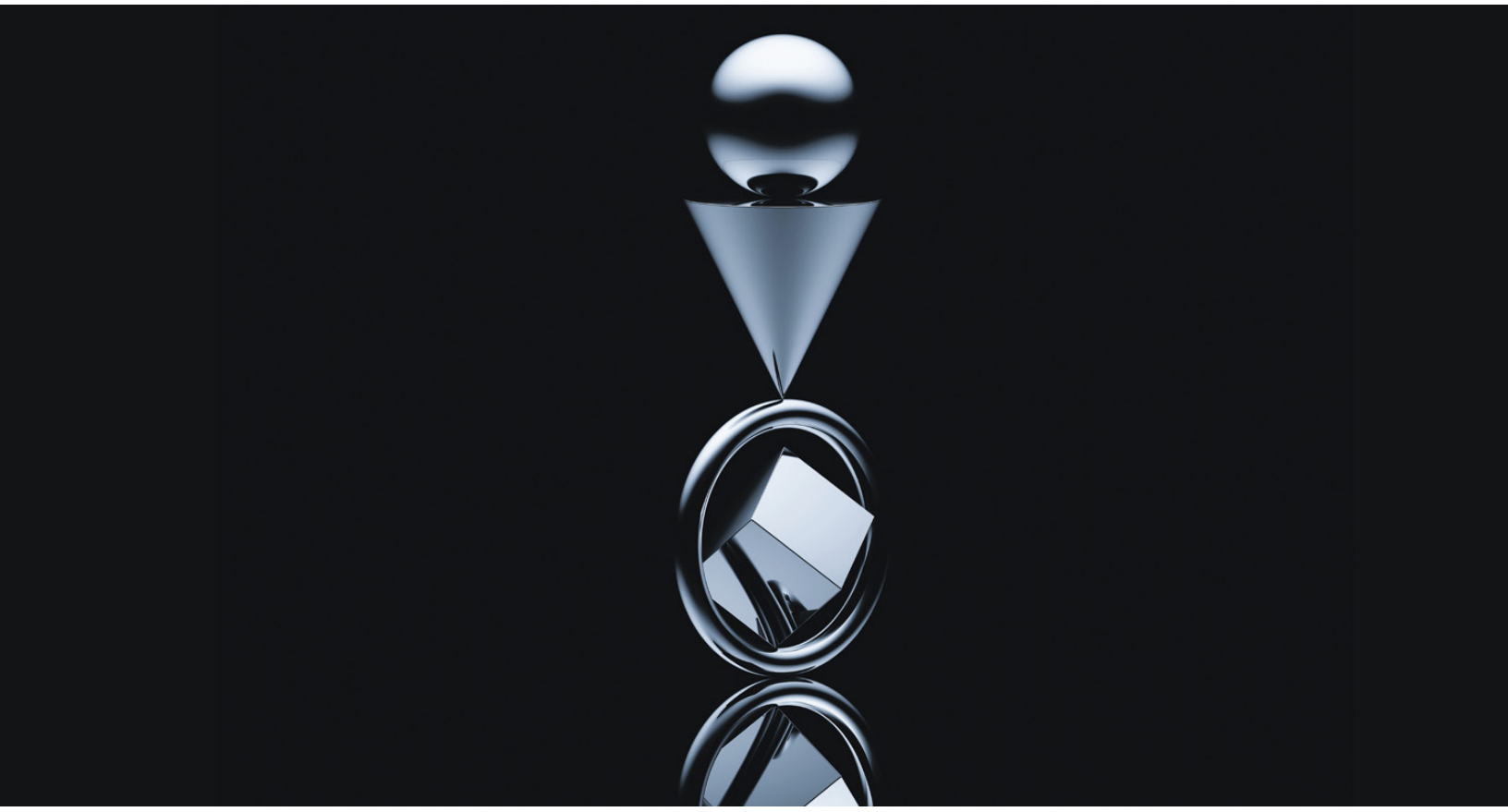
Rich Isenberg is a partner in McKinsey's Atlanta office, **Ida Kristensen** is a senior partner in the New York office, **Mihir Mysore** is a partner in the Houston office, and **David Weinstein** is an alumnus of the New Jersey office.

The authors wish to thank Venky Anant, Tucker Bailey, Dumitru Dediu, Aman Dhingra, Ciaran Martin, and Daniel Wallance for their contributions to this article.

The coming opportunity in consumer lending

The resumption of the credit cycle will offer innovative entrants rare access to underserved customer segments.

by Frank Gerhard, Abhimanyu Harlalka, Andreas Kremer, and Ramlal Suvanam



The global COVID-19 pandemic touched off economic effects that essentially ended the previous credit cycle in most markets. As these markets slowly resume normal activity, a new credit cycle will begin, offering innovative lenders a rare opportunity to expand into credit markets and win market share. The resumption of the cycle will also offer a window for new entrants such as utilities, insurance companies, and other nontraditional lenders to join the market.

Although banks provide financing solutions to a significant share of the global population, large segments of consumers are underserved or not served at all. New-to-market lenders can identify the gaps in lending coverage and try to bridge them. Many potential customers would like innovative, tailored solutions that are not always cost efficient for traditional banks. New entrants can design new offerings quickly and are unencumbered by legacy processes or infrastructure. They can move from concept to fully developed offering in two or three months, compared with one to two years for incumbents.

Unlike incumbents, these new-to-market lenders may not yet have consumer-lending operations and may not be serving consumers with credit history. They likely lack the appropriate lending infrastructure, credit-risk models, and reference data. While they develop these capabilities, they will need to take a structured approach to manage the risk of this business.

New-to-market lenders could include traditional banks expanding market share as well as nonbank financial institutions. These lenders will need to actively manage credit-risk decisions and also the enabling technology. By doing the advance work required to establish a credit-decision platform, lenders can move quickly while still taking the right level of credit risk. To that end, new-to-market lenders could follow a four-part framework (Exhibit 1).

1. Utilize data from a wide range of sources

To model credit risk, new-to-market lenders will need to aggregate data from a broad range of sources. They can make up for any lack of credit expertise by capturing diverse data, including data that they own exclusively. Some traditional categories of credit behavior and demographic data are widely available, particularly for established financial institutions. These include loan information from lenders, deposit data with banks, other current-account information, and point-of-sale transaction data. Nonfinancial companies have other internal sources of customer data, such as product usage, interactions with customer-relationship-management systems, call records, email records, customer feedback, and website navigational data.

Respecting all applicable privacy regulations and guidelines, lenders can seek to employ data from further sources. These include external data from sources such as retailers, telecommunications companies, utility providers, other banks, and government agencies. For certain types of lenders, acquiring needed data through partnerships may be an avenue worth exploring. This strategy—a joint venture with companies that have complementary data about consumer segments—may be particularly suited to lenders with a regional presence.

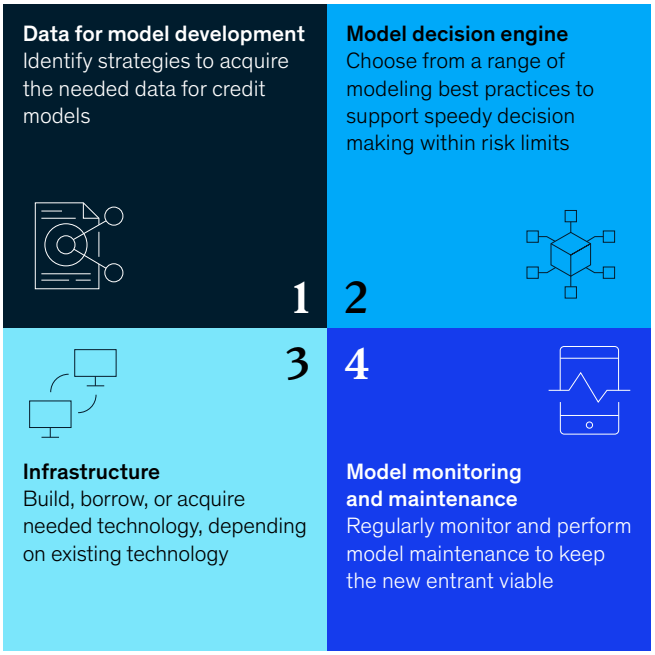
An approach taken by one telecommunications company is instructive. The company launched an unsecured cash-loan product to serve customers lacking access to formal credit. The challenge was that the company had little credit information available to develop the offering. In response, the company turned to its customer-usage data—specifically, data on mobile bill payments. The data enabled the company to devise a proxy target variable that it could use to train its credit model. When back-tested for model development, the target variable performed in the same way as typical credit-related information would perform for banks. From that point, the company was able to extend credit to prepaid customers via a pilot model, which it then refined based on real-world information.

2. Build the decision engine

The second major step is to build the decision engine. In this area, new entrants will have a large advantage over existing lenders with legacy software that they do not want to alter. The new decision engine can largely be built using advanced

Exhibit 1

Four enablers of credit solutions are essential to the new-entrant strategy.



analytics, machine learning, and other tools that capitalize on speed and agility.

By using machine learning, the new-entrant lenders will be able to automate as much as 95 percent of underwriting processes while also making more accurate credit decisions. Similarly, real-time machine-learning solutions can improve pricing and limit setting and help organizations monitor existing customers and credit lines through smarter early-warning systems. Lenders can also use straight-through processing to generate faster transactions and a better customer experience.

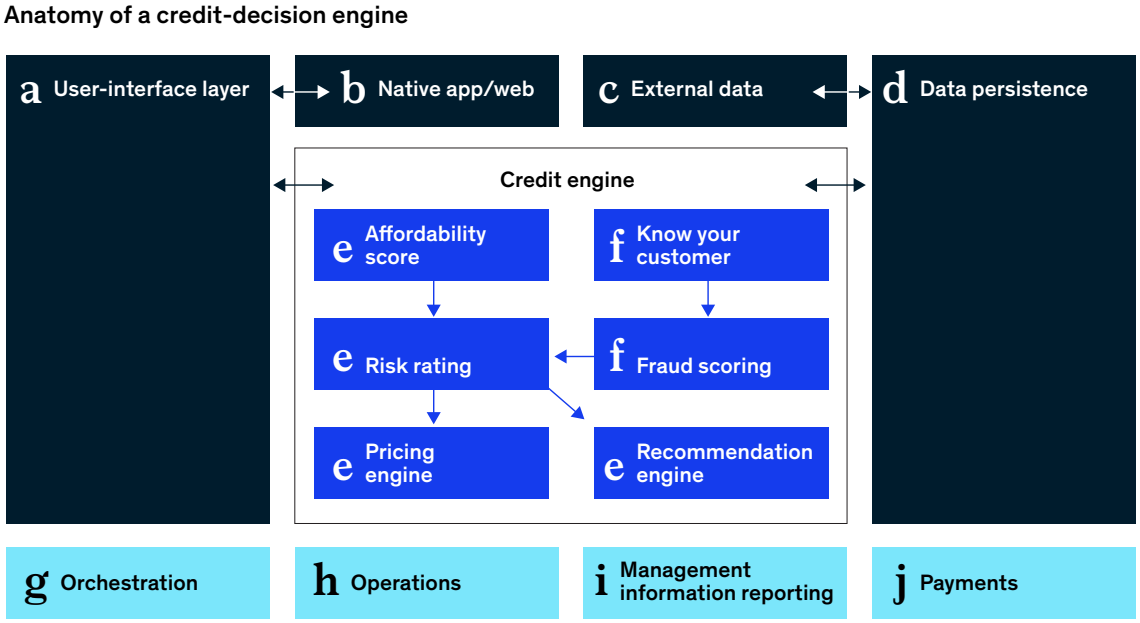
The design of the decision engine can be modular for maximum flexibility. That will allow lenders to retain control of strategic processes while potentially outsourcing other parts. The modular format can also facilitate risk assessment. This approach involves a series of steps, completely integrated from the front end to the back end, and is designed for objective and quick decision making (Exhibit 2).

This approach to risk assessment contrasts markedly with the risk engine in place at many large organizations. The traditional setup is often a single, massive system incorporating every aspect of the lending process, from assessing creditworthiness to printing documents. That approach is increasingly outdated, as it constrains incumbent lenders from adapting quickly.

Based on our experience, applying agile development and implementation can reduce the launch time for a credit engine to less than six months—compared with nearly a year for traditional approaches. One European bank, for example, wanted to launch a digital lending unit. The bank was hindered by legacy systems and entrenched processes, which created long development times for new offerings. To manage this challenge, the bank designed a modular credit-decision engine, which blended parts of the existing system and enabled the team to develop new modules where they were needed. The result was a faster time to market for the newly launched digital business.

Exhibit 2

Lenders can take a modular approach to the credit-decision engine, with strategic parts retained and others potentially outsourced.



3. Create scalable infrastructure

In developing technology infrastructure, new-to-market lenders have a range of options to consider. They can start by identifying their ambition, their perceived advantage in the market, and the degree to which their current technology and data availability will support the initiative—or hinder progress. From that point, organizations can plot the right path forward.

Companies that aim to compete primarily through strong customer relationships might need only basic risk-assessment processes. These companies can buy turnkey solutions from established solution providers. Different standard market solutions are available for acquisition or as outsourced services. Most have a comprehensive offering that includes credit origination, line management, automated decision making for credit assessment, customer acquisition, renewals, and exposure monitoring. With such end-to-end capabilities, lenders can easily see the performance of the entire portfolio or a single customer; they can also access credit-bureau solutions to enrich their data. The turnkey approach offers lenders the advantage of speed but entails limits in customization. In addition,

configuring a turnkey solution with a company's existing IT architecture can be cumbersome.

At the other end of the spectrum are lenders whose competitive distinctiveness will rely on an integrated, tailored solution. That can mean designing and building infrastructure from the ground up. Such complex tailored solutions demand significant investment in time and money. This approach may also require hiring talent with specialized skills and capabilities.

Between off-the-shelf and fully tailored approaches, lenders can find a middle ground by buying individual solutions and applications that can be fitted together in a modular way. This will serve their competitive edge in the market: lenders will be able to customize infrastructure to better address target customer segments with their own credit-risk models and solutions. Lenders may also choose a variant of hybrid solution, entailing a custom-built front-end infrastructure—such as the workflow manager—and a standard market solution for back-end elements, such as collateral-management or exposure systems.

Another telecommunications company, with a subscriber base that comprised about 80 percent of its country's population, collaborated with fintech partners to launch a new lending business. The project required designing technology to support the company's existing data platforms. The company had to train current employees and hire new talent to run the lending business. The long-term goal is to expand the offerings with new products, build the scale of the infrastructure to support the broader portfolio, and collaborate with more financial institutions in the region (by selling credit-scoring services, for example).

Buy-versus-build choices always involve trade-offs between flexibility and cost. The level of spending on development, installation, and maintenance is a determinant of solution flexibility.

4. Monitor and maintain the models over time

Finally, new-to-market lenders need to track key metrics to monitor the performance of the models over time. The development of each model is a one-time effort, but maintaining and monitoring models are ongoing responsibilities. By using established metrics to track changes in the incoming customer population and model performance over time, a lender can spot problems early on.

Metrics include, for example, the population-stability index, which measures a lender's current customer base against the population for which a risk model was originally established. Similarly, the credit-default rate will determine the financial health of the current portfolio. And metrics based on Gini coefficients will determine whether the risk model is making accurate predictions.

Amid the COVID-19 pandemic, lenders have become acutely aware that their solutions must account for significant disruptions, whether in the form of financial crises or environmental shocks.

One incumbent lender decided to move into and serve a new customer segment exclusively through digital channels. The lender developed a standard set of model-monitoring metrics and frameworks. These aggregate information and feed it to a dashboard where all aspects of model performance are compared against industry benchmarks. All anomalies are flagged for review. This approach is helping the bank assess models in real time and anticipate any necessary maintenance or correction.

Amid the COVID-19 pandemic, lenders have become acutely aware that their solutions must account for significant disruptions, whether these come in the form of financial crises or environmental shocks. Certainly during the pandemic, data anomalies and disjunctures led to model failures. Developers must consequently design mechanisms within models to anticipate future large disruptions. The goal is to build models that can be proactive rather than reactive, even under rapidly changing conditions. That way, credit solutions will keep pace with the lending environment.

The coming resumption of the credit cycle offers a rare opportunity for innovative lenders to gain access to new markets and customer segments. New entrants can be incumbent financial institutions expanding into new segments and markets or nontraditional lenders seeking to establish credit operations. By choosing to follow the steps discussed here, either kind of organization can set up operations to manage credit risk. With a distinctive strategy and the requisite expertise, innovative lenders can overcome obstacles and capitalize on an emerging opportunity.

Frank Gerhard is an associate partner in McKinsey's Stuttgart office; **Abhimanyu Harlalka** is an expert in the Gurugram office, where **Ramlal Suvanam** is a senior expert; and **Andreas Kremer** is a partner in the Berlin office.

Enterprise cybersecurity: Aligning third parties and supply chains

In today's riskier, more connected environment, organizations must collaborate closely with external partners to reduce vulnerabilities to cyberattackers.

by Ayman Al Issa, Tucker Bailey, Jim Boehm, and David Weinstein

Enterprises today are embracing digital and analytics transformations as never before. Even those that did not expect to embark upon major IT changes have had to adopt fully remote ways of working due to the COVID-19 pandemic. In fast-moving business environments, companies make many necessary IT changes on the fly, with security waivers and risk-mitigation promissory notes issued almost as readily as authorization-to-operate (ATO) certifications. Cyberattackers and corporate spies are having a field day. They are capitalizing on the disruption, meeting in virtual rooms to engage in advanced persistent mapping of enterprise IT environments and associated vulnerabilities—including the areas of those environments that are reliant on third-party support and capabilities.

As cyberbreaches and attacks mount, top managers of corporations in every sector are looking into the sources of their vulnerabilities, including the third parties and supply chains that make their businesses possible. In the wake of high-profile events such as the recent Sunburst malware attack, however, chief information officers (CIOs) and chief information security officers (CISOs) are being deluged with conflicting messages. The Sunburst attack proved that enterprise environments and third-party capabilities are interpenetrated and indistinguishable. Attackers are opportunistic, adapting to whatever foothold they can gain, no matter the source.

This creates a conundrum for CIOs and CISOs; they must now secure their own IT environments while also accounting for the security of the third-party elements of those environments. Third parties must be made to comply, technically and in contract-driven risk-mitigation elements, with security that supports the enterprise's purposes. To ensure cooperation while providing sufficient protection for all sides, enterprises must, therefore, bring third parties into the inner circle of their security perimeters. Meanwhile, CIOs and CISOs are being told to scrutinize third parties intensively. On the surface, the two mandates are counterposed. But must they be? The short answer is no. The two stances, trust and scrutiny, do not have to be in opposition. In fact, they are most effective when contained in a reciprocal relationship.

The Sunburst attack reveals that certain types of attackers form broad-range alliances to achieve their threat-focused objectives. CIOs and CISOs, together with their third-party colleagues, can and must do likewise. They can work together to set the tough objectives and achieve the security excellence needed to meet the risk-mitigation requirements of the enterprise. Make no mistake, cyberthreats are becoming more perilous the world over. Attackers will have the advantage until enterprises appropriately staff and train their organizations, acquiring needed capabilities and tools. This means working together with their third parties to sustain a united security front.

CISOs and CIOs are aware of more gaps and weaknesses in enterprise cybersecurity than they are comfortable with. In third-party relationships, furthermore, those weak spots are often papered over. But the Sunburst attack has made these spots glaringly obvious. The time has come to openly challenge the status quo in cybersecurity. Companies must link arms with their third parties in the face of the mounting challenges and demand the very best when it comes to security.

Understanding the risks

Recent cyberattacks have made many cybersecurity challenges more apparent. One of the most important revelations is that enterprise security is as dependent on the global cyber ecosystem as it is on the actions of particular institutions. CIOs and CISOs are accustomed to managing their own operations and, ideally, having a strong influence on how the enterprise's employees and contractors behave.

The truth is that no matter how large an enterprise is, it is one player among millions across the global internet. Its security posture is dependent on every one of its employees, contractors, suppliers, resellers, cloud partners, and sometimes even customers—but also on those same elements belonging to any other company out there, both in their own market and in the wider global economy.

An enterprise has its hands full even keeping under control all its direct users. To address vulnerabilities generated across all cyberspace requires a

commonly maintained global security defense. That means that enterprises have to communicate openly with their partners and rivals. CISO-to-CISO conversations may feel awkward, but they are now necessary.

Enterprises need to examine operations realistically to determine their most likely forms of attack. New exposures from acquisitions or sales of business units need to be addressed. Attacks can come in the form of advanced persistent threats from nation-states, ransomware operations, cyber theft and industrial espionage, or malicious actions by individuals (insider or outsider threats).

The most viable enterprise-security strategies have to address the several dimensions of the threat environment, each of which is subject to change, sometimes dramatically, at any point in time:

— the nature of attackers and their most likely tactics

— the nature of the current and imminent enterprise-security environment

— the nature of the business, including acquisitions, operations, market conditions, partners, and competitors

A company acquiring an overseas asset to improve its market share and positioning may be exposing itself to threats it never before considered. The due-diligence team will have to examine the acquired operation and any of its third parties to determine potential new threats and vulnerabilities. If the acquisition is a defense contractor, for example, the parent company could even be targeted by a nation-state attacker. Once the new acquisition's systems are connected to the new parent's corporate network, everything contained within it could be exposed to spying or theft.

Communication and third-party cybersecurity

Two good areas to begin improving defenses are communication and third-party cybersecurity. As with any at-scale improvement, these issues have no simple solution. Many public institutions and private-sector companies have, however, achieved much by tackling these two areas in tandem.

"Cybersecurity hygiene"—the care, stringency, and thoroughness with which cyber defenses are maintained—is of critical importance. To maintain a uniformly high level of cybersecurity hygiene across the organization, including for new acquisitions and third parties, transparency and open communication are needed.

Across collective ecosystems, enterprises can achieve both transparency and toughness on cybersecurity hygiene through common work. Attackers are often very capable and motivated in constructing strategic campaigns. To face these very real threats, enterprises, as defenders, must be as capable and as motivated. The following recommendations are based on the insights and experiences of organizations that were successful at reducing third-party cyberrisk.

For companies using third parties

For companies reliant on third-party services and capabilities, such as software development and technology tools, consider taking the following measures and actions, as appropriate:

— Apply role-based access controls to applications, databases, and infrastructures; remove single-user accounts on highly privileged systems (such as network-access systems). To the extent possible, proceed according to zero-trust-based expectations, if not actual zero-trust controls.

— Enforce appropriate risk-based multifactor authentication (MFA) for all privileged role-based access.

— Build use cases in the security-operations center to identify suspicious third-party use cases. These could be "impossible log-ins"—single-user log-ins made in a short time period from several geographically distant IP addresses—or "impossible tokens" (SAML tokens valid for 24 hours should be flagged).

— Create incident guides for third-party supply-chain attack scenarios and conduct tabletop exercises with key software vendors. Establish

point-of-contact connections (CISO to CISO are particularly effective), secure channels of communication, and ensure that all staff are aware of procedures for handling incidents.

— Mandate security training and certifications, service-level agreements (SLAs), and escalation protocols in third-party contracts. Surprisingly, many third-party contracts for technology services and capabilities do not specify security requirements, SLAs, or escalations. Work with company-procurement functions to ensure that these elements are included as a matter of course in any relevant vendor contract.

— Assess your tier-two (and beyond) suppliers. Many of these organizations are small and medium-size businesses with limited security and compliance resources. As such, striking a fair balance between assessing their cybersecurity hygiene and overburdening them with information requests will be of critical importance.

— Adopt a third-party risk-management framework that performs an algorithmic risk rating of your suppliers. Regularly evaluating suppliers on a relative risk can help inform strategic decisions on procurement, risk management, and resource allocation.

For third-party providers

To serve customers more securely, consider the following actions, as appropriate, for third-party providers:

— Conduct security reviews across all products and transparently report to customers on the current state of security, including vulnerabilities.

— As soon as possible, identify and patch product vulnerabilities that might be exploited; communicate those activities to customers.

— Use threat modeling during product development and share results with customers. Build threat models that account for both inside-out and outside-in attack scenarios. Ensure that as much emphasis is put on scenarios covering denial of legitimate service as those covering potential compromised assets.

— Expand existing code-testing capabilities (such as general, static, and dynamic security testing) to include stress-testing on code tampering, degradation of data integrity, and suitability of corporate integration.

— Conduct red-team exercises using attack scenarios on the software supply chain to stress-test the infrastructure-security posture

Striking a fair balance between assessing your tier-two suppliers' cybersecurity hygiene and overburdening them with information requests will be of critical importance.

for current products. Tweak the exercises to anticipate different attempts to infiltrate the supply chain.

Legal and other enhancements

Legal avenues are another means of reducing enterprise risk from third-party attacks. Organizations can (and should) contractually require that third parties meet enterprise cybersecurity standards. Third parties should also be contractually obligated to impose the same standards on any subcontractor that could affect enterprise data or systems.

Companies can also contractually require regular technical testing of third parties. This would mean penetration testing and red-team exercises, which many vendors do not yet permit. Yet to improve communications and cybersecurity across the enterprise ecosystem, these tests must become part of the routine. Enterprises need penetration tests and red-team exercises for their own homegrown capabilities to ensure that they are in line with security requirements; the same approach must be required of third parties as well.

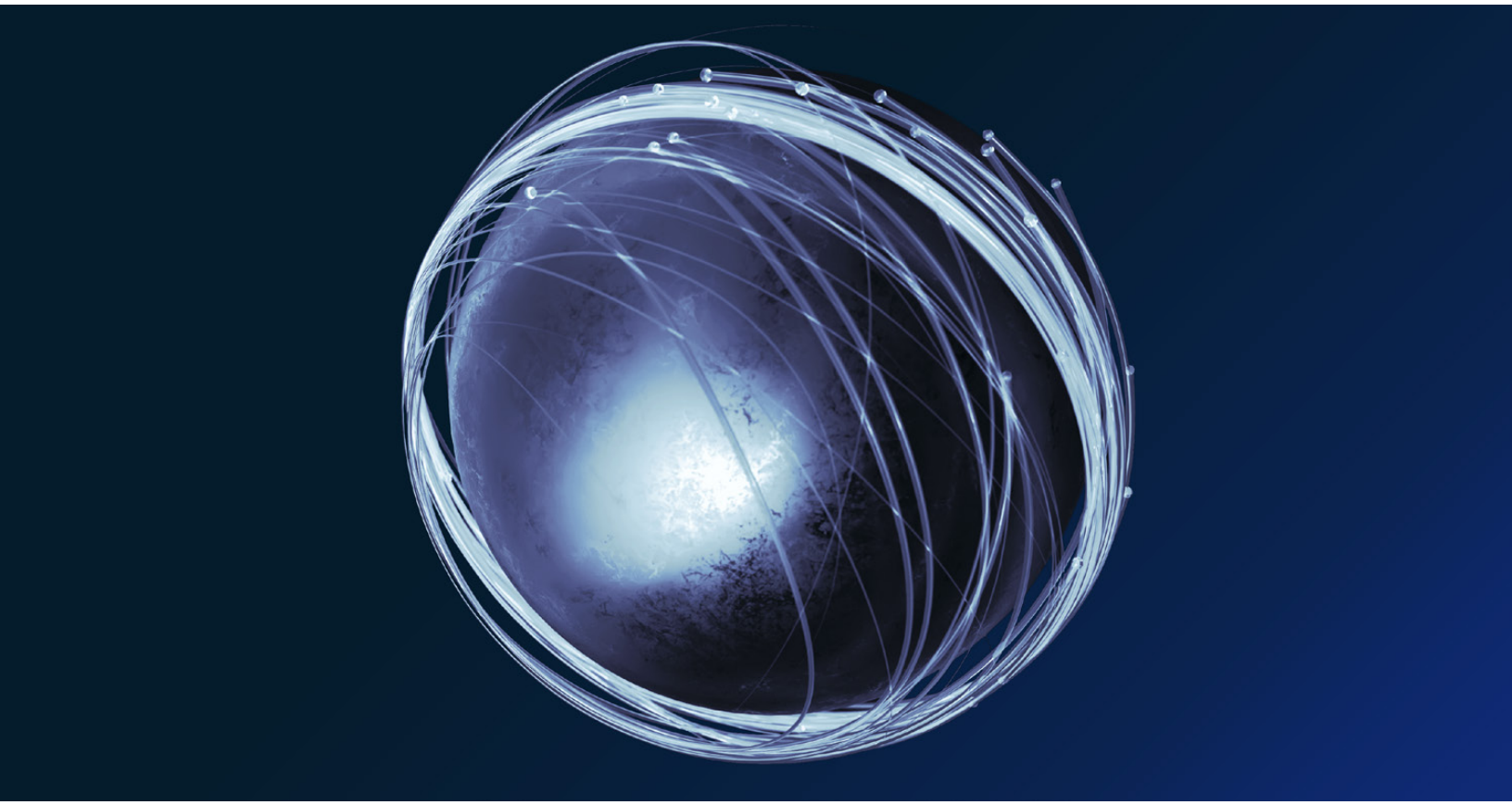
A new age of cybersecurity has been defined by more sophisticated cyberattacks, widespread adoption of digital and analytics transformations, and workplace changes, especially work-from-home arrangements. The conditions challenge existing third-party and supply-chain security-management procedures. A radical new approach is needed, one that focuses on robust communication and the complete alignment of third-party cyber protection with the requirements and standards of the enterprise. The new approach goes beyond meeting compliance requirements; its goal is to markedly reduce enterprise-wide risk. The change is significant but necessary because the security environment, as CIOs and CISOs well know, has become much more dangerous.

Ayman Al Issa is a senior expert in McKinsey's Abu Dhabi office; **Tucker Bailey** is a partner in the Washington, DC, office, where **Jim Boehm** is a partner; and **David Weinstein** is an alumnus of the New Jersey office.

Derisking digital and analytics transformations

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

by Jim Boehm and Joy Smith



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

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

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

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

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

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

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

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

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

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

The advantages of digital and analytics transformations are real, but so are the risks (Exhibit 1). By understanding the insights from our research and taking the approach outlined here, companies can achieve the value of digital and analytics transformations while also safeguarding their organizations and customers. Ultimately, companies can inspire more productive relationships among groups and foster a sustainable competitive advantage for the company by preserving the impact of their transformation activities for the long term.

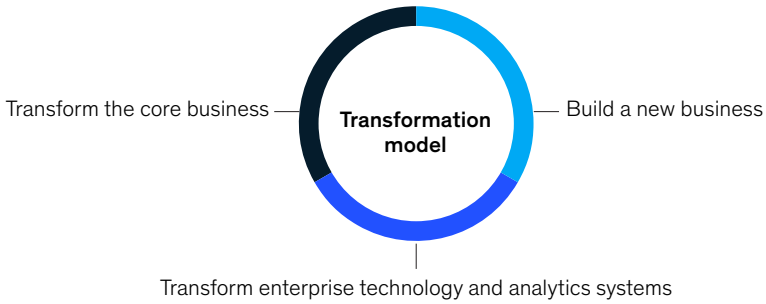
A broad set of new (and expensive) risks

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

Exhibit 1

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

Approach to digital and analytics transformations



Transformation domains

- Multichannel customer experience: redesign and digitize top customer journeys end to end
- Digital marketing and pricing: use revenue management, promotion-dynamic B2B pricing, cross-selling, and upselling
- Sales digitization: emphasize digital sales and remote-selling effectiveness
- New digital propositions: create new revenue streams by building digital propositions, using next-generation AI technologies to achieve cost savings
- Supply chain and procurement: digitally redesign and manage operations to improve safety, delivery, and costs
- Next-generation operations: drive step changes in efficiency through digitization, artificial intelligence, advanced analytics, and agile-lean approaches
- Digital architecture: set up digital architecture combining APIs, microservices, and containers
- Data transformation: unify data governance and architecture to enable next-generation analytics
- Core system modernization: achieve through refactoring or platform replacement
- Cloud and DevOps: migrate applications to hybrid cloud and/or software as a service and implement software development and IT operations
- Digital and analytics talent and capabilities: acquire needed new talent and build capabilities at scale

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

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

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

A telecom company allowed its call-center staff to work from home, but it left specific policies up to team managers. The result was that 30 percent of the staff were permitted to use unsecured personal devices to connect remotely, exposing the company to "bring your own device" attacks. Similarly, a bank found that employees were printing documents on their home printers, thus running corporate data through unsecured home routers, which are notoriously vulnerable to hackers. Another company expressed concerns about employees having "smart home" listening devices that could record discussions during video calls in executives' home offices.

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

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

A snapshot of digital and analytics transformation risk management

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

Transformations are becoming commonplace across industries

Survey participants completed an average of six transformations in the past three years, with a range of objectives. More than 80 percent have implemented at least one end-to-end customer journey transformation, and 70 percent developed new digital propositions and ecosystems.

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

Organizations are also changing their operating models to support the changes. Approximately 80 percent of companies intend to shift up to 30 teams to work in agile ways in the next three years; the remaining 20 percent are shifting more than 30 teams to agile. This means, of course, that 100 percent of the 100 companies we surveyed intend to adopt or scale agile in the coming years. If done well, this is very good news for risk managers, given the inherent risk-mitigating structures and culture of early identification and remediation of defects inherent in well-implemented agile teams.

Risk management is not keeping pace

Companies' risk-management capabilities are lagging behind their transformation efforts. Organizations are transforming far more frequently than they are updating their risk frameworks to include new and exacerbated risks, and risk and legal professionals often operate in separate silos; hence the risk infrastructure is not keeping pace with the innovation. Overall, most respondents assess their risk-management maturity as average, but more than 75 percent have not conducted a formal, holistic risk assessment for half of their digital and analytics transformations. Surprisingly, 14 percent have never formally assessed the risks for these initiatives—a big oversight for established companies.

Companies are unsure of how to manage digital risks

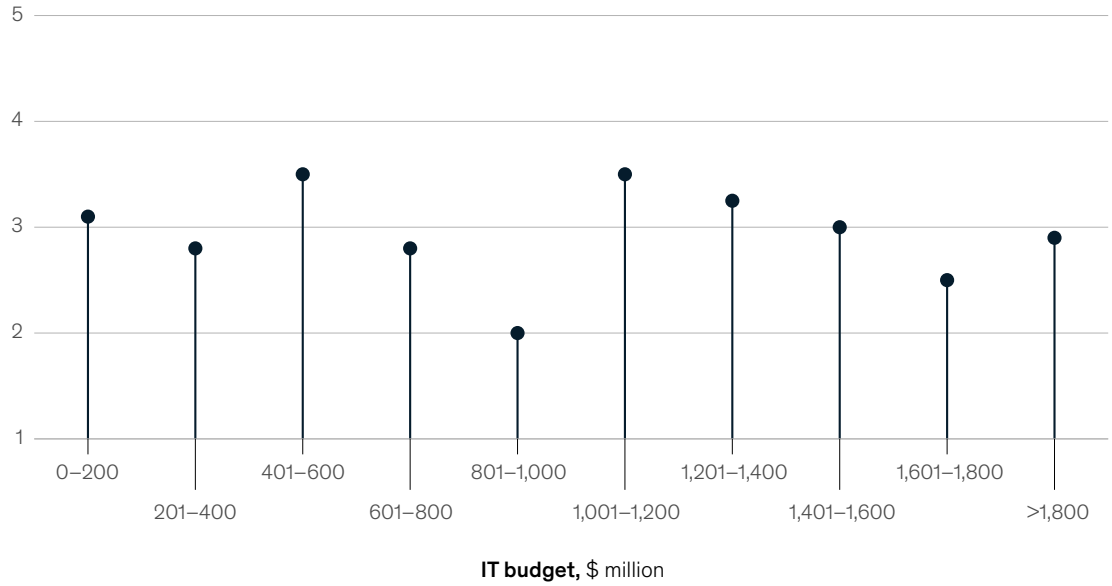
Unlike for financial risk management, in which companies tend to have established roles and processes (such as model risk management), companies in our survey do not have established roles, processes, or even consolidated understanding of digital and analytics risk drivers. The biggest challenge leaders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

Notably, the survey results show virtually no relationship between IT-spending levels and overall

Exhibit 2

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

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



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

risk-management maturity for digital and analytics transformations. Simply put, the challenges are not solved by budget size (Exhibit 2).

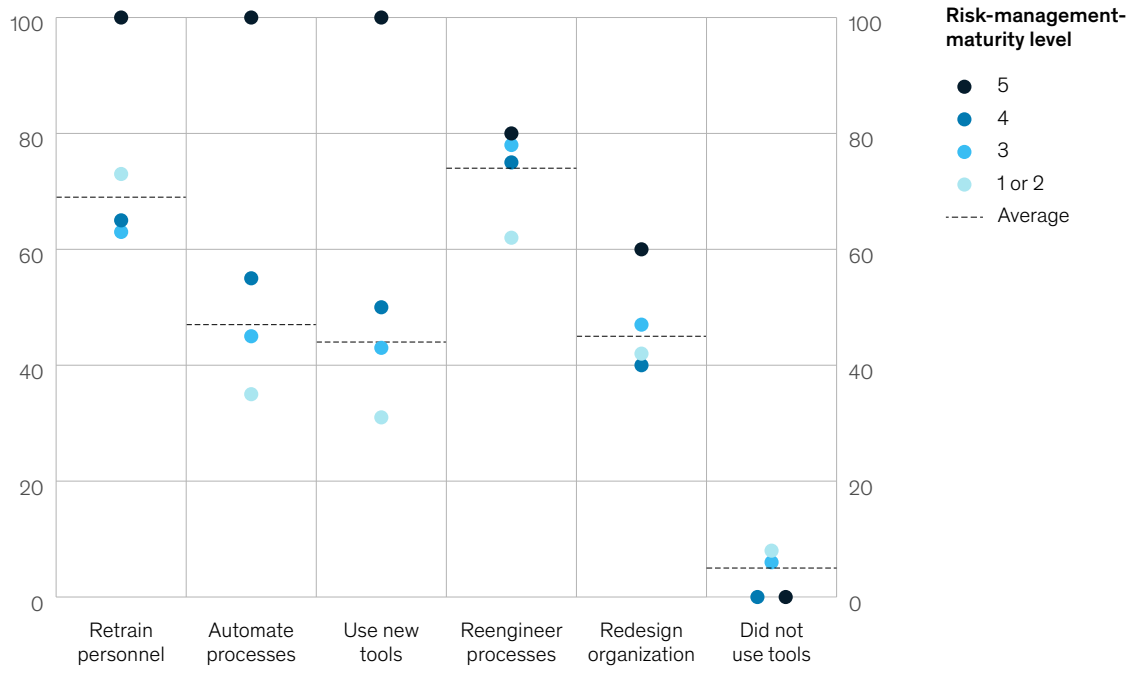
Roles and responsibilities are insufficiently clear
Survey participants little agree on where responsibility should lie for addressing digital- and analytics-transformation risks. For almost all respondents, the chief information or chief data officer leads digital- and analytics-transformation activities;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

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

Exhibit 3

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

Reported use of transformation practices by risk-management-maturity level,[1] % of respondents



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

Here are the most relevant approaches leaders cite:

— *Reengineering processes and retraining employees.* Respectively, 74 and 69 percent of respondents across industries and regions cite these practices, making them the most popular for managing digital and analytics transformation. These practices are especially important for agile ways of working. When implemented well, they can be critical to derisking technology using agile methodologies. The agile approach permits companies to automate, create new organizations, or deploy new tools with less effort and has early identification and remediation of defects inherent in its culture.

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

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

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

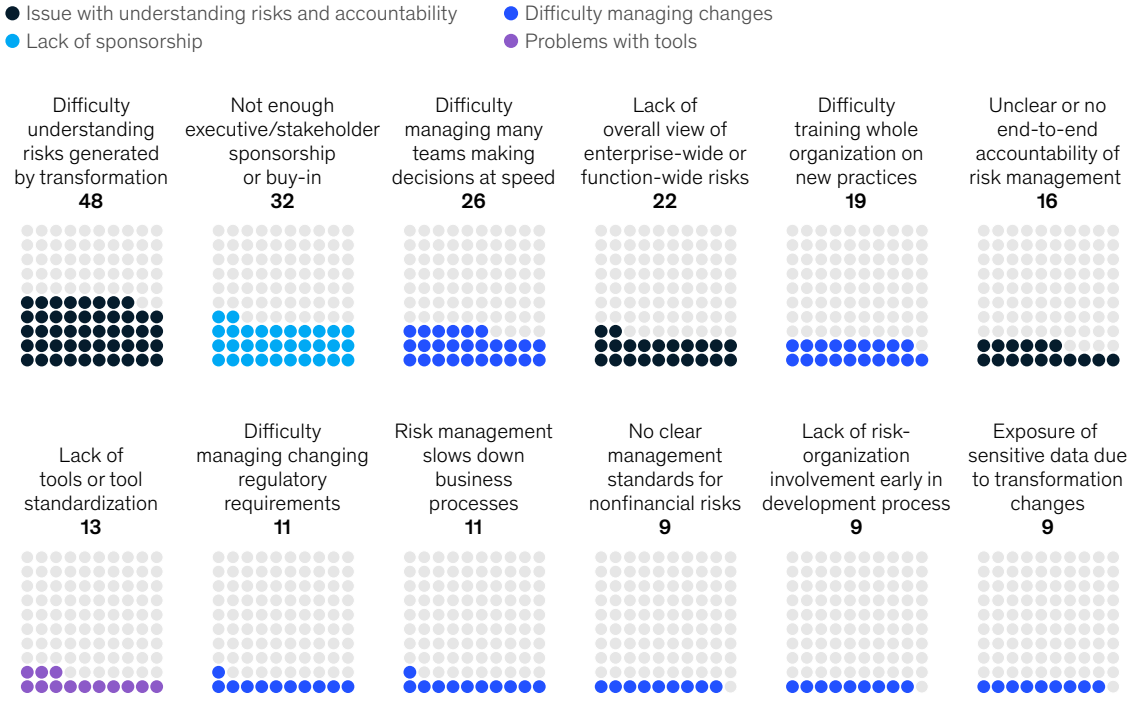
Pain points in managing digital and analytics transformation risks

Survey participants also describe their biggest pain points in identifying and mitigating risks.

Exhibit 4

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

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



[1]Question: In your most recent digital and agile projects, what were the top 5 risk-management pain points?
Source: McKinsey Global Survey on Digital and Analytics Transformations in Risk Management, 2020

Understanding risks

The top concern, which 48 percent of respondents cite, was simply understanding the risks associated with digital and analytics transformations (Exhibit 4). Many transformation leaders are essentially flying blind: risk ownership is not clear, the complex and changing technology and regulatory environments are not well deciphered, and design and test plans do not consider risks early enough in the process. Unlike financial risks, nonfinancial risks are hard to benchmark, and there is no one standard to manage them.

Managing changes at speed

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

Accessing resources

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

Overcoming operational limitations

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

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

A framework for digital and analytics transformations

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

- defining a mature enterprise-risk framework
- developing an effective risk governance with taxonomy, risk appetite, reporting, and key risk indicators
- building a risk organization and operating model (including the three lines of defense, where relevant) and assembling the needed resources and talent
- establishing risk-management processes
- creating a risk culture

These activities are critically important to digital and analytics transformations. They must be transformed alongside digital and analytics teams, however. This is because risk management will have to keep pace with the rapidly changing digital-risk landscape to continue mitigating risks but avoid slowing down the business. Our framework makes it easier for organizations to do this. It consists of four steps that define, operationalize, embed, and reinforce the elements of the transformation.

The framework fosters a dynamic approach, helping adapt the existing ERM infrastructure for an increasing flow of risk-mitigating information and actions. Within the framework, organizations design transformation activities and make appropriate interventions. The framework is updated as the activities change ways of working, risk appetites, risk exposure, and talent needs (Exhibit 5):

- *Define.* In the first step, organizations apply the technology-specific elements of their existing risk-management framework—in place to address traditional categories, such as financial and regulatory risk—to the transformation scenario. Organizations without an ERM framework in place will need to start there, ideally creating one with a transformation-specific framework to address digital and analytics risks. The objective is to articulate risks and hypothesize potential solutions through a relevant risk matrix with a clear taxonomy, defined risk owners, available controls and resources, and a governance structure for the initiative.
- *Operationalize.* In the second step, transformation leaders work with risk subject-matter experts or a risk center of excellence to convert risk-management hypotheses into solutions. Specific actions could include introducing software and data controls, validating algorithmic models, implementing systems and infrastructure patching, teaching frontline technologists relevant cybersecurity practices, and validating product resilience through defect and unit testing. As a part of this step, teams also start generating risk reports based on clearly defined metrics such as key risk indicators and key performance indicators that critically measure not only risk effectiveness but risk-management efficiency as well.
- *Embed.* This step is designed to embed the lessons from risk management—including testing results, risk assessments, incident reports, and performance measurement—into existing control implementation operating models, processes, governance, and, if needed, organizational design. In this step, new derisking initiatives are generated based on these lessons. Frontline colleagues in the transformation team and in units being transformed are fully trained on risk awareness, identification, and mitigation.

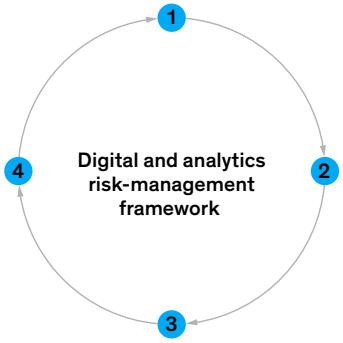
Exhibit 5

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

Current state

- Cumbersome risk and compliance reviews lead to frequent delay of product launches
- Challenges from second line are perceived as convoluted and do not always lead to clear set of actions for front line
- Inadequate tools for risk identification result in a lack of appropriate transparency and guardrails

Transformed state



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

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

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

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

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

Benefits of the framework and transformation roles

The framework enables companies to manage the risks of a digital and analytics transformation systematically, so that it keeps pace with an organization's innovation. It incorporates lessons from the front line to improve the conceptual matrix and adjusts risk-management methods along the transformation journey. It meshes with agile working models to enable better risk management, encourages collaboration, and fosters an enhanced risk culture.

Companies have already seen significant risk-mitigation effectiveness and risk-management efficiency from taking this approach. Although in its early stages, the approach promises to yield further benefits to risk managers and transformation teams (Exhibit 6).

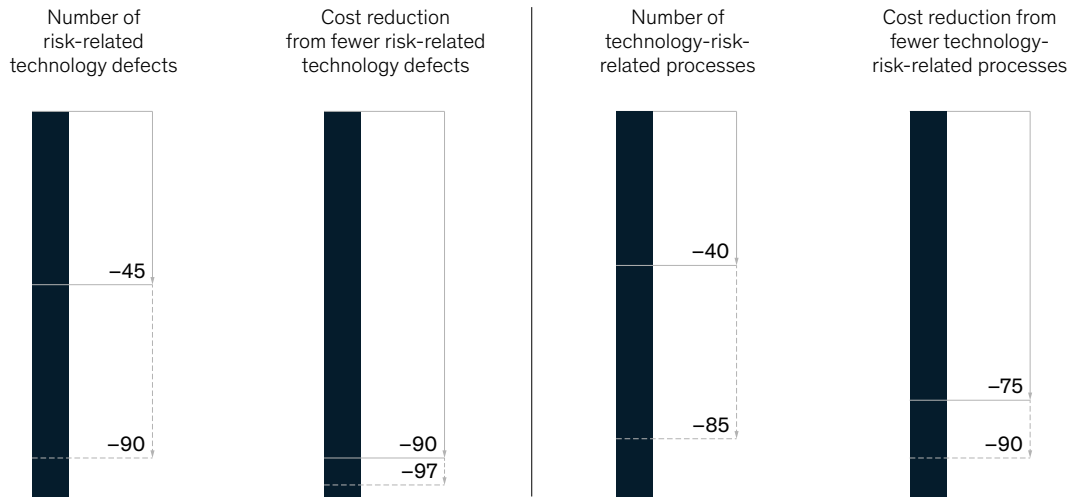
To support the framework and put its approach into practice, companies will need to also define these roles and responsibilities for digital and analytics transformation risks:

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

Exhibit 6

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

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



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

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

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

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

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

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

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

Finally, companies will have to raise awareness of digital and analytics risks in the organization, including with the executive team and board. Likewise, they must adequately incorporate digital

Snapshot of a successful transformation

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

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

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

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

and analytics risk management into their formal risk governance models (see sidebar, "Snapshot of a successful transformation").

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

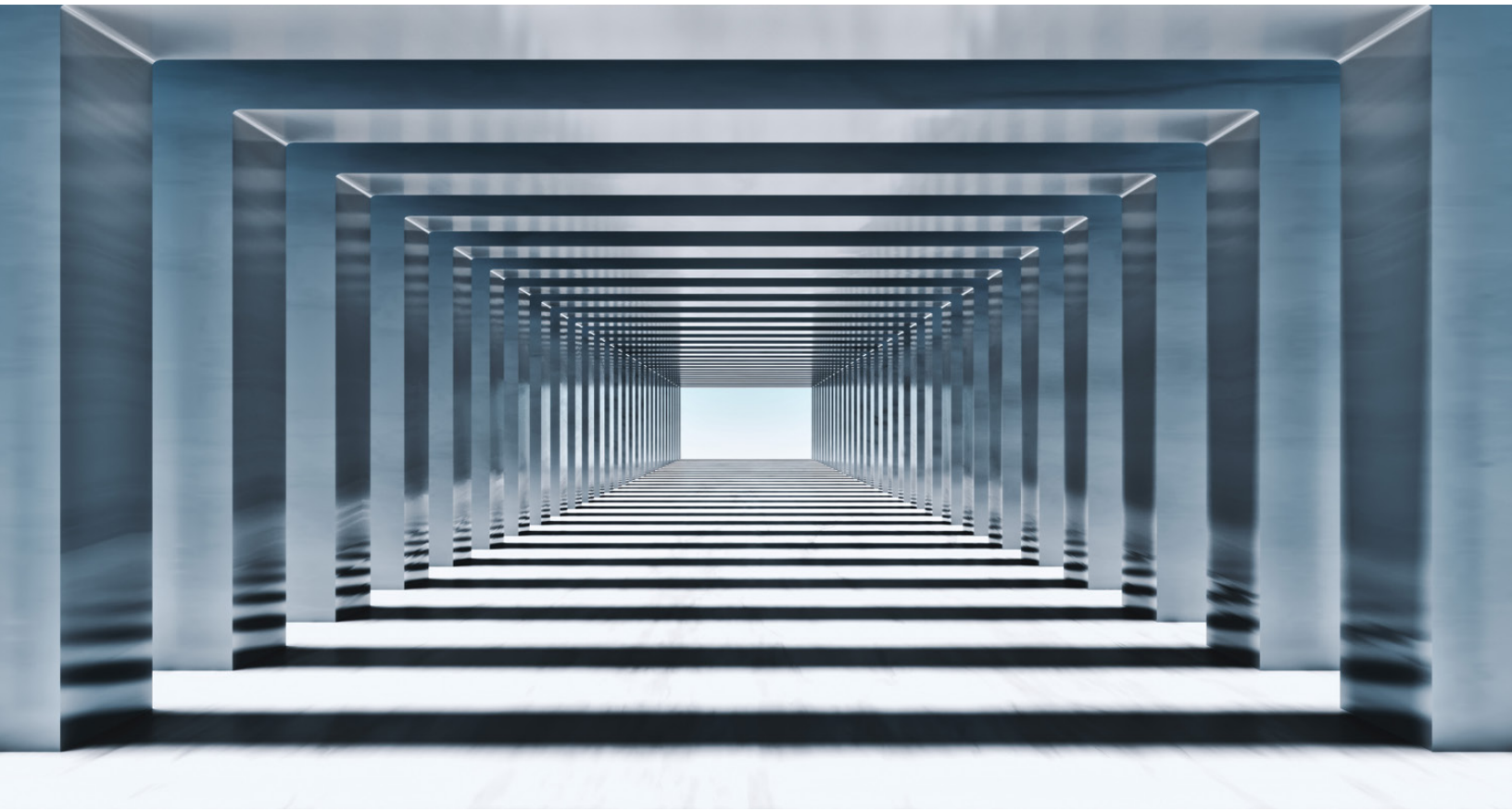
Jim Boehm is a partner in McKinsey's Washington, DC, office, and **Joy Smith** is an expert in the Philadelphia office.

The authors wish to thank Liz Grennan, Arun Gundurao, Grace Hao, Kathleen Li, and Olivia White for their contributions to this article.

Solving the know-your-customer puzzle with straight-through processing

Banks can become more efficient and effective in combating money laundering while improving the experience of their customers and employees.

by Irene Peschel, Kate Robu, Sebastian Schneider, and Alexander Verhagen



The amount of money laundering that occurs each year is equivalent to as much as 5 percent of global GDP, according to the United Nations Office on Drugs and Crime (UNODC).[1] The vast majority of these illicit funds pass through the financial system. This creates a challenge for financial institutions in knowing the sources of client funds over the full period of the client relationship. Banks are therefore relying increasingly on periodic know-your-customer (KYC) reviews (as part of ongoing due diligence) in compliance frameworks. However, the KYC process often remains highly manual, which makes it expensive and prone to errors.

Banks typically employ around 10 percent of the workforce in financial-crime-related activities.[2] KYC reviews are often the costliest activity. They can be undertaken annually; three- and five-year reviews are also common, with event-driven actions prompting additional reviews. In addition to the frequency, the required resources for outreach, identification, verification, and risk processes all add to the cost.

While most banks have automated some aspects of reviews, few have adopted end-to-end straight-through processing (STP), which can make a significant difference in efficiency. To do this, banks can adopt a strategic mindset and acquire or develop needed technical and organizational capabilities. Implementation and scaling of STP can be a complex undertaking, but leading banks have shown that STP can significantly boost review effectiveness, improve customer service, and enable closer alignment with regulatory obligations.

KYC-review challenges

In conducting KYC reviews, the most common pain points relate to data collection, transaction analysis, and determination of sources of wealth:

— *Customer-data collection.* At many institutions, the collection and documentation of key customer data is done through outreach. Banks manually send emails or even rely on letters sent by case handlers. Data are then copied over into KYC-workflow tools. These tasks are often seen as low value, an attitude that leads to institutional inattention—which tends to increase the chance of errors.

— *Transaction analysis.* More or less half of KYC-review time is spent on transaction analysis. The reasons for the outsize expenditure of time can be diverse. The scope of the exercise can be ill defined, taking between six months and three years. Appropriate tools might be inadequate, such as raw Excel data requiring manual analysis. Descriptive statistics, which can offer a quick view of customer-transaction profiles and red-flag transactions, may be unavailable.

— *Sources of wealth.* Determining the customer's source of wealth is another challenge. Case handlers often lack targeted insights—they are unable to categorize data into types of income (salary, investment, rental, and so forth) and do not have access to descriptive statistics for transaction groups. In addition, guidelines on the scope of the investigation and documentation requirements often are not sufficiently detailed.

Banks can address these pain points with a clear, step-by-step workflow, requirements for risk differentiation, standardized ways of working, and automated processes. The degree to which they already do this determines average handling times (Exhibit 1). While many banks have started to automate individual process steps, only a few have implemented end-to-end STP solutions.

STP solutions: Value at stake

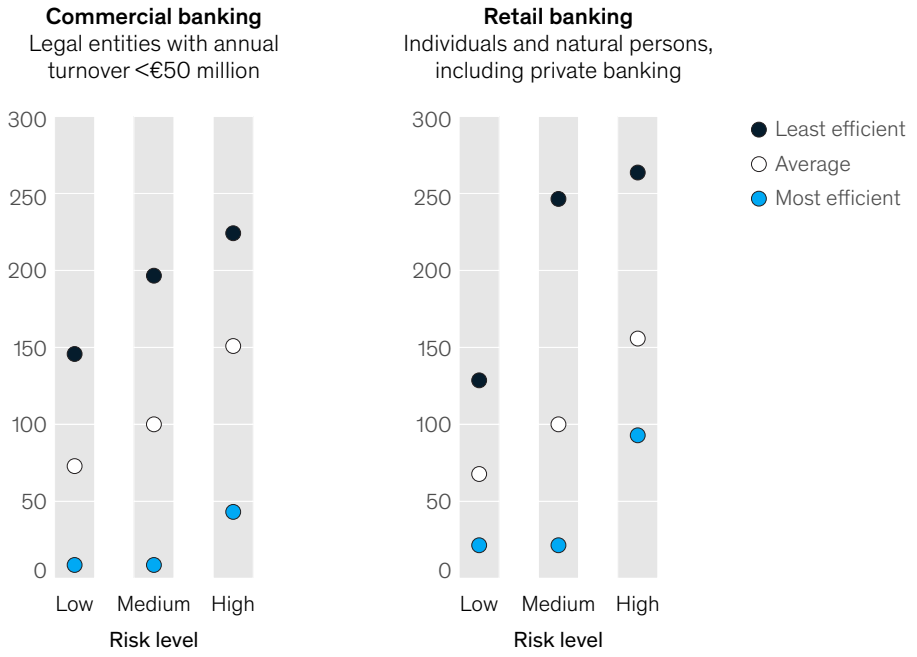
Leading organizations have addressed the key pain points in the review process. In doing so, they have been able to reduce case-handling times for mainly low-risk retail-customer portfolios to 20 or 30 percent of the time spent by competitors. In our benchmark analysis, average periodic reviews

[1] "Money laundering," United Nations Office on Drugs and Crime, unodc.org.
[2] McKinsey survey conducted in the first quarter of 2021 of ten domestic systemically important banks (D-SIBs) in Western Europe.

Exhibit 1

Banks can address inefficiencies in handling times with a clear workflow, risk differentiation, standardization, and automated processes.

Average handling times for manual review, index



for low-risk customers can take 100 minutes to complete; for organizations in the best-performing quartile, the reviews are completed in 30 minutes, on average, through an approach blending automation and targeted intervention.

To achieve a 30-minute average review time across the low-risk segment, organizations need to be able to use a blend of STP (no handling time) and manual handling (60 to 90 minutes). Experience indicates that the 30-minute average is achievable when 50 to 65 percent of the customer-file population is subject to STP.

Complete customer data are essential to success, for both manual and automated case handling. This means that data are collected and validated before the review. Digital tools are critical in this endeavor. Once the data are in good shape, an STP solution or manual case handler can perform a risk assessment without time-consuming and costly outreach. Through increased automation and shorter case-handling times, leading banks are able to realize a number of benefits:

— *Significantly lower KYC-operations costs.* Depending on the scale of automated reviews and share of customers subject to those processes, banks have been able to streamline KYC work by 20 to 30 percent. As banks move from periodic and event-driven reviews, process automation helps them manage the shift.

— *Better-quality KYC reviews.* Automating case reviews leads to more standardized, more predictable, and better quality-assurance results. Assuming that standardization and coding of rules are performed correctly, quality can be improved significantly (by a range of 15 to 40 percent, experience indicates). Manual

Banks that are able to ask KYC questions as a natural part of the digital journey tend to achieve high levels of customer satisfaction.

errors are reduced, and the identification and documentation of risks are improved. Rework loops can be shortened as well, as "first time right" ratios and regulatory targets are met more quickly. And the faster institutions are able to scale up KYC capabilities, the sooner they will benefit from quality improvements.

— *Improved customer experience.* Automating the review process often goes hand in hand with automating the outreach process. Customer-experience scores typically improve, given more streamlined and targeted digital interactions. Banks that are able to ask KYC questions as a natural part of the digital journey, including follow-ups and reminders, tend to achieve high levels of customer satisfaction.

— *Higher levels of employee satisfaction.* Automation frees up employees from tedious tasks, such as checking for completion, and allows them to spend more time on judgment-focused activities. With end-to-end STP, KYC-operations staff often find their workflows more efficient, their jobs enriched, and their career paths more interesting.

Core components of an STP solution

Building an STP solution requires four distinct steps: defining criteria for automation, determining requirements for data completeness, establishing rules for reviews, and defining review completion and documentation.

Defining criteria for automation

Banks should assign cases to STP review, human oversight (targeted review), or full manual review. The total composition will primarily depend on the risk appetite of the individual institution. Some common entry criteria for STP are as follows:

— *Specific segments.* Such areas could be private-wealth customers or retail businesses; the latter could include certain small and medium-size enterprises, such as owner-operated businesses.

— *Risk classes.* Classification is especially helpful for low- or medium-risk customers in the retail segment; most banks start their STP journeys here and scale up in a second phase.

— *Other common characteristics.* This could include identifying customers living in a certain geographical location or using accounts for a specific purpose.

Usually excluded from STP review are complex business customers, high-risk segments, and nonstandard accounts. The restriction of STP to low-risk customers only is, however, a common pitfall. In truth, if applied skillfully, STP can eventually be used with customers in higher-risk segments.

Determining requirements for data completeness

An STP approach to KYC reviews can only be undertaken after customer-data fields are made complete and up to date. Depending on the bank's

customer-risk-rating model, common data fields for low-risk retail customers include the following:

— *Static fields.* These include name, ID, address, citizenship, date of birth, social-security number, tax eligibility, gender, status as a politically exposed person (PEP), products and services, justified reasons, and roles.

— *Behavioral fields.* These include (incoming and outgoing) foreign transfers, domestic transfers, source of funds, and cash deposits.

Financial institutions first set the minimum number of data fields required for STP review, categorized by risk rating and segment. For a low-risk retail-banking customer, typically, 20 to 30 data fields are used. Institutions then determine whether data fields are complete (blank or not blank) and up to date. Customer segments that are complete are eligible for STP. The bank should also check whether the data have been validated recently.

Establishing rules for reviews

Institutions need to set the rules for automated review, including drop-off criteria (when customers are dropped from the STP solution) and reintegration possibilities (when customers are restored to STP). How do banks distinguish usual and unusual behavior across the different data fields? Many financial institutions use definitions in their standard operating procedures and case-handling guidelines. However, these definitions can require case-handler judgment and would therefore be insufficiently specific to enable encoding into an STP solution.

To establish the STP rules engine, rules may have to be specified through segmentation analysis or machine-learning patterns. Thresholds could include these examples: no cash deposits in the past 12 months, no foreign transactions in the past 12 months, source of funds limited to a certain value, unknown transactions limited to 20 percent of total volume, or account-turnover maximum at a certain value. An algorithm can be used to check these variables. Where the conditions are not met, the customer would drop off the STP solution.

Depending on the reasons for the drop-off and whether the issue is easily remedied (such as misclassified data or transactions that can be identified and explained), the case could be reintegrated into the STP flow after a targeted human intervention. If the issue is more complex, additional human control will be needed. Unusual cases can be channeled into focused handling or fully manual handling. The exercise of defining these criteria for STP review should start with the bank's risk appetite and internal standards and be refined into detailed requirements for the STP solution (Exhibit 2).

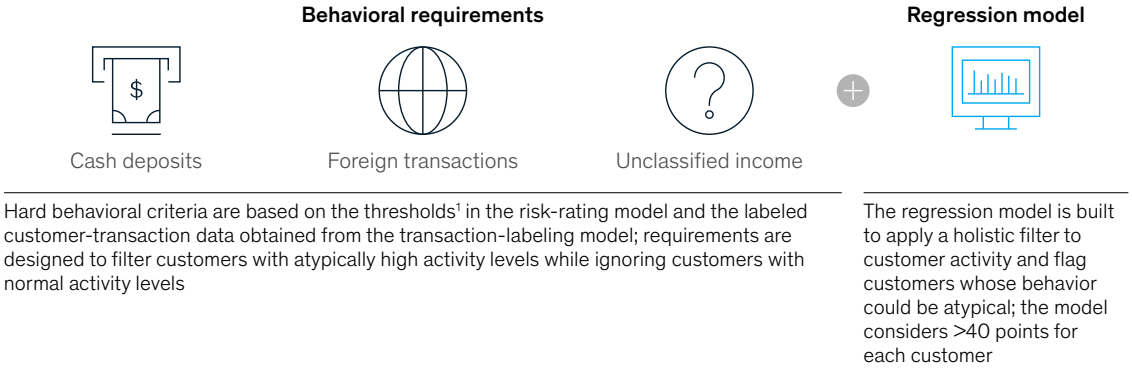
Exhibit 2

The automated-review process is defined in three stages.

	Risk-appetite specifications	High-level requirements	Detailed requirements
What	Outlining risk-appetite specifications: – Types of risks inherent in low-risk-customer population – Coverage; areas deemed acceptable for straight-through-processing solution	Requirement setting for checks and validation to be performed by automated solution (such as eligibility checks and behavioral limitations)	Translation of high-level requirements into specific checks to be performed (such as cash transactions exceeding a specified annual threshold)
How	Top-down specification based on local regulatory requirements and industry best practice	Working sessions focused on specific risk categories as identified in risk-appetite specification	Work performed by cross-functional teams, including first-line risk, business, IT development, and data science
Who	Compliance function leads effort, with dedicated support from first-line-risk function	Effort owned by first-line-risk function, with support from business function; approved by compliance function	Joint effort of first-line-risk, business, IT-development, and data-science functions; approved by compliance function

Exhibit 3

Behavioral filters can be used to choose a model for automated know-your-customer review.



[1]Behavioral thresholds are based on risk ratings and regression models.

The criteria for the type of review to be deployed (STP, focused, or fully manual) usually encompass *hard behavioral thresholds*, in line with the banks' customer risk-rating model, and *anomaly detection or peer-group modeling*, designed to identify additional suspicious behavior that may lead to risk reclassifications or offboarding (Exhibit 3). Banks should periodically review the criteria and adjust for new regulation as required.

Defining review completion and documentation

Once all the analyses are completed, a case assessment is generated. Most leading banks choose a concise standard conclusion, including the type of customer reviewed, the type of controls performed, assessment findings (such as no transactions outside determined limits), and risk implications.

An approach to developing an STP solution—a minimum viable product (MVP)—quickly can take between four and nine months. Banks can speed the process by augmenting internal capabilities with third-party components for such activities as customer outreach, data validation, risk rating, and assessment.

Key success factors

The banks that successfully enhanced KYC reviews through STP solutions have commonly done five things right in design and implementation:

— *Close up-front stakeholder alignment.* Successful projects align stakeholders first, detailing risk requirements across the three lines of defense. Additionally, they often inform regulators in advance about the proposed approach to testing, validation, and quality control.

— *An agile, cross-functional team.* The team includes representatives from business, operations, IT, and data-analytics functions as well as engineers, compliance professionals, and those from any other department involved in KYC activities or strategy. The team is ideally ring-fenced to ensure sufficient focus and short feedback loops.

— *Testing and validation.* Once the STP solution is developed, banks undertake a thorough testing and validation process. After they go live, a continuous quality-control agenda is necessary for cases in the STP flow.

— *Clearly defined ownership.* The responsibilities for documenting, maintaining, and developing the solution are made clear, and the clarity should extend to the underlying logic for dropping cases from STP into either targeted or full review. Ownership should be unambiguously embedded within the bank's governance framework, consistent with the division of roles and responsibilities for other (detection) engines and models.

— *Focus on data-quality management.* Given the importance of automated, up-front data collection, a thorough data-quality-management approach is required. The approach includes quality definitions, measurement (including dashboards), and controls.

Moving from highly manual KYC reviews to STP is a challenging task requiring considerable commitment and resources. Banks capable of astute decision making and effective implementation, however, have generated significant benefits. They have become more efficient and effective in combating money laundering and financial crime, improved regulatory compliance, and enhanced their customer and employee experience. You could not ask for more from an operational improvement.

Irene Peschel is an associate partner in McKinsey's Copenhagen office, **Kate Robu** is a partner in the Chicago office, **Sebastian Schneider** is a senior partner in the Munich office, and **Alexander Verhagen** is an associate partner in the Brussels office.

The next S-curve in model risk management

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

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

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

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

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

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

An optimized model landscape

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

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

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

The role of the MRM function

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

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

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

Sharing responsibility for model management

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

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

— *Validation.* The MRM function and risk function will still focus on validation practices, ensuring that models are of good quality and model risk is capably managed. But the business stakeholders and model developers are the ultimate users of models. As such, they must be responsible for ensuring that development costs are justified, programs are run efficiently, and models are well monitored and maintained. Such active collaboration eliminates work silos, allowing the use of common elements across the model life cycle. This minimizes friction and boosts efficiency.

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

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

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

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

The big lesson for the new MRM framework is that it must establish standards and standardize processes. This work is essential for streamlining and automation.

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

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

Streamlining and automation

This perfect storm of model-inventory revisions and development presents organizations with a unique opportunity to act strategically. The requirement is clear: institutions need to streamline the entire model life cycle, including ideation, development, implementation, validation, and monitoring. The objectives are to avoid future bottlenecks, support business continuity, and improve institutional performance while minimizing risk and cost. Crucially, banks must develop a model strategy for the coming years that meets these demands in a cost-efficient manner.

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

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

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

Finding efficiencies in the model life cycle

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

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

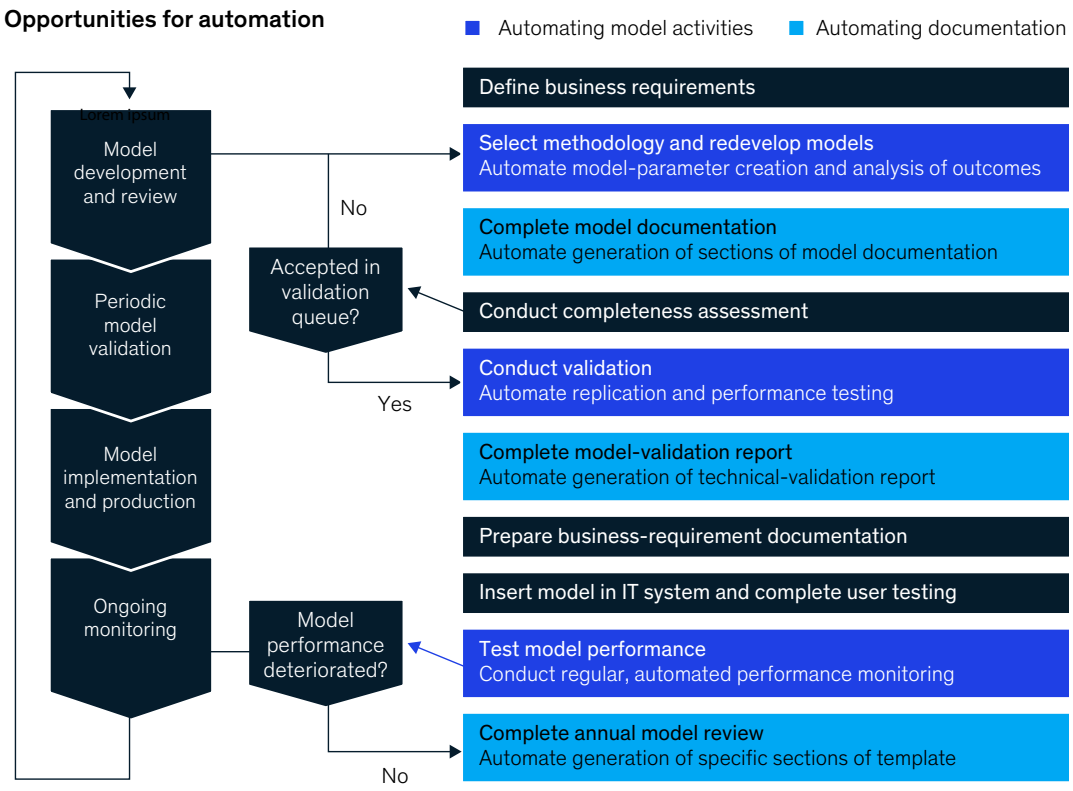
— *Model testing.* Some companies have been able to reduce the time it takes to perform testing during development by as much as 30 percent by applying standard model principles, a standard library of testing codes, automatic testing, and other techniques.

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

— *Model monitoring.* A predefined monitoring pack built around a library of key performance indicators can reduce the time required to

Exhibit

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



execute ongoing monitoring activities by as much as 35 percent.

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

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

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

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

Frank Gerhard is an associate partner in McKinsey's Stuttgart office; **Pedro J. Silva** is a solution managaer in the London office, of which **Thomas Wallace** is an alumnus; and **Maribel Tejada** is a senior expert in the Paris office.

The authors wish to thank Pankaj Kumar for his contribution to this article.

Next-generation nowcasting to improve decision making in a crisis

Traditional nowcasting has served its purpose well, but the COVID-19 crisis proved challenging for most models. A next-generation approach supports critical decision making and strategy moving forward.

by Frank Gerhard, Marie-Paule Laurent, Kyriakos Spyrounakos, and Eckart Windhagen

In the face of major economic uncertainty, the ability to gather and interpret information quickly is crucial for decision makers, especially when a crisis turns into a recovery, or vice versa. Those able to understand and react to the evolving situation quickly and appropriately will not only survive but also create a more resilient organization.

To this end, leading institutions increasingly add nowcasting—a prediction model developed in response to the dot-com bubble and the 2008 recession—to their decision-making toolbox. Nowcasting resulted from overreliance, during past crises, on typical economic data—often subject to publication lags of up to six months—which exposed many organizations to both missed opportunities and potential risks.

Nowcasting uses complex econometric techniques and contemporaneous data from a broad set of sources to provide a timely view of economic indicators and drivers and bring insights several months forward, enabling more dynamic planning. When the COVID-19 pandemic hit, many government, financial, and other institutions, hoping to capture the rapid economic shifts taking place around the world, turned to nowcasting for answers.

While traditional nowcasting has often served its purpose well—letting institutions know where they stand at the moment—it has also faced unique challenges during major unforeseen events such as the COVID-19 crisis, Brexit, and the US–China trade conflict, all of which created significant macroeconomic structural breaks in many of the relationships between economic indicators.

In addition, typical nowcasting models have become extremely complex, with many incorporating up to 50 drivers of economic growth and a variety of data and assumptions. And the more complex the model, the greater the number of historical relationships between variables that can change in response, rendering the model's estimates unreliable. At the same time, alternative high-frequency variables, such as data about footfall, air-pollution levels, and online searches, transmit market signals effectively but are not included in traditional models. Making robust decisions without consulting these variables can be problematic.

We therefore believe that today's approach to nowcasting should be revamped. We observe more reliable results when we reduce the number of variables by choosing only the most relevant, complementary, and robust key performance indicators (KPIs) for each sector and geography. And we find that outcomes are more accurate when models include selected high-frequency explanatory variables, which regularly provide a more consistent view of the way the economy is evolving and are more robust over time, creating resiliency in modified statistical models.

This new approach to nowcasting makes it easier to interpret estimates, understand structural breaks, and provide up-to-the-moment information. Further, by taking a close look at a nowcasted view of economic indicators, institutions can observe which industries are the most resilient, adapt accordingly, and make more informed decisions based on the latest data. Even for these more robust models, of course, organizations need a thorough check for structural breaks.

Nowcasting provides a real-time view

Timely information is never more important than during the onset of a major economic shift or when recovery sets in at a crisis's trough, as it allows institutions to monitor real-time information for policy analysis. While traditional forecasting has a role to play in such cases, nowcasting goes further, helping institutions understand both the current economic situation and the recent past, even when formal economic indicators have not yet been published. It has proven extremely effective as a predictor of GDP growth vis-à-vis published data, for example, which tend to lag by several months and force crisis-monitoring dashboards and scenario analyses to rely on outdated data or subjective views—creating the potential to not only impair decision making but also increase risk.

Nowcasting has given companies and regulators timely intelligence on which to base decisions and accurately predict the pace of a recovery.

Nowcasting has therefore been able to give companies and regulators timely intelligence on which to base decisions, identify scenarios as they materialize, and accurately predict the pace of a recovery. It has proved especially powerful when traditional models and proxies have failed to provide accurate estimates because of publication lags and has given policy makers and companies an edge when reacting to crisis situations.

Economic crises strain the model

Despite their usefulness, we recommend that institutions revisit their traditional nowcasting models. These models frequently generated implausible results during the COVID-19 pandemic and provided misleading reads of the economy—a result we expect in any situation characterized by great economic stress and uncertainty or periods of economic disruption.

The models' unreliability is primarily due to their reliance on too many variables. During a structural break brought about by a pandemic, for instance, and the resulting lockdown of countries and closure of businesses around the world, relationships between a multitude of variables break down and are unable to capture the impact of unexpected events and explain the economy in real time.

In addition, while global economic crises such as the 2008 recession have often had comparable effects across regions and industries, the pandemic-related shutdowns hit each country and sector quite differently. Countries that rely more on international travel, such as the United Kingdom, were harder hit than those that rely on intracountry travel, such as Germany. The automotive and hospitality industries ground to a halt, and factories, showrooms, hotels, and restaurants closed. The demand for consumer goods, fitness equipment, and healthcare products, however, soared.

It's time for a next-generation nowcasting approach

In light of the limitations of the traditional models, we recommend a modified approach to nowcasting that uses country- and industry-specific expertise to boil down the number of variables to a selected few for each geography or sector, depending on the individual economic setting. Given the specific selection of each core variable, the relationships between the variables will be relatively stable over time, even during a major crisis. Admittedly, the more variables used, the easier it is to explain an economic shift; however, using more variables also means a greater chance of a break in some of the statistical relationships, particularly in response to an exogenous shock.

This revised nowcasting model will be more flexible and robust in periods of economic stress. It will provide economically intuitive outcomes; include the consideration of complementary, high-frequency data; and offer access to economic insights that are at once timely and unique.

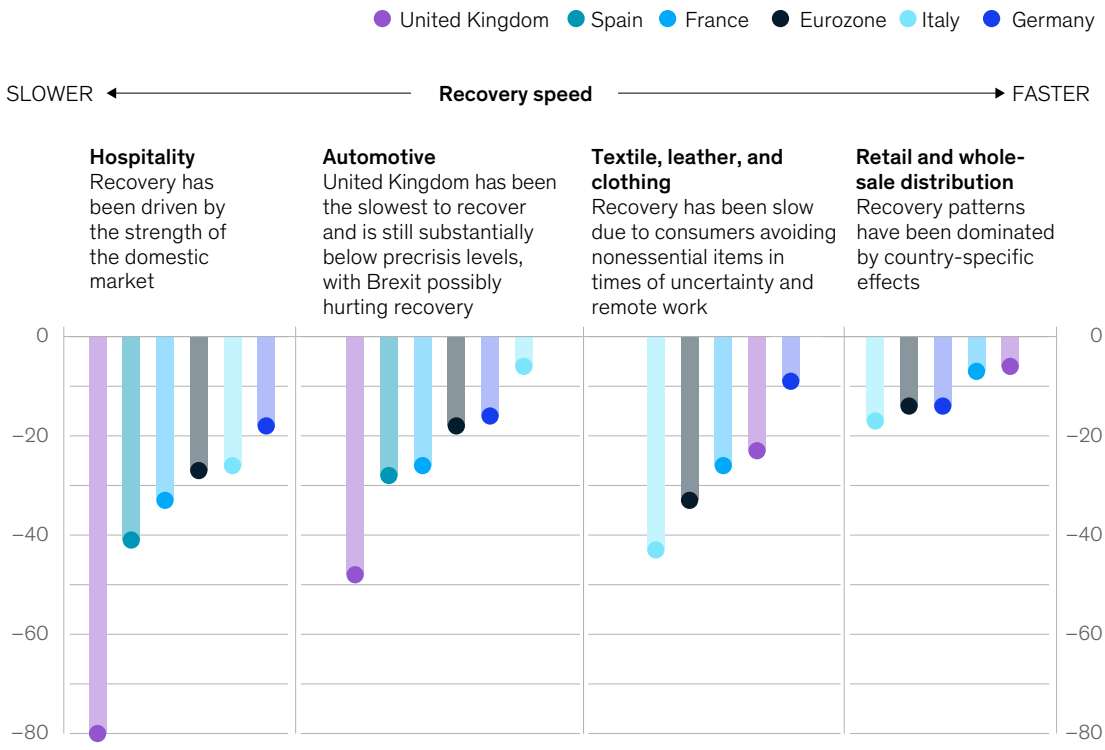
For example, consumer spending can be estimated in different US cities by combining data such as wages from business applications and footfall from mobility-trend reports. As a more complex example: eurozone capitalization rates are, at the time of the writing of this article, available only through January 2021. However, a revamped nowcasting model can estimate current capitalization rates in various European countries by employing a handful of real-time and high-frequency variables for each, such as retail-confidence indicators, stock-exchange indexes, price expectations, construction estimates, base-metals prices and output, and even deposits into financial institutions. The choice of variable should, of course, be guided by industry and sector experts.

Similarly, published figures for gross value added (GVA) at the sector level in Europe are available only up to the second quarter of 2020. However, by utilizing selected variables, the new approach to nowcasting can provide an estimate of GVA through the first quarter of 2021. It can also highlight the different experiences of each region and industry sector in the recent recovery. Note that the sectors reliant on in-person interactions and of a nonessential nature have been slow to recover, as have the countries more reliant on international markets (exhibit).

Exhibit

Nowcast for the first quarter of 2021 shows differing recovery speeds by sector and geography.

Gross value added Q1 2021 as percentage of Q1 2019,[1] %



[1]Percentage difference between nowcasted Q1 2021 and actual Q1 2019 gross value added, with precrisis levels set at zero. Comparison is made with Q1 2019 because Q1 2020 numbers may already include some COVID-19-crisis impact.

Nowcasting supports decision making and strategy

Organizations of all types can use the up-to-date country and sector information produced by this new type of nowcasting model to support their decision making and shape their recovery strategies, taking into account the fact that individual sectors are affected differently in different countries and during different types of crises.

For government institutions, nowcasting can provide real-time insights into the current state of the economy and the direction in which it is heading. It can inform revenue planning and cash-flow management. It can provide assessments of the impact of previous policies and instruct the need for adjustments. And it can proactively prepare support packages in the event of a significant downturn in a given sector.

For financial institutions, nowcasting can help make economic assessments that support the identification of investment opportunities in specific sectors and geographies. It can also shape sales campaigns based on insights into sectoral trends and economic recovery paths; instruct lending strategies, pricing, and restrictions; and update input to the early-warning system.

Industrial businesses can also use nowcasting to provide a timely view of consumer-demand and sector evolution, allowing them to rethink their production and sales strategy.

Organizations can create a new nowcasting model by first identifying the KPIs that have a lengthy publication lag and that are most important for decision making. They should then link these KPIs statistically with related variables that are available more quickly and frequently. They should have experts review the resulting model, which they can then use to support informed decision making. The model can be further refined over time based on its performance and the availability of more data to support estimates.

Once the new model is complete, organizations should be sure to integrate it into their processes and systems, enabling reliable monitoring, easy updates, and direct input into the decision-making process.

Frank Gerhard is an associate partner in McKinsey's Stuttgart office; **Marie-Paule Laurent** is a partner in the Brussels office, where **Kyriakos Spyrounakos** is an expert; and **Eckart Windhagen** is a senior partner in the Frankfurt office.

Risk & Resilience Practice leadership

Maria del Mar Martinez and Fritz Nauck
Global
Maria_Martinez@McKinsey.com and
Frederic_Nauck@McKinsey.com

Gabriele Vigo
Asia
Gabriele_Vigo@McKinsey.com

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

Kevin Buehler
Risk Dynamics
Kevin_Buehler@McKinsey.com

Ida Kristensen
Cyber Practice
Ida_Kristensen@McKinsey.com

Marco Piccitto
Risk People
Marco_Piccitto@McKinsey.com

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

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

In this issue

August 2021
Designed by McKinsey Global Publishing

McKinsey.com