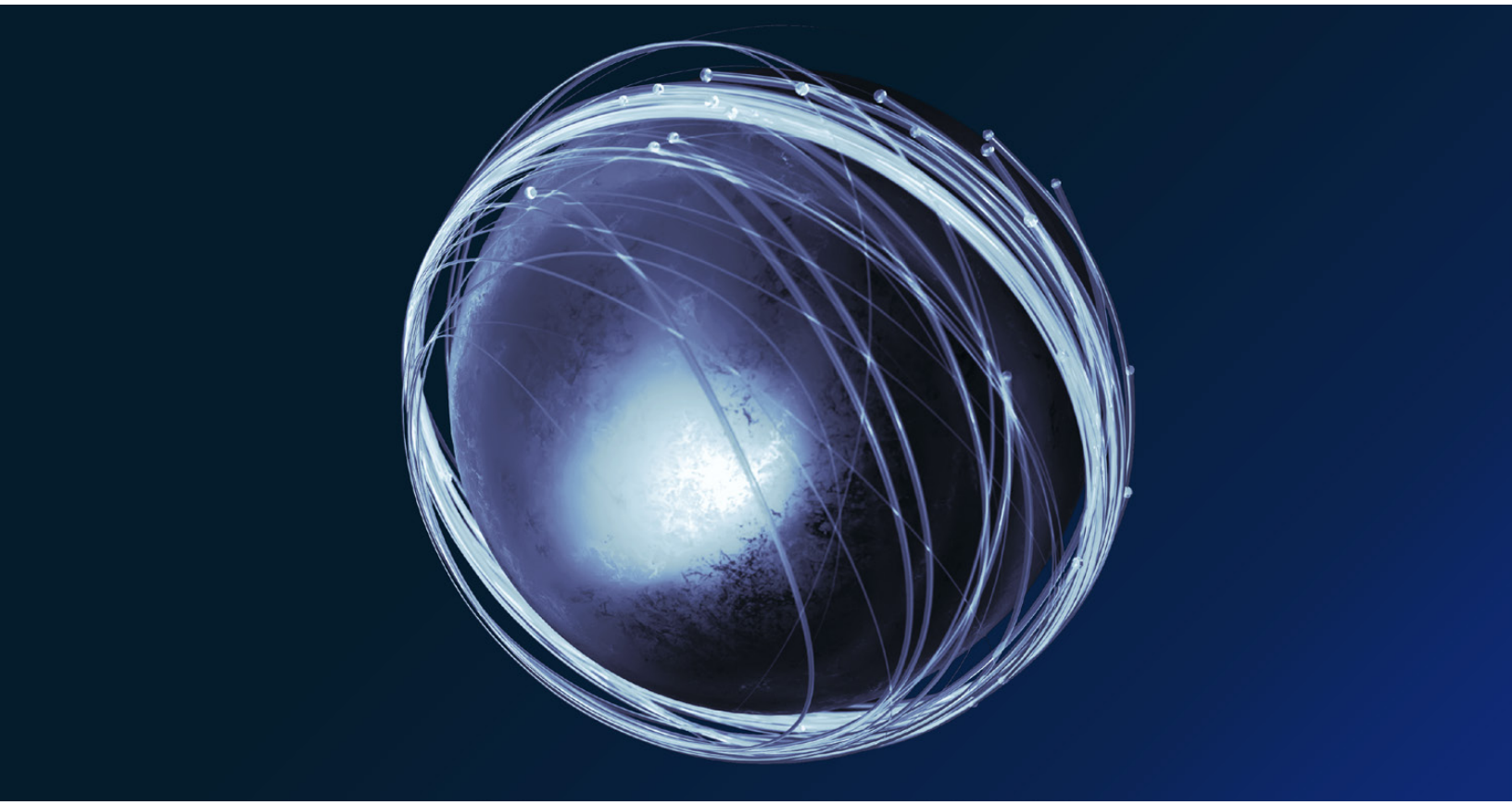
McKinsey & Company

Risk Practice

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



January 2021

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

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

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

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

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

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

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

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

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

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

risk-management demands of digital and analytics transformations.

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

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

A broad set of new (and expensive) risks

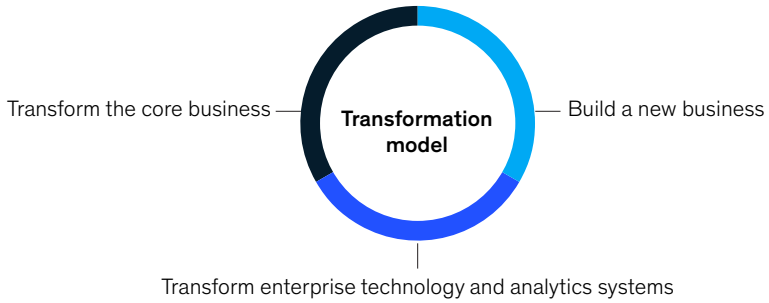
Most companies appear to do little about the nonfinancial risks generated and exacerbated by digital and analytics transformations. The scope of these risks is broad. Digital and analytics transformations are often deployed across organizations, involving many departments and third parties. Soft factors 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.

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

Exhibit 1

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

Approach to digital and analytics transformations



Transformation domains

- Multichannel customer experience: redesign and digitize top customer journeys end to end
- Digital marketing and pricing: revenue management, promotions-dynamic business-to-business pricing, cross-selling and upselling
- Sales digitization: digital sales, remote-selling effectiveness
- New digital propositions: create new revenue streams by building digital propositions, using next-generation 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 application programming interfaces (APIs), microservices, and containers
- Data transformation: unify data governance and architecture to enable next-generation analytics
- Core system modernization: achieve through refactoring or platform replacement
- Cloud and DevOps: migrate applications to hybrid cloud and/or software as a service (SaaS) and implement software development and IT operations (DevOps)
- Digital and analytics talent and capabilities: acquire needed new talent and build capabilities at scale

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

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

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

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

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

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

A snapshot of digital and analytics transformation risk management

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

Transformations are becoming commonplace across industries

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

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

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

Risk management is not keeping pace

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

Companies are unsure of how to manage digital risks

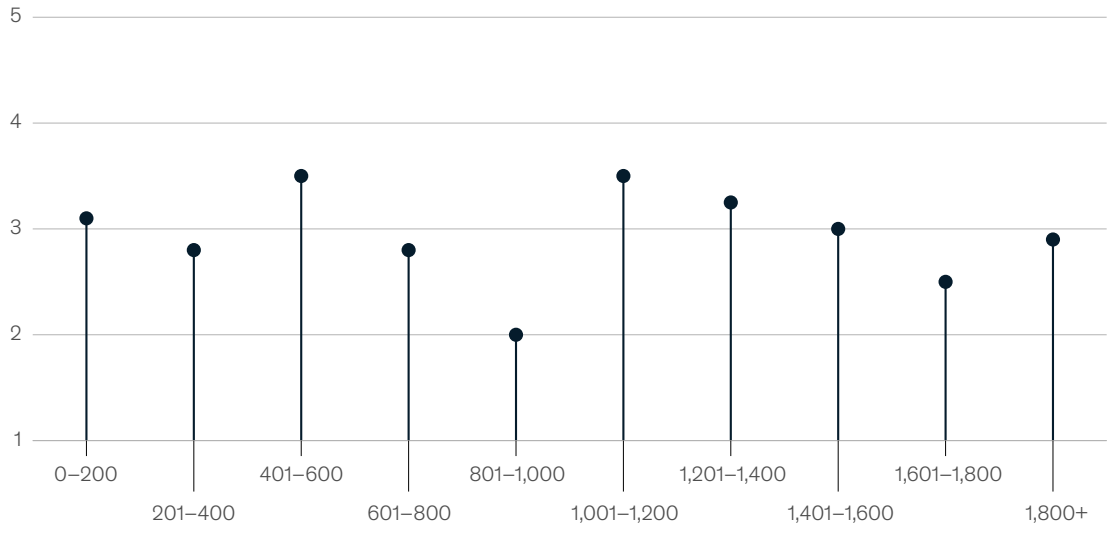
Unlike for financial risk management, in which companies tend to have established roles and processes (such as model risk management), companies in our survey do not have established roles, processes, or even consolidated understanding of digital and analytics risk drivers. The biggest challenge leaders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

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

Exhibit 2

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

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



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

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

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

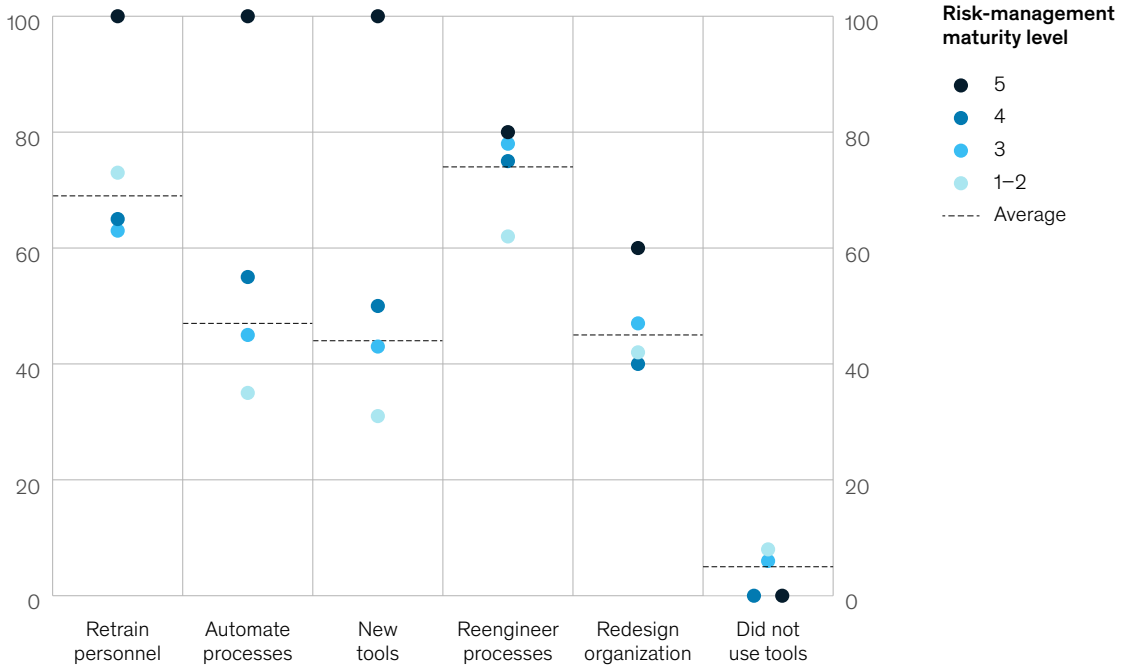
Here are the most relevant approaches leaders cite:

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

Exhibit 3

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

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



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

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

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

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

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

Pain points in managing digital and analytics transformation risks

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

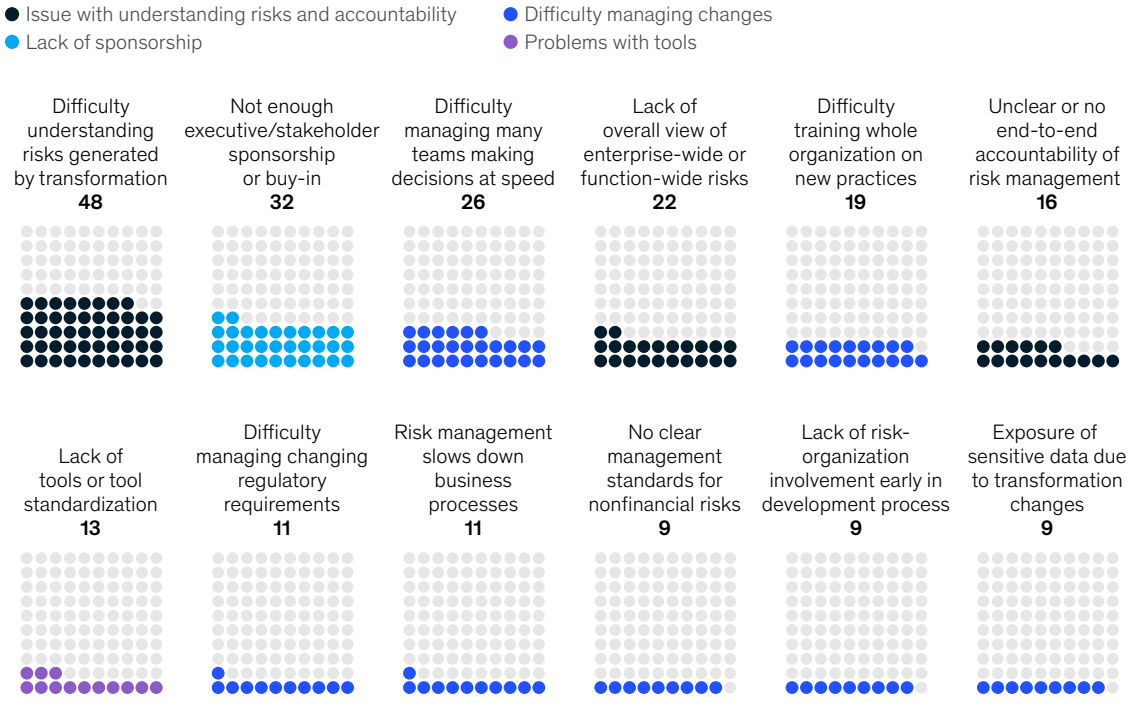
Understanding risks

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

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 five risk-management pain points?
Source: McKinsey Global Survey on Digital and Analytics Transformations in Risk Management, 2020

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

Overcoming operational limitations

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

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

A framework for digital and analytics transformations

The risks engendered in a digital and analytics transformation may be different from those that companies normally face—or they may be traditional

risks that happen with extraordinary frequency and potential for significant impact. Fortunately, most companies already have a foundation in place to begin addressing these risks: their existing enterprise-risk-management infrastructure, which is used for financial and regulatory risks. Enterprise risk management typically consists of several common activities, including the following:

— defining a mature enterprise-risk framework

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

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

— establishing risk-management processes

— creating a risk culture

These activities are critically important to digital and analytics transformations. They must be transformed alongside digital and analytics teams, however. This is because risk management will have to keep pace with the rapidly changing digital-risk landscape to continue mitigating risks but avoid slowing down the business. Our framework makes it easier for organizations to do this. It consists of four steps that define, operationalize, embed, and reinforce the elements of the transformation. The framework fosters a dynamic approach, helping adapt the existing ERM infrastructure for an increasing flow of risk-mitigating information and actions. Within the framework, organizations design transformation activities and make appropriate interventions. The framework is updated as the activities change ways of working, risk appetites, risk exposure, and talent needs (Exhibit 5).

— *Define:* In the first step, organizations apply the technology-specific elements of their existing risk-management framework—in place to address traditional categories such as financial

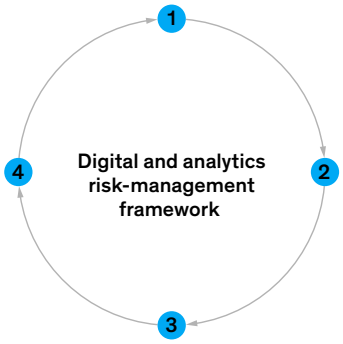
Exhibit 5

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

Current state

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

Transformed state



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

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

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

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

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.

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

Benefits of the framework and transformation roles

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

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

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

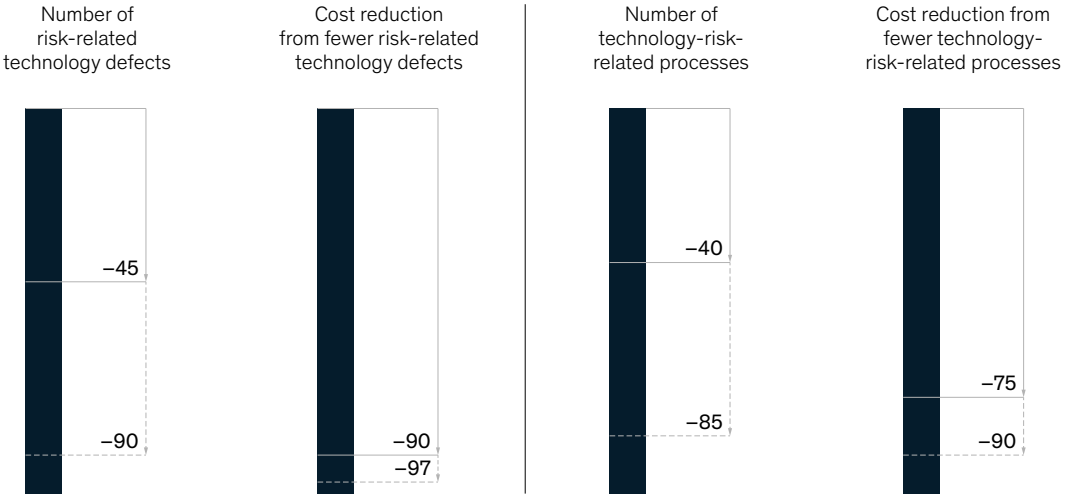
— *Digital and analytics transformation lead*: This lead is accountable for delivering the digital and analytics transformation activities.

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

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, %



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

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

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

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

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

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

Finally, companies will have to raise awareness of digital and analytics risks in the organization,

Snapshot of a successful transformation

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

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

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

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

including with the executive team and board. Likewise, they must adequately incorporate digital and analytics risk management into their formal risk governance models (see sidebar, "Snapshot of a successful transformation").

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.

Designed by McKinsey Global Publishing