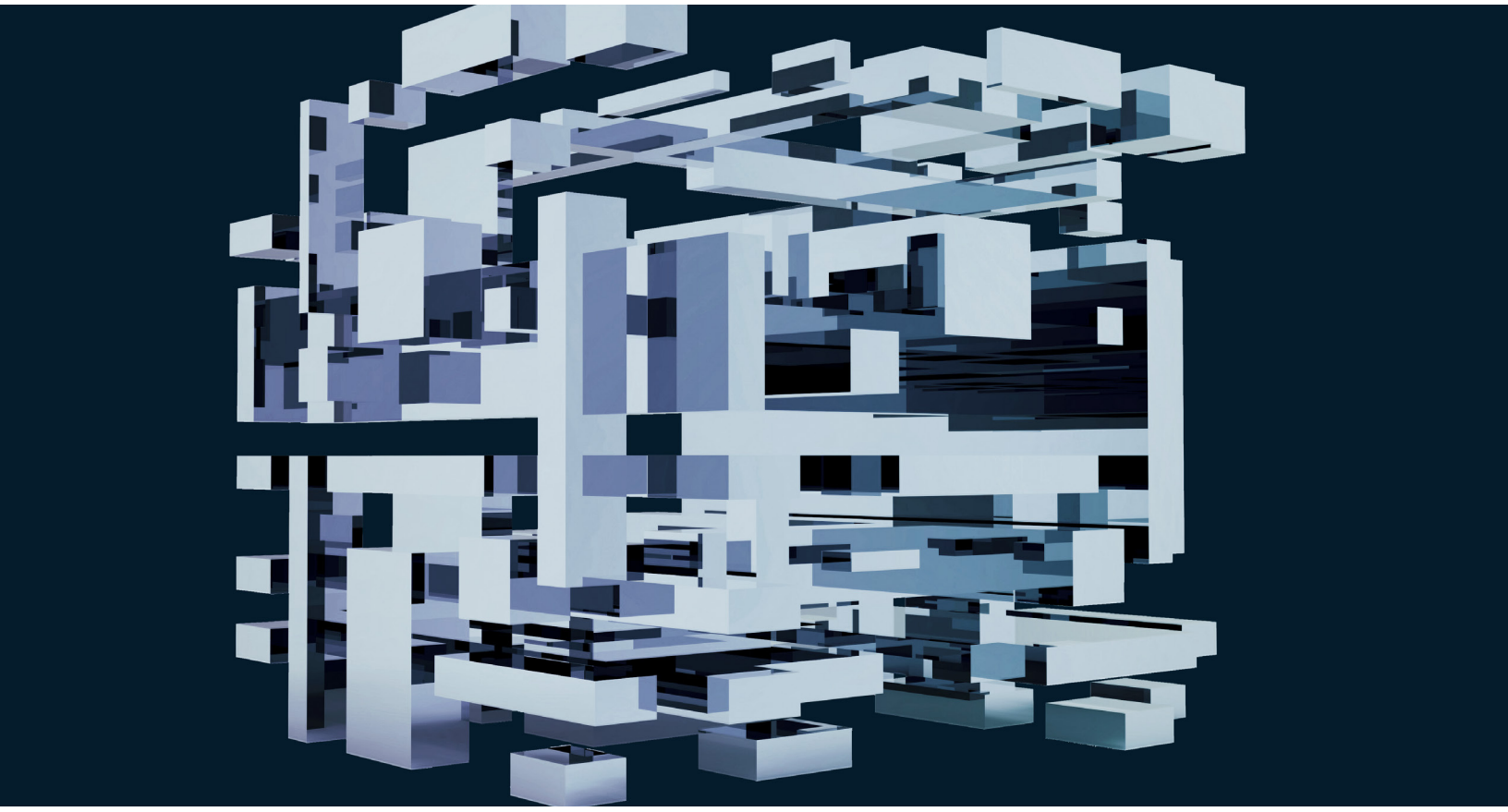
McKinsey & Company

Risk Practice

Transforming risk efficiency and effectiveness

An enterprise-wide risk transformation can substantially improve risk management while also sustainably trimming costs.

by Oliver Bevan, Matthew Freiman, Kanika Pasricha, Hamid Samandari, and Olivia White



April 2019

Since the financial crisis of 2008 to 2009, financial institutions large and small have significantly expanded their risk and compliance functions. Many global banks have added thousands to their head count in these areas. At large regional banks, the growth rate of the risk function has been as much as twice that of the rest of the organization. At many smaller institutions, the handful of people working on compliance as part of the legal function or on risk as part of the finance function have now grown into full-scale risk and compliance functions with several hundred people.

With increased head count came increased complexity. Many institutions grew rapidly and piecemeal, often scrambling to respond to regulatory feedback or indirect pressures. Often the expansion was "two for one": when banks added risk managers to the second line of defense, they also had to hire in the first line, to execute the additional requirements set by the expanded risk function. Conversely, additions to the first line prompted second-line hiring at a higher rate than before, to provide oversight in a more demanding regulatory environment. Alongside staff growth, policies, committees, and reports proliferated. Complex risk functions and burgeoning policy landscapes in turn led to more involved processes, often with layers of controls added over time, without consideration of a holistic design.

Most banks today are looking to improve productivity. In recent years, many institutions have seen risk management as off limits for cost reductions. Actions to reduce cost required cutting through the complexity and therefore were viewed as hazardous, given the demands of risk management and regulatory expectations. Now, seeing potential regulatory stability on the horizon, some banks are seriously considering efforts to decrease the cost of risk management.

However, efforts to improve risk-function efficiency can only draw from the standard set of productivity measures at their peril. Effective risk management requires a large diversity of roles with highly specialized knowledge and technical skills and so is not suited to boilerplate application of transformation levers, such as spans and layers. Furthermore, while regulatory pressures may ease, they will not disappear. Banking regulators remain appropriately concerned about the strength and integrity of risk functions. Attempts to improve risk-function efficiency, if not carefully nuanced, will invite more scrutiny. Most important, risk management guards against costly mistakes and failures. Today's environment is characterized by rising levels of risk emanating from the shift to digital channels and tools, greater reliance on third parties and the cloud, proliferating cyberattacks, and multiplying reputational risks posed by social media. Faulty moves to make risk management more efficient can cost an institution significantly more than they save.

Fortunately, the most potent levers for increasing risk-management effectiveness, if applied in careful sequence, also improve efficiency. A well-executed, end-to-end risk-function transformation can decrease costs by up to 20 percent while improving transparency, accountability, and employee and customer experience.

A sequential transformation in mutually reinforcing stages

Banks looking to transform risk management should, in our view, focus on four mutually reinforcing areas: organization, governance, processes, and digitization and advanced analytics. While enhancements isolated in each area can boost both effectiveness and efficiency, the true potential comes from tackling them in *sequential order*. Organizational optimization facilitates governance rationalization, which facilitates effective streamlining of processes, which enables digitization and advanced analytics to yield maximal benefit:

— *Optimizing the organization.* Organizational optimization yields effectiveness gains by clarifying responsibilities, increasing accountability, and matching talent to jobs. These same changes also promote efficiency by reducing redundancy in activities across the first and second lines of defense. Perhaps most important, organizational improvements lay a necessary foundation for rationalizing governance, streamlining processes, and digitization.

— *Rationalizing governance.* By rationalizing governance, banks can focus attention on what matters most and remove pain points for the business. Eliminating unneeded activities frees up a scarce and precious resource—management bandwidth—while yielding some direct efficiency benefits. Most critically, rationalized governance sets the foundation for streamlining processes as well as for digitization.

— *Streamlining and strengthening processes.* By streamlining processes, institutions can take dramatic steps on the efficiency–effectiveness curve while creating better employee and customer experiences. Streamlined processes are also easier to digitize, either in targeted ways or in full.

— *Digitizing and deploying advanced analytics.* Finally, digitization and advanced analytics can augment and magnify the impact of process redesign, allowing for full impact to both risk-management effectiveness and efficiency. Appropriately automated processes are less error prone and less costly. Perhaps even more important, digitization permits institutions to embed automated real-time (or near-real-time) risk controls within core processes. This reduces control failures and makes far more efficient use of resources.

The sections that follow discuss all four areas, providing detail on challenges, improvement opportunities, and implementation.

Optimizing the organization

A clear and streamlined organizational structure serves as a starting point for end-to-end risk-transformation efforts. By then clarifying roles and responsibilities across the first and second lines of defense, institutions can improve accountability, ensure full coverage of the risks they face, and reduce duplication of effort. Through judicious centralization, banks can improve standardization and trim overlap. Moreover, selective relocation of resources (offshoring or near-shoring) can expand talent pools.

Tailoring organizational reporting lines in the risk function

A number of banks are looking to improve their risk-management organizational structures but are unsure how to move beyond making piecemeal changes. Given the diversity of risk-management demands that must be met in a coordinated way, getting the core structure right is a challenge.

No single answer is appropriate for all banks, which have established many different roles reporting to the chief risk officer (CRO) (Exhibit 1). However, the risk organizational structure typically involves four different types of roles:

— *Risk-aligned roles* have end-to-end oversight of a major risk type (such as credit, compliance, or operational risk) or a collection of conventional risk types, such as nonfinancial risks.

— *Business-aligned roles* oversee business units or areas of broad business focus, such as consumer or commercial banking.

— *Geography-based roles* oversee activity in specific locations, usually at institutions with significant international operations, or where required by local jurisdictions.

— *Enterprise-wide roles* have responsibility for activities that need to span risk types, businesses, and geographies in a coordinated way. Examples include enterprise risk management (ERM)

Exhibit 1

The risk organization's structure typically accommodates four different types of roles reporting directly to the chief risk officer.

Selected examples

Risk-aligned roles
Credit risk
Market risk
Liquidity risk
Model risk
Compliance
Operational risk
Reputation risk

Business-aligned roles
Consumer
Commercial
Investment bank
Wholesale
Asset management
Wealth management

Geography-based roles
Asia–Pacific
Europe
Latin America
Middle East and Africa
North America

Enterprise-wide roles
Enterprise risk management
Risk governance
Risk reporting
Advanced analytics
Model development
Country risk
Programs office
Regulatory relations
Risk human resources
Risk finance
Risk operations

or analytics and model development. Many institutions have special programs established to meet a specific need, such as a large-scale digital transformation or high-profile remediation, that would also fall under this category.

CROs can apply the following five ideas to create a fit-for-purpose structure that provides a foundation for effective and efficient risk management:

— *For each major risk-oversight activity, assign primary responsibility to either risk-aligned or business-aligned groups.* In our experience, for at least some risk-management activities, many institutions either fail to specify what role has primary responsibility—leaving gaps—or else give the responsibility to several groups—creating overlapping authority. In either case, the result is confusion and duplication. To guard against this, CROs should determine which role has primary responsibility for each activity, thereby improving effectiveness by enforcing coordination within the second line while limiting duplication of resources. For example, both business- and risk-aligned groups may want to conduct independent testing. If they do this without coordination, however, the business is unduly burdened and the independent results are difficult to aggregate or even reconcile. A better approach is to have either the business- or the risk-aligned group be clearly responsible for testing. That group would build testing to the standards and requirements of both, so that results can be readily aggregated by risk type as well as by the business.

— *Assign risk-aligned units responsibility for setting policies, reporting, and testing standards for their risk type.* If these activities are left to business-aligned groups alone, each may tailor approaches to its own specific needs, generating confusion, hindering cross-company transparency, and making it difficult to aggregate risk at the enterprise level. In practice, the risk-aligned roles directly reporting to CROs should

cover the areas of highest risk. Most CROs have direct reports for credit risk, operational risk, and compliance. Institutions with large trading books typically have a head of market risk reporting to the CRO; taking on a head of model risk has also grown increasingly common, particularly at the largest banks in the United States.

— *Ensure that businesses have unambiguous points of contact in the risk organization.* The risk organization should have sufficient business expertise to provide effective oversight while also providing business units with clear points of contact. Smaller institutions often do not have business-unit-aligned roles reporting to the CRO; instead, each risk-aligned group maintains a single point of contact for each major business. This approach requires each business to manage multiple points of contact and can become burdensome at scale. Larger or growing institutions should therefore consider having a CRO direct report for each major business area. For example, one growing regional bank had only risk-type roles reporting to the CRO; to ensure that the business had clear points of contact, the bank established business-aligned roles with significant oversight and monitoring resources. Risk-aligned roles continued to develop policy and provide aggregated risk-type reporting. Banks with a mature and integrated mode of operating and sufficient distributed expertise may not require formal business-aligned roles in the risk organization. In our experience, however, this is the exception rather than the rule.

— *Within geography-based groups, mirror the groupwide approach for setting responsibilities for risk-aligned versus business-aligned roles.* Many jurisdictions require all risk-management personnel to report through the regional CRO, who has ultimate jurisdictional accountability for risk-management oversight. Too often, the risk leadership in different geographies of multinational banks make their own independent decisions on responsibilities within their team, impeding enterprise-wide consistency and aggregated risk reporting. To achieve a coordinated approach, institutions should clarify group-level principles and apply them across all geographies. Exceptions make sense only where local regulations impose a substantially different or higher standard (an issue well known to foreign banking organizations operating in the United States).

— *Create single-point senior accountability for activities requiring enterprise consistency.* Certain activities require common standards and consistency of approach across risk types, businesses, and geographies. Examples include enterprise-wide approaches to risk appetite, risk identification, and issue management. An enterprise risk-management function is reemerging, even at larger banks, as a critical unit reporting to the CRO with responsibility for such areas. Many larger banks also have or are establishing a head of regulatory relations as a CRO direct report, to establish standards and governance over regulatory interactions. Any enterprise-wide roles should have a clear mandate, to avoid proliferation of central project-management-type positions.

In our experience, a successful risk reorganization should begin with an honest assessment of the strengths and weaknesses of the existing organization, incorporating business input. Using this as a basis for applying the principles described above will yield an organization that is more responsive to the business, with a consistent, logical structure guided by principles, discharging its oversight responsibilities effectively and efficiently.

Clarifying roles and responsibilities across the lines of defense

All too often, responsibilities can overlap both across and within the lines of defense, compromising the ability to streamline governance and processes. For example, we frequently observe overlapping control and testing environments across the first and second lines of defense. The following central ideas can guide institutions in clarifying roles and responsibilities:

— *Form a clear view of all risk-management activities actually undertaken.* At most banks, the precise nature of at least some risk-management activities is unclear. The lack of clarity suggests the possibility of gaps, duplication of work, or inadvertent inconsistencies in approach across businesses or risk types. Two common examples of duplication are monitoring and risk reporting undertaken by both the first and second line of defense. Likewise, activities related to vendor management or complaints processing across businesses are examples of areas where inconsistencies commonly occur. Clarity around who is doing what throughout the risk organization is also a valuable, efficiency-fostering outcome in and of itself.

— *Define and clarify roles across the lines of defense, applying them to activities.* Not uncommonly, risk roles are poorly delineated across the lines of defense, as groups in different lines carry out similar activities (Exhibit 2). Duplication is most likely to arise where regulatory guidance on roles is not specific—in vendor management, for example, or in monitoring and testing. Poor delineation of roles can also lead to gaps, with no group clearly responsible for performing needed activities. Appropriate corporate-risk activities for cyberrisk, for example, are not performed at many institutions. To eliminate both gaps and duplication, banks should establish principles for delineating lines of defense and use them to sort each activity as belonging in either the first or the second line of defense.

— *Avoid the notion of a '1.5 line of defense' by incorporating such activities into the true first line.* Some banks create what they call a "1.5 line of defense," mandated to complete first-line risk activities, such as quality assurance and reporting. Despite its apparent logic, the 1.5 line can create more confusion than clarity. Where it exists, the true first line—the frontline business—often fails to integrate risk management into its core processes and decisions. This removes real accountability from the business and often implies that risk-management activities are not its responsibility. The second line, meanwhile, can either become overly reliant on the 1.5 line or else view it as inadequate and perform its own, duplicative control testing.

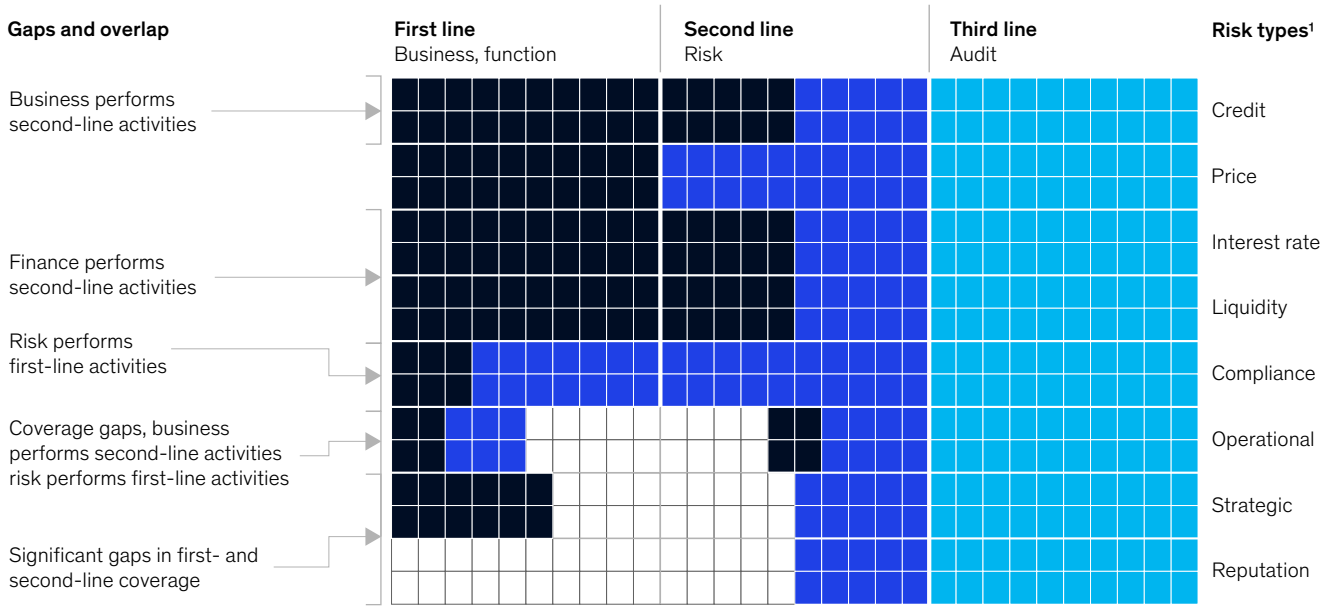
— *Ensure a clear approach to activities performed within enterprise functions, including legal, HR, and finance.* In our experience, at nearly all institutions, enterprise functions have ambiguous relationships to the lines of defense. Banks should clarify this by putting in place a systematic approach to oversee the component activities within each function. The board and the risk function, as well as enterprise-function leaders themselves, might all play a role in such oversight. At the same time, institutions need to specify which activities executed by the rest of the organization are overseen by enterprise functions. For example, HR might provide oversight of risk related to incentive compensation throughout the enterprise, including responsibility for related activities, such as developing policies or conducting independent testing and monitoring. Finally, banks need to establish principles for how these enterprise functions will participate in enterprise-wide risk-management programs—such as risk identification, risk reporting, and risk appetite—contributing to the aggregate view of risk across the bank.

Achieving the correct alignment of roles and responsibilities across the lines of defense is a difficult undertaking. Enterprise-wide projects with this aim can generate mountains of paper without yielding clarity or benefit. Successful organizations begin by establishing principles for which type of activities fall into which lines of defense. Next, these banks make inventories of activities through working sessions with businesses, enterprise functions, and corporate-risk groups, also identifying gaps and areas of duplication. Finally, they realign activities to be consistent with lines-of-defense principles. This step often results in organizational adjustments: for example, some banks have moved parts of the chief information security officer's organization to

Exhibit 2

By delineating roles across the three lines of defense, institutions can improve clarity, eliminate gaps, and reduce overlaps in activities.

Schematic example of roles and responsibilities before improvement



[1] The eight categories of risk for bank supervision as defined in *Comptroller's Handbook: Corporate and Risk Governance*, Office of the Comptroller of the Currency, July 2016, occ.gov.

corporate risk to provide second-line coverage of cyberrisk; others have moved groups focused on controls testing from operational risk into the relevant businesses.

Centralizing resources and optimizing location

Even after clarifying roles and responsibilities, banks can discover inefficient resource and talent allocations resulting from overly segmented resources. At most banks, similar risk-management activities are duplicated in different physical and organizational locations or talent is mismatched to roles. For example, data scientists in wholesale risk may be asked to write reports or fix technology issues because demand for analytics in their specific area is insufficient to keep them fully occupied. Meanwhile, other risk areas may be using nonspecialists on analytics work because the demand is inadequate for a dedicated specialist. An appropriately agile strategy for centralization and location should be based on the following principles:

— *Centralize common activities, particularly those requiring specialized skills or consistency.* Some banks have centralized certain resources and activities to maximize gains from existing talent and maintain consistency. Typical candidates for centralization are activities requiring specialized talent (such as data and analytics) and those for which consistency creates demonstrable benefits (such as testing and monitoring). The results are sometimes termed "centers of excellence" (COEs). They can help balance workloads, reduce duplication, promote consistency of approach, and conserve scarce talent. The creation of a "center," however,

does not guarantee "excellence." Achieving excellence requires much more than gathering people within a single organizational construct. A regional bank discovered inefficient hand-offs and duplicate activities among its dispersed modeling groups within the risk function. By creating one data-and-modeling group and realigning underlying processes, the bank addressed these shortcomings, better balanced the workload, and promoted greater discipline around data management.

— *Establish clear protocols for COEs to interact with the rest of the organization.* In creating centers of excellence, banks should proceed with caution. COEs can erode trust between the parts of the organization that have lost resources to centralization and now experience a change in service level. To ensure that COEs truly achieve their intended objective, banks should adopt a clear model for interaction between each COE and businesses or functions; this model can include service-level agreements and specify turnaround times. Without a clear, agreed-upon model for interaction, the businesses might re-create COE capabilities in shadow functions that will further bloat the organization and generate additional confusion around responsibilities.

— *Develop an appropriate location strategy.* To tap new talent pools and conserve resources, some institutions have moved certain activities to offshore locations. Reconfiguring the geographic footprint of the risk function requires a nuanced and discipline-specific approach. Many risk roles, particularly those with a strategic or advisory focus, cannot be relocated, as they need to be close to the first line. However, some important roles, including model development and validation, are suitable for relocation. While moving these roles can improve efficiency, banks must carefully balance such movements with their need to have the right talent in each role. For some activities, in fact, needed talent may be more readily available in offshore locations.

— *Adopt a more agile model to balance the seasonal workload.* The seasonal or periodic nature of certain critical risk activities (such as stress tests and project-based remediation efforts) has been a consistent pain point for banks and the employees tasked with working on these projects. Banks can struggle to maintain efficient utilization of resources at times when these employees' main responsibilities are not as demanding. In addition, employees long serving in these roles may lose motivation and start looking elsewhere for better opportunities. Redeploying talent for shorter periods of time on a project-by-project basis would address the imbalance. This may also help retain talent, resolve resource gaps around the organization, and cross-pollinate best practices. A further benefit may be better integration of these activities into business-as-usual activities over time. For example, teams developing stress scenarios for regulatory exams could also support economic forecasting for particular lines of business.

Careful decisions about what and how to centralize, what is an appropriate location strategy, and how to inject agility into the risk organization are needed if an institution is to deploy talent efficiently and complete essential risk activities. These decisions typically build on the detailed activity analysis generated by the work to clarify roles and responsibilities. Decisions can also be tackled independently, provided that adequate attention is paid to the centralization, location, and talent strategy as well as the nuances of the risk context.

Rationalizing governance

With an optimized risk organization, institutions can proceed to developing appropriate governance. To focus attention on what matters most, banks need to rationalize policies and eliminate unnecessary effort on downstream procedure management. Committees need to be streamlined to improve focus, accountability, and lines of escalation—and to save executives' time. Together with an optimized

organizational structure, rationalized governance is a precondition for streamlining processes and digitizing risk management.

Rationalizing policies

At many firms, risk policies have become too numerous and therefore difficult to manage. Thousands of hastily created risk and compliance policies can be in place at midsize and large banks, with single policies spawning dozens of procedures across businesses, each of which influences process and control design.

Institutions have reduced as many as 30 percent of their policies while improving the quality of the remainder (Exhibit 3). Policies can be structured to focus attention on the areas of highest risk while removing unnecessary red tape for the businesses. Meanwhile, the cost and effort of policy administration and management are likewise reduced.

Institutions attempting a transformation can discover that nearly all policies merit some adjustment, if not total rewriting, to better reflect risk appetite, improve clarity, and achieve the right level of detail. They can begin renovating their policies by establishing a set of design principles, to understand the challenges and identify the target state. The following four principles are essential, each addressing common pain points:

— *Cover all risks, businesses, and cross-enterprise programs with precisely worded policies.* Missing or vague policies admit activities that are not aligned with the institution's risk appetite. Gaps in coverage arise most commonly in policies governing cross-business or cross-functional programs, such as new business initiatives and third-party risk management. Gaps are also found in policies addressing less mature areas of risk management, such as cyberrisk and conduct risk. At one bank, for example, ambiguous policies governing new-product initiatives resulted in unclear roles and responsibilities for the evaluation of new ventures, thus allowing decisions that were misaligned with the bank's risk appetite.

— *Ensure that no topic is covered by more than one principal policy.* Overlapping or redundant policies can result in varying requirements for the same areas, leading people to do the wrong thing or to waste time figuring out what is required. Such duplication can arise when a new policy is added without full consideration of existing policies—such as in response to specific regulatory feedback. At one bank, for example, two policies established different requirements for third-party risk reviews, resulting in confusion among businesses and support functions. At another, distinct requirements in enterprise policies and commercial business standards related to financial crimes led to inconsistent processes across businesses.

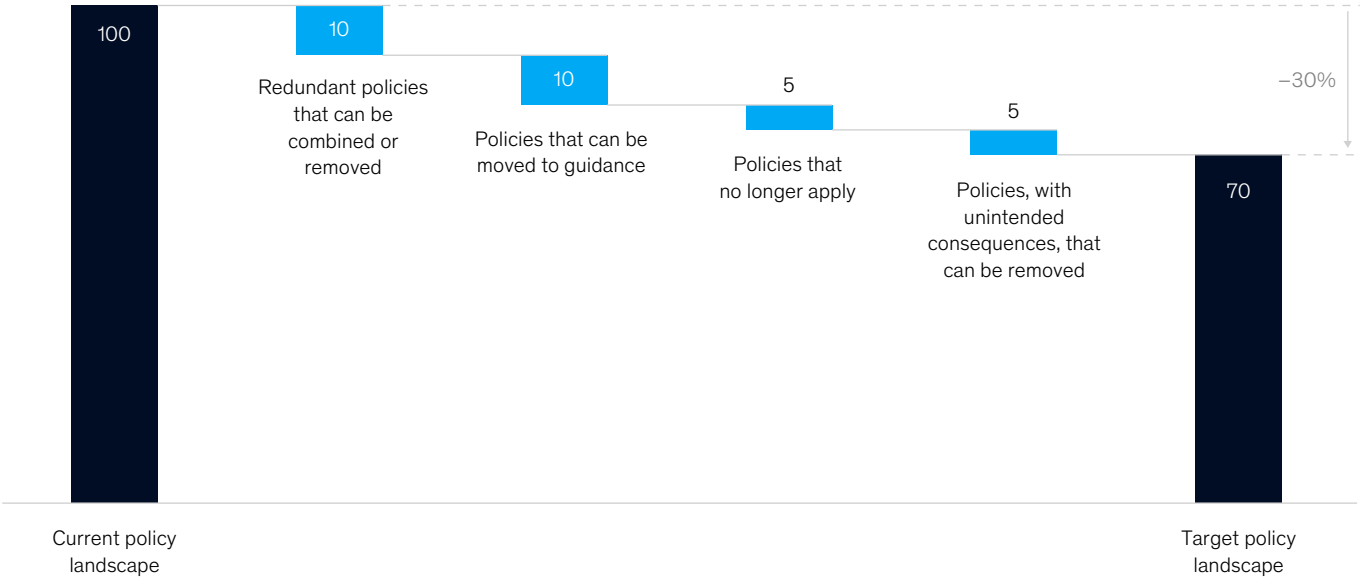
— *Focus on meaningful outcomes rather than overly prescriptive procedures.* Policies that are too prescriptive can constrain behavior in ways unnecessary for risk management

Institutions have reduced as many as 30 percent of their policies while improving the quality of the remainder.

Exhibit 3

Many institutions can reduce the number of policies dramatically.

Bank risk policies, %



and harmful from a business standpoint—for example, by blocking revenue generation or adding expensive activities. At one bank, a rigid interpretation of a policy for the credit-review process led to excessive conservatism in ratings when benchmarked against peers. By eliminating overly prescriptive policies, banks can maintain the quality of risk management without needlessly impeding the business.

— *Require only those tasks that have a clear risk-management rationale.* Policies requiring unnecessary tasks divert focus and add expense. For example, a policy at one bank required all frontline individuals who had interacted with any at-risk credit to attend monthly calls. With simple policy changes, total employee time on these calls was cut by 90 percent without compromising effective risk management.

Experience has shown that banks trying to redesign policies by relying entirely on a central policy office or other administrative unit tended to struggle to achieve their goals. A central policy office can, however, be helpful in building the full inventory of all risks and defining the target policy architecture—an architecture that is unmarred by the previously mentioned gaps and overlaps. Banks that have been successful in implementing this target state have then assembled a working group, composed of business and risk representatives, to create detailed recommendations. These are reviewed by area-level policy committees, such as a credit-policy committee and the board, if necessary. The working group should be small and include respected leaders from both the risk function and the business—success depends on contributions from the right people from the business, support functions, and risk, highlighting specific policies and pain points.

Simplifying the committee structure

Since the financial crisis, many firms have added committees, sometimes without harmonizing the roles of the new and existing committees. Institutions can have more than a hundred committees, many with unclear or overlapping mandates and suboptimal memberships. Committee overgrowth unduly

burdens the schedules of senior executives while also delaying or hampering decision making.

With fewer committees and clearer mandates and escalation paths, banks can provide full coverage of important areas, while improving transparency. A rigorous review of the committee structure can improve governance while cutting the time dedicated to committees nearly in half. Although such a committee review at a large bank can take four to six months, institutions can begin by developing a set of design principles and using them to understand the existing challenges. The following five central ideas can help guide this work:

— *Build a dedicated holistic committee structure covering all risks and businesses.* Gaps in domains covered by committees are most common in areas requiring a holistic, enterprise view spanning risk types, businesses, and enterprise functions. Some institutions, for instance, have found that they do not have sufficient senior-level committee discussion focused on reputational risk, geopolitical risk, or major regulatory risks.

— *Charge committees with clear and distinct mandates.* Committees with ambiguous or overlapping mandates may make inconsistent or conflicting decisions. At some banks, separate committees dedicated to individual product-risk or operational risk domains sometimes arrive at conflicting decisions, frustrating business owners who must implement them. Clearly delineating decision-making mandates for these committees (and eliminating or merging committees with overlapping mandates) can prevent these challenges.

— *Ensure meaningful decision rights and clear lines of escalation in each committee.* Without clear decision-making authority and responsibility, committee meetings can become mere discussions resulting in no meaningful progress. Unclear accountabilities or lines of escalation can cause confusion in the organization about how to address important risks, issues, or decisions. For example, many institutions have not fully clarified lines of escalation or accountabilities among newly created conduct-risk committees and existing compliance or people committees.

— *Include members from outside risk.* Commonly, HR and the business are underrepresented on committees. Gaps in membership can cause committees to be too cautious or miss important risk issues. Without HR representation, for example, links to performance management, training, and employee relations might be missed. With limited business involvement, committees focused on areas such as liquidity risk can struggle to assign tailored deposit-outflow factors, sometimes leading to unnecessarily conservative buffers.

— *Limit membership and attendees.* Conversely, in attempting to make sure all voices are heard, firms can create committees with more members than necessary. This taxes schedules of senior managers while impeding effective decision making. Even where membership is limited, banks have seen attendance creep up over time, with those invited to particular meetings continuing to attend long after their presence is needed. Membership overgrowth should be addressed and reversed through intelligent committee redesign and disciplined reinforcement by committee chairs.

Challenges in the prevailing committee design can be identified in dedicated workshops with relevant stakeholders. A small, temporary working group can then remove or consolidate committees according to the design principles agreed upon and the results of the targeted discussions. The charters and membership of the remaining committees can then be redesigned. The working group should consult with senior business and functional leaders outside the risk function. The organization can begin implementing its new committee structure, to test and refine results and to demonstrate real change in action. Meaningful changes to the committee structure can act as strong signaling mechanisms that the risk organization is committed to a transformation.

Streamlining and strengthening processes

With aligned organization and governance, institutions can begin capturing significant efficiencies. Streamlined processes are less error prone, better controlled, and more conducive to enhanced customer and employee experiences. They are also more efficient. As an example, some banks that have mapped their credit-underwriting and adjudication process have discovered efficiency-improvement opportunities leading to freeing up underwriter capacity by more than 20 percent and credit-officer capacity by more than 10 percent. Even without technology changes, significant impact is often possible from simplifying the many layers of process that have been created through step-by-step additions over multiple years. At the same time, such simplification can help lay the groundwork for more effective digitization.

Opportunities lie in streamlining and strengthening core risk processes as well as processes that are not owned by the risk function but are risk prone. Risk has greater control over core risk processes, such as credit adjudication, fraud prevention, and anti–money laundering/know your customer (AML/KYC) review—and this is where risk efficiency-and-effectiveness transformations commonly begin. The risk function can also be a catalyst for improving and streamlining high-risk processes owned outside the function. For such processes, including sales-force performance management, customer onboarding, and payments processes, risk can offer clear policies and associated requirements on monitoring, controls, and testing.

Transparent processes and transparent controls enable the business to act as a more engaged first line of defense. For example, at one regional bank, a complex process for managing credit-portfolio concentrations resulted in limited engagement by the first line, which adopted an approach of asking for exceptions instead of working within process constraints. Transparent processes help focus attention on the highest-impact activities and reduce the risk that deficiencies in complex processes or controls will go unnoticed. At the same time, business leaders become better risk managers by understanding the existing controls and their intended purposes.

Since streamlining major processes is a big job, institutions would be wise to start in a targeted way, with a few prioritized use cases. This approach increases the chances of success and helps quickly demonstrate value. To prioritize use cases, banks should weigh the feasibility of streamlining and the potential gains in effectiveness and efficiency. Processes that are complex and involve many people are prime candidates for streamlining.

The following four steps are particularly relevant to ensuring and maintaining transparent, lean processes:

— *Maintain clear mapping of processes and controls.* Process mapping involves identifying the individual steps and controls in a process, understanding how the various steps relate to one another, and identifying the people and roles involved in carrying out the process. Institutions that have successfully streamlined processes usually begin by mapping existing processes and controls. The first steps involve compiling a comprehensive inventory of risk-ranked processes and developing a robust control taxonomy. It is important to perform the mapping at the right level—the level at which a detailed understanding of the process and key pain points emerges, but without so much detail that the mapping takes months, leaving little time and energy to address the pain points. It is also critical to conduct the mapping with all the control, operational, and technology use cases in mind: one well-executed mapping exercise should be able to satisfy all these needs.

— *Apply Occam's razor—the law of economy—to each process step and control to eliminate every nonessential activity.* Many banks have processes that have evolved, over time, to

incorporate activities or controls that do not improve effectiveness. One bank, for example, found that interim relationship reviews conducted by the portfolio-management function resulted in a change in credit ratings for an insignificant number of low-risk credits. The bank updated its policies to reduce the interim-review requirements. Another bank found that the final layer in its credit-adjudication process changed credit ratings less than 1 percent of the time, with most changes improving a risk rating. The bank removed this layer without affecting credit standards or ratings practices.

— *Segment based on risk.* Aligning the level of risk-management efforts to the level of risk inherent in each activity enables design of controls that balance effectiveness and efficiency. Where this principle has been ignored, there is usually a dramatic opportunity to improve both effectiveness and efficiency. For example, one regional bank redesigned its commercial-credit triaging process after discovering that it was needlessly processing lower-risk, commercial loans through a high-cost channel. The lack of visibility into middle- and back-office activities also resulted in a lengthy application-to-decision time. By redesigning the triaging process, as well as its credit memos to align the length and level of required analysis with the level of risk of the credit, the bank reduced underwriting overhead and freed capacity by 25 percent. The improved credit memos made it easier for credit officers to zero in on the most pressing areas.

— *Reduce variability, standardizing when possible.* Where possible, banks should seek to standardize processes to reduce operational risk and overhead while improving decision making. Continuing the example outlined above, along with taking an approach to segment its credit operations based on risk, the regional bank set clearer criteria for auto-declines and increased its use of straight-through processing of commercial credits. The full suite of initiatives allowed it to reduce time to decision by 60 percent and increase its pull-through rate by 15 percent (Exhibit 4). Most banks also find significant room for improvement in processes associated with operational risk and compliance and with model development and validation. For example, by standardizing customer-onboarding questions and aligning them directly with the customer risk-rating model, one institution improved its ability to flag high-risk customers while eliminating back-and-forth interactions among compliance, bankers, and customers.

Once the process has been mapped, the team will work to streamline it, eliminating extraneous activities and controls. The redesigned structure is then rolled out in small pilots and reviewed before a large-scale deployment. During these pilots, the new process and associated controls are assessed to ensure that the process is running smoothly and that the controls are operating appropriately—including that they are properly matched to risk levels and that there are no gaps in controls. Establishing clear, measurable performance objectives, with close tracking of performance, will help identify issues with the revised process.

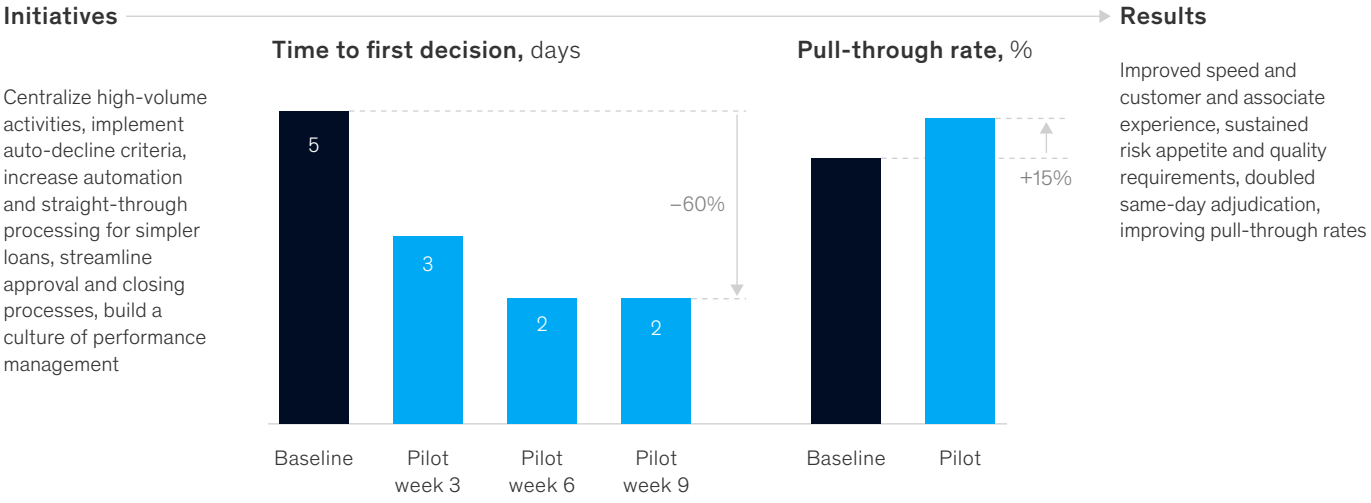
Digitization and advanced analytics

Digitization and advanced analytics augment and magnify the impact of process streamlining, unlocking potential for full risk-management effectiveness and efficiency gains. For example, by automating data capture and improving its decision engine, one bank was able to achieve straight-through processing for 70 percent of loans, reducing cost of origination by 70 percent and the time needed to make decisions to under a minute. In addition, a global bank, experiencing extremely high false-positive rates in AML monitoring, identified data errors as a root cause of the issue. To address this increasingly onerous problem, the bank developed an approach using natural-language processing to reduce the data errors, which resulted in many fewer false positives, saving tens of thousands of investigation hours.

Exhibit 4

By redesigning the commercial-credit process, an institution dramatically reduced application-to-decision times, using fewer resources.

Redesigned credit process



Digitization and advanced analytics are indeed the only viable approach for managing many types of nonfinancial risk, including cyberrisk, fraud, and third-party risk, that involve monitoring thousands or even millions of touchpoints. Such a large number of interactions cannot be monitored manually, so institutions are turning to analytics and machine learning to check for data quality, detect outliers and anomalies or identify and prioritize high-risk behavioral patterns.

The most suitable stance toward digitization and advanced analytics in risk management will depend on where a bank stands in its overall digitization journey. Digital transformations offer promise well beyond risk, and banking as a sector is undergoing a digital revolution. The level of digitization achieved varies widely across institutions, however. While some banks have begun or even completed (especially in Asia) full-scale transformation efforts, others are still considering when, where, and how to begin.

Beginning to capture benefits

Even institutions in the early stages of maturity can adopt three “no regrets” ideas to begin to capture the benefits in efficiency and effectiveness that digitization offers:

— *Define a vision for digital risk as a guide for improvements over time.* Even at banks not yet actively considering a broad digital transformation, the risk function should develop a vision for managing the risks associated with a digitized operation and ecosystem, including the activities the risk function will undertake and the corresponding role and mandate. Such a vision provides a basis for initial, perhaps piecemeal, digitization improvements. Moreover, managing the digital risks associated with efforts within the risk function should be a primary concern.

— *Adopt digital work flows within at-scale risk processes as far as possible, prioritizing high-impact efforts.* In undertaking digitization

efforts, institutions would be wise to start in a targeted manner, with a few prioritized processes. To prioritize, banks should weigh the feasibility of streamlining and the potential gains in effectiveness and efficiency. For instance, in selecting automation use cases, one risk function considered three factors to weigh the potential gains and feasibility: regulatory and business outcomes (effectiveness), the amount of resources affected (efficiency), and the automation potential (feasibility) (Exhibit 5). While priority processes to digitize will vary by institution, prime candidates tend to include processes linked to credit adjudication and monitoring, AML/KYC, and third-party risk management.

— *Use advanced analytics to full effect by piecing together existing data sources, even if they are disparate.* Most institutions have more available data than they suspect. In the absence of the broad data architecture needed for a full digital transformation, banks can identify, ingest, and use various unconnected data sources to address well-defined individual use cases. Prime potential examples include fraud analytics, complaints analysis, and conduct risk monitoring.

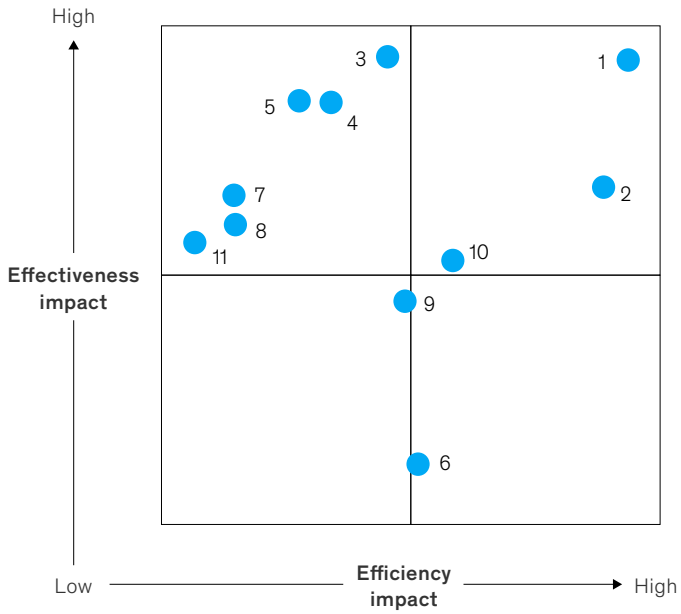
Toward a full digital transformation

The opportunity for improvement in risk management efficiency and effectiveness is significantly higher at institutions undertaking a full digital transformation. Risk can shape that transformation so that it supports risk-management effectiveness and efficiency directly—by making needed data easily accessible, for example. At the same time, digitization and advanced analytics expand the ability of the risk function to help improve processes and decision making outside of risk, beyond what processes streamlining alone can accomplish. Three key ideas can help guide CROs.

Exhibit 5

In prioritizing risk processes for automation, banks should consider feasibility as well as the impact on effectiveness and efficiency.

Risk processes, ranked by automation feasibility



Feasibility ranking

1 BSA and AML operations[1]
2 Credit review
3 Third-party risk management
4 Operational risk (nonfinancial)
5 Operational risk (implementation)
6 Product-approval support
7 Stress testing
8 Transaction testing
9 Modeling and validation
10 Consumer credit approval
11 Credit portfolio management
Credit review
Commercial/corporate credit approval
Privileged account management
Risk-appetite setting and monitoring
Risk reporting
Risk identification
Policy setting
Risk technology and systems management

High
Low

[1] BSA refers to the Banking Secrecy Act; AML refers to anti–money laundering.

— *Sign on early as a champion and participant in the bank's overall digital transformation.* As an early partisan of the digital transformation, the CRO will be able to help design and deploy automated preventive or detective controls as integral parts of the digital flows. Automated controls are the key to significant cost reductions in operational risk and compliance while providing the right real-time transparency to all lines of defense. In addition, participation in the overall digital transformation will better inform the CRO about the risks that enterprise-wide digitization brings and better able to mitigate them. On the other hand, a lack of coordination between the risk function and the digital transformation can magnify risks. At one bank, critical vulnerabilities were introduced into production code in a transition to agile software development. The effort had outrun the cybersecurity control function and led to breaches and loss of customer data. To repair the damage and prevent future breaches, the bank's operational risk team worked with cybersecurity and business-continuity experts. Together they created and implemented effective controls in the development process so that the efficiency of the agile team would not be impaired.

— *Actively define data requirements across all key risk use cases for integration into the broader enterprise data transformation.* This effort should look at use cases with a multiyear time horizon. It should include all nontraditional data sources that may be needed for more advanced modeling, together with all required attributes such as quality and latency. Enterprise data transformations typically set both "defensive" aims (control) and "offensive" aims (business enablement). While ideally these should be pursued in tandem, many institutions have begun on the control side—with risk, compliance, and finance. An appropriately comprehensive and forward-looking vision of the risk data requirements is not only critical to risk but can provide the template for other control functions. The view of risk data requirements can also serve as a basis for engaging the businesses on defining their own requirements, leading to a comprehensive and unified view of the target state.

— *Enable a bankwide artificial-intelligence (AI) transformation.* Risk can be an early adopter of AI techniques and put in place the right safeguards for bankwide AI development, enhancing effectiveness and efficiency in both ways. AI can directly enhance the efficiency of risk-specific processes—as demonstrated in the previous example of AML monitoring—and also improve controls in broader enterprise-wide processes involving thousands or millions of touchpoints. At the same time, bankwide AI efforts can only reach scale and produce their full effectiveness and efficiency benefits if a very robust framework is in place to manage the considerable associated ethical, regulatory, and operational risks. This requires guidelines, processes and governance, from the early decision to pursue an AI solution to problems to the appropriate validation of resulting AI models.

Digitization and advanced analytics are the final steps in capturing the full impact of a risk transformation. Together they augment and magnify the impact of process redesign, which was enabled by rationalized governance and improved organization. It can be argued that over time, the largest share of cost savings in a risk function will come from this last step.

Establishing a successful transformation program

While some banks have focused risk improvement in one or two particular areas, experience demonstrates that the greatest gains belong to institutions that

carefully sequence efforts across organization, governance, processes, and digitization and analytics. Such end-to-end risk transformations can reduce the cost base by 15 to 20 percent while meaningfully improving the quality of risk management.

Four initial steps are essential to success.

1. *Define the scope of transformation.* Banks seeking to improve productivity face a choice of risk-focused transformation or broader cross-enterprise transformation in which the risk function is a component. Given the cross-enterprise nature of the risk function, an enterprise-wide approach tends to create greater value, both throughout the enterprise and within the risk function.
2. *Set the ambition.* At this point, banks determine the size of the available opportunity. Only after identifying the full potential of the transformation should institutions proceed to a detailed plan, with the risk-function leadership ensuring that the plan is designed to capture the full potential. Some leaders may shy away from ambitious goals, wanting instead to make more incremental changes. The trade-offs will need to be understood and discussed among the executive team beforehand, to ensure alignment.
3. *Establish proper governance and focus.* The potential value in the transformation will be realized only through strict governance with clearly defined roles. In our experience, success in risk-function transformations hinges upon appointing a transformation officer who has responsibility for drawing together the threads of the transformation and keeping things moving. This person must have a strategic rather than project-management mandate and be sufficiently senior to influence both business heads and direct reports to the CRO. Next, initiative owners will be responsible for designing each initiative, including the financial case, implementation timeline and resourcing, and impact on risk effectiveness. Finally, critically important aspects of the transformation are proper executive focus, the removal of roadblocks, and the maintenance of organizational discipline. A common feature of successful efforts is a weekly meeting, in which executives meet with the transformation officer and initiative owners to understand the recent progress, remove potential obstructions, and help ensure that the transformation delivers on its agreed-upon ambition.
4. *Build the right narrative and put in place the right communication.* These efforts are no different than any other change effort. Managing organizational buy-in, energy, and momentum is as important as the substance of the work and requires as much, if not more, senior-leadership attention.

Transformations involve significant behavioral shifts. Addressing new demands and building new skills requires careful change management and patient leadership sustained over a multiyear time horizon. Successfully transformed organizations know, however, that the rewards—greater risk-management effectiveness at lower cost—are well worth the challenge.

Oliver Bevan is an associate partner in McKinsey's Chicago office; **Matthew Freiman** is a partner in the Toronto office; **Kanika Pasricha** is a consultant in the New York office, where **Hamid Samandari** is a senior partner; and **Olivia White** is a partner in the San Francisco office.

The authors wish to thank Grace Liou, Peter Noteboom, Luca Pancaldi, Ishanaa Rambachan, and Kayvaun Rowshankish for their contributions to this article.