

McKinsey  
& Company



# McKinsey on Risk

Transforming risk efficiency  
and effectiveness

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

This issue is available online at [McKinsey.com](https://www.mckinsey.com). Comments and requests for copies or for permissions to republish an article can be sent via email to [McKinsey\\_Risk@McKinsey.com](mailto:McKinsey_Risk@McKinsey.com)

Cover image:  
© Jorg Greuel/Getty Images

**Editorial Board:**

Kyra Blessing, Richard Bucci, Philipp Härle, Alok Kshirsagar, Maria Martinez, Luca Pancaldi, Thomas Poppensieker, Kate Robu, Roger Rudisuli, Kayvaun Rowshankish, Himanshu Singh, Mark Staples, Marco Vettori, John Walsh

**External Relations, Global Risk Practice:** Kyra Blessing

**Editor:** Richard Bucci

**Contributing Editors:**  
Laura DeLallo, Joanne Mason, Steve Sakson, Allen Webb

**Art Direction and Design:**

Nicole Esquerre,  
Leff Communications

**Data Visualization:**

Richard Johnson,  
Jonathon Rivait

**Managing Editors:**

Heather Byer, Venetia Simcock

**Editorial Production:**

Elizabeth Brown, Roger Draper, Gwyn Herbein, Pamela Norton, Katya Petriwsky, Charmaine Rice, John C. Sanchez, Dana Sand, Katie Turner, Sneha Vats, Pooja Yadav, Belinda Yu

**McKinsey Practice Publications**

**Editor in Chief:**

Lucia Rahilly

**Executive Editors:**

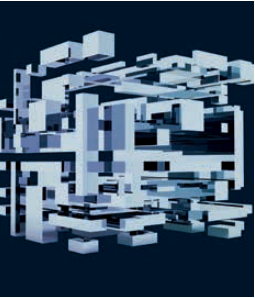
Michael T. Borruso,  
Allan Gold, Bill Javetski,  
Mark Staples

Copyright © 2019 McKinsey & Company. All rights reserved.

This publication is not intended to be used as the basis for trading in the shares of any company or for undertaking any other complex or significant financial transaction without consulting appropriate professional advisers.

No part of this publication may be copied or redistributed in any form without the prior written consent of McKinsey & Company.

# Table of contents



## 3 Transforming risk efficiency and effectiveness

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

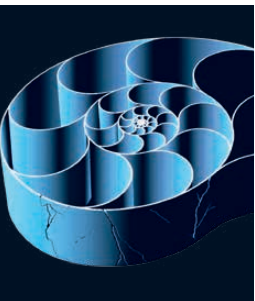
---



## 19 The compliance function at an inflection point

McKinsey's benchmarking survey of leading banks helped identify five steps toward transforming the efficiency and effectiveness of the compliance function.

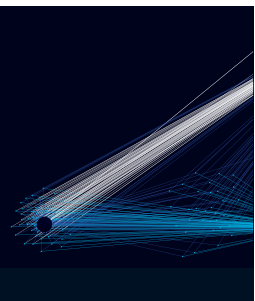
---



## 27 Confronting the risks of artificial intelligence

With great power comes great responsibility. Organizations can mitigate the risks of applying artificial intelligence and advanced analytics by embracing three principles.

---



## 35 Derisking machine learning and artificial intelligence

The added risk brought on by the complexity of machine-learning models can be mitigated by making well-targeted modifications to existing validation frameworks.

---



## 41 Going digital in collections to improve resilience against credit losses

With delinquencies on the rise, lenders need to transform their contact approaches now to suit customer preferences.

---



## 49 Bubbles pop, downturns stop

Economic downturns are both impossible to predict, and sure as sunrise. Build resistance now, because when the sun comes up, you'd better be moving.

---



## 57 Fighting back against synthetic identity fraud

Digging deep into the data trails people leave behind can help banks detect whether their customers are real or not and stem losses from this fast-growing financial crime.

---



## 63 Critical infrastructure companies and the global cybersecurity threat

How the energy, mining, and materials industries can meet the unique challenges of protecting themselves in a digital world.

---

# Introduction

We present our latest issue of *McKinsey on Risk*, the journal offering McKinsey's global perspective and strategic thinking on risk. This publication focuses on the risk areas that affect the performance of the world's leading companies, taking a truly global view across business sectors and functions. The articles offer industry insights and recount hands-on experience to highlight the strategic skills and analytical tools companies are using to transform all areas of risk management.

In this issue, the lead articles "Transforming risk efficiency and effectiveness" and "The compliance function at an inflection point" offer detailed discussions of *how financial institutions can tackle the increased operational costs that came from postcrisis expansion*. Through digital-based transformations to improve organization, governance, and processes, they can achieve better performance while sustainably trimming costs.

As financial institutions and corporates across sectors address the *strategic imperatives of digitization and artificial intelligence*, the advantages gained are accompanied by new and challenging perils. "Confronting the risks of artificial intelligence" and "Derisking machine learning and artificial intelligence" address these diverse and complex risks. From insecure data to misbehaving models, they can be mitigated with structured detection approaches, robust controls, and targeted modifications to validation frameworks.

The theme of *institutional resilience in a downturn* is rapidly gaining strategic importance. It is discussed in "Going digital in collections to improve resilience against credit losses" and "Bubbles pop, downturns stop." The latter article zeros in on what distinguished resilient companies from less resilient ones in the last downturn. The former explores the meaning of resilience in the context of lenders' credit positions and how these may be improved in advance of any future economic slowdown.

The issue concludes with "Fighting back against synthetic identity fraud" and "Critical infrastructure companies and the global cybersecurity threat," discussions of different aspects of *cyber breaches*. One delves into the unique security challenges facing critical infrastructure companies, addressing how they can fight back successfully with cybersecurity transformations to protect against crippling threats. A second piece tackles the detection and prevention struggles of synthetic identity fraud, highlighting the use of data trails to stem losses from this fast-growing financial crime.

We hope you enjoy these articles and find in them ideas worthy of application. Let us know what you think at [McKinsey\\_Risk@McKinsey.com](mailto:McKinsey_Risk@McKinsey.com) and on the McKinsey Insights app.



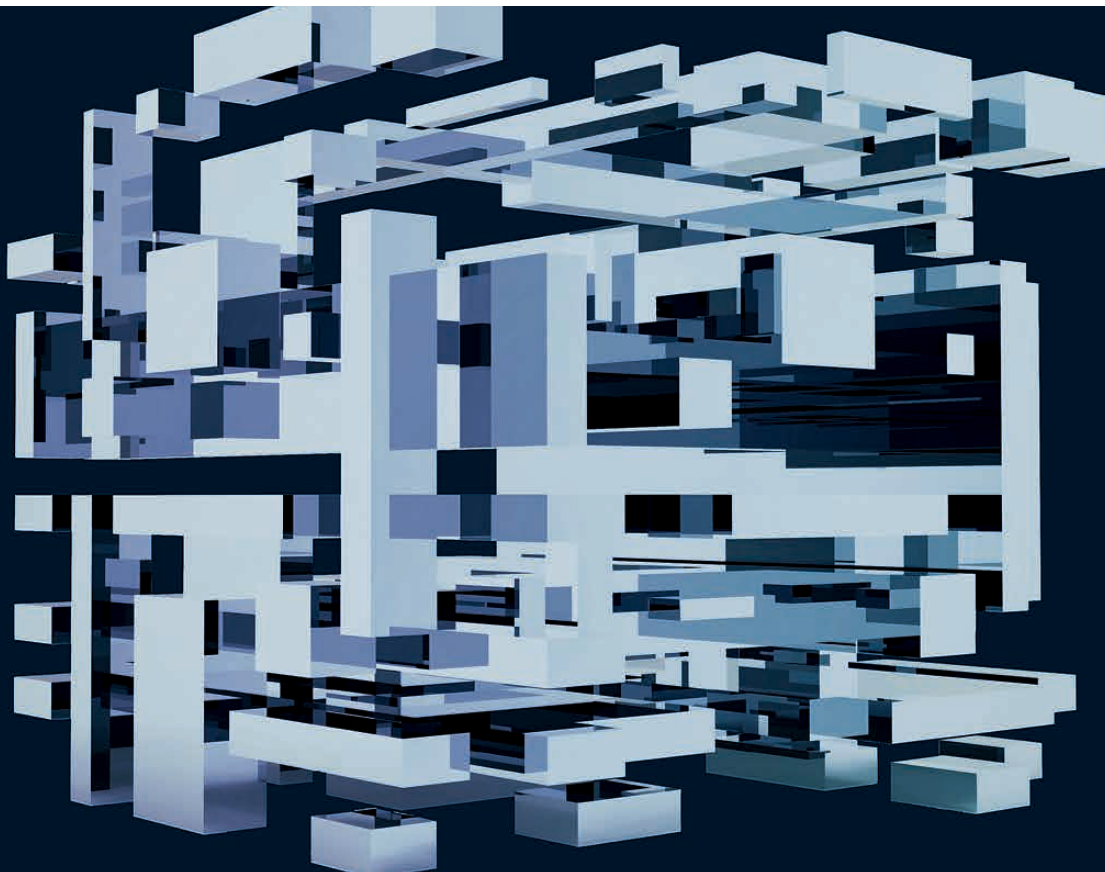
**Thomas Poppensieker**

*Chair, Global Risk Editorial Board*

# 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*



© WLADIMIR BULGAR/Getty Images

**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

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

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) 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.

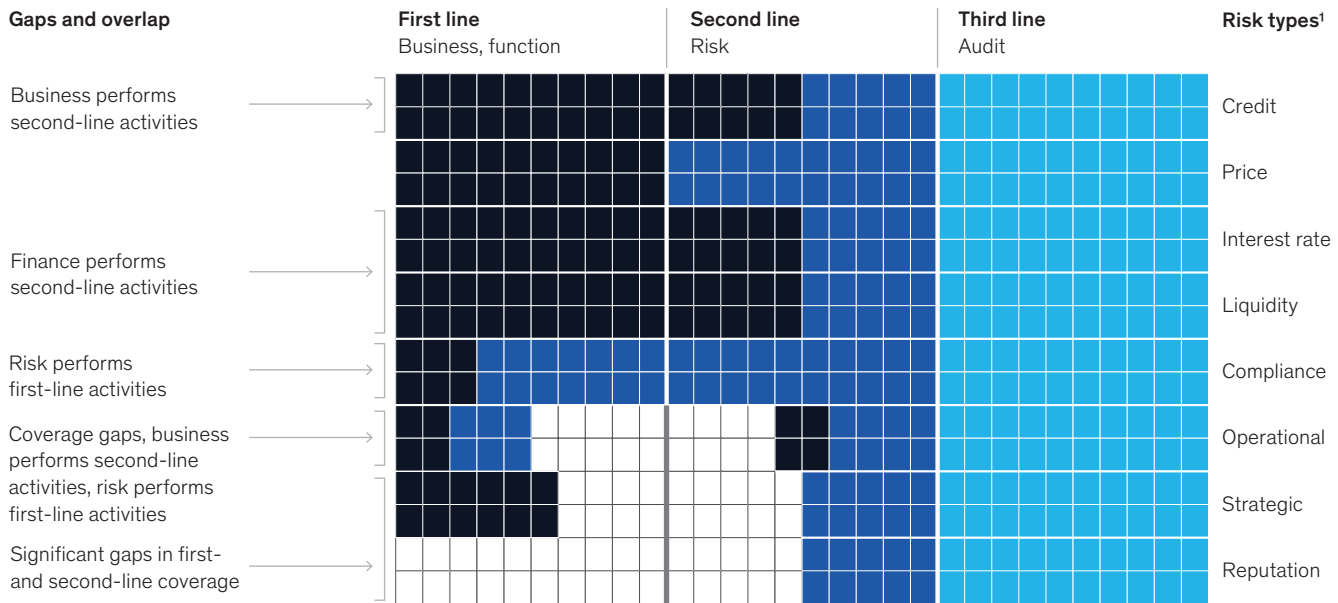
### **Clarifying roles and responsibilities across the lines of defense**

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 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.

**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**



<sup>1</sup> 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.

- *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 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.

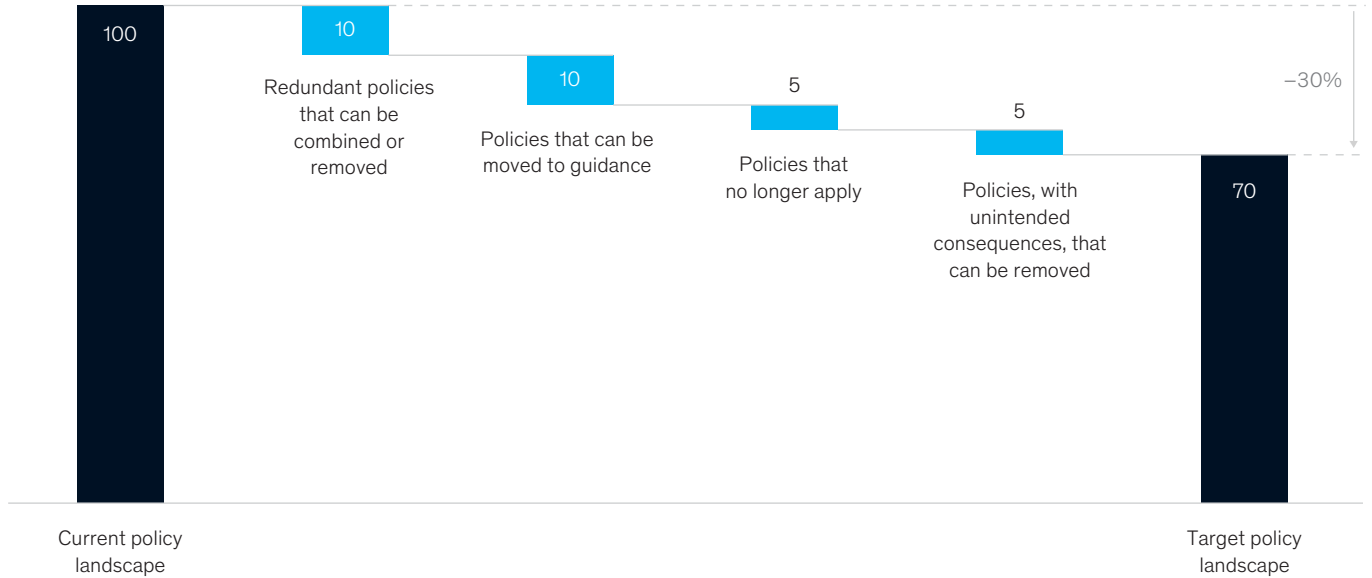
Institutions have eliminated up to 30 percent of their policies while improving the quality of the remainder (Exhibit 3). Policies can be structured to focus attention on the areas of highest risk while removing unnecessary red tape for the businesses. Meanwhile, the cost and effort of policy administration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

## Many institutions can reduce the number of policies dramatically.

Bank risk policies, %



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 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 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

Exhibit 4

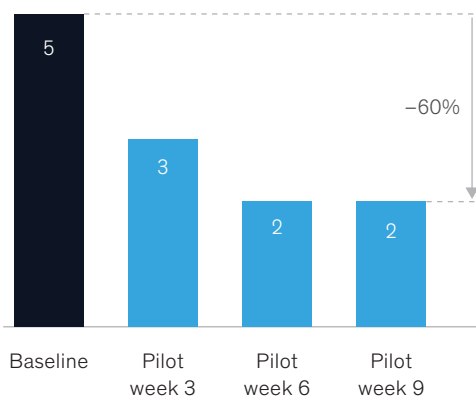
## By redesigning the commercial-credit process, an institution dramatically reduced application-to-decision times, using fewer resources.

### Redesigned credit process

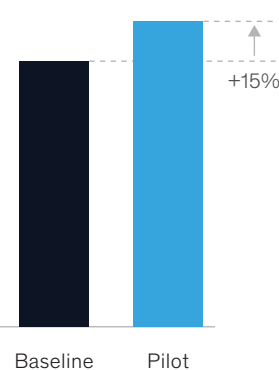
#### Initiatives

Centralize high-volume activities, implement auto-decline criteria, increase automation and straight-through processing for simpler loans, streamline approval and closing processes, build a culture of performance management

#### Time to first decision, days



#### Pull-through rate, %



#### Results

Improved speed and customer and associate experience, sustained risk appetite and quality requirements, doubled same-day adjudication, improving pull-through rates



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.

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.

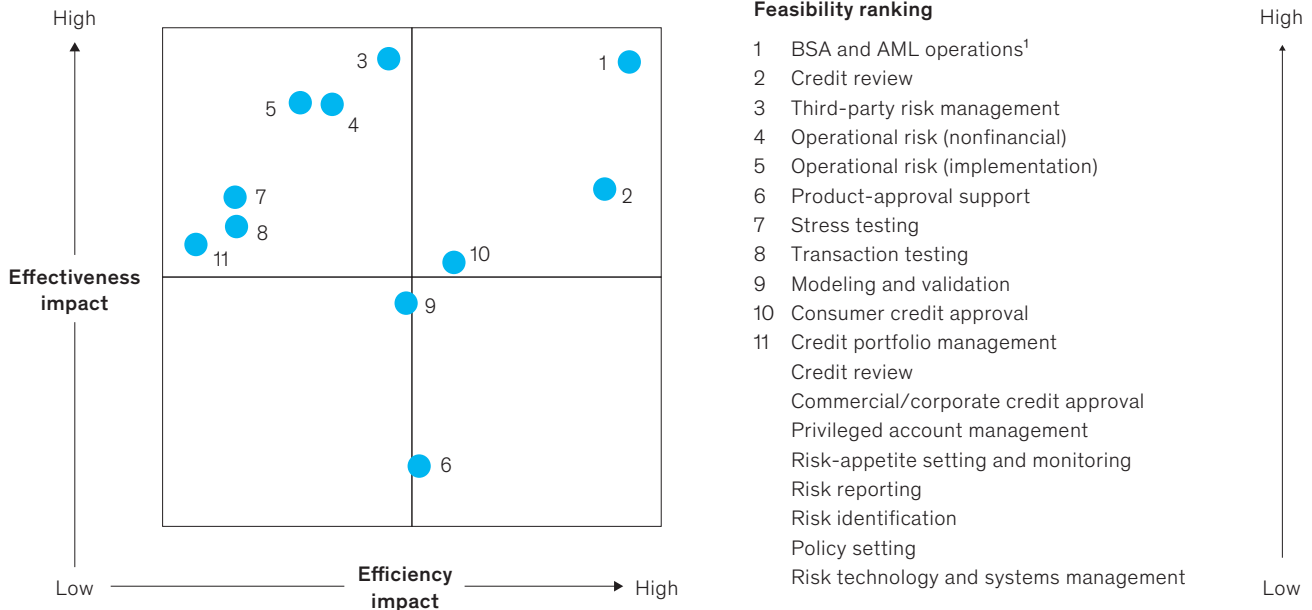
### **Beginning to capture benefits**

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,

**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



<sup>1</sup> BSA refers to the Banking Secrecy Act; AML refers to anti-money laundering.

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.

- *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, participating in the overall digital transformation will make the CRO better informed 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 AI solutions 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 from 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.

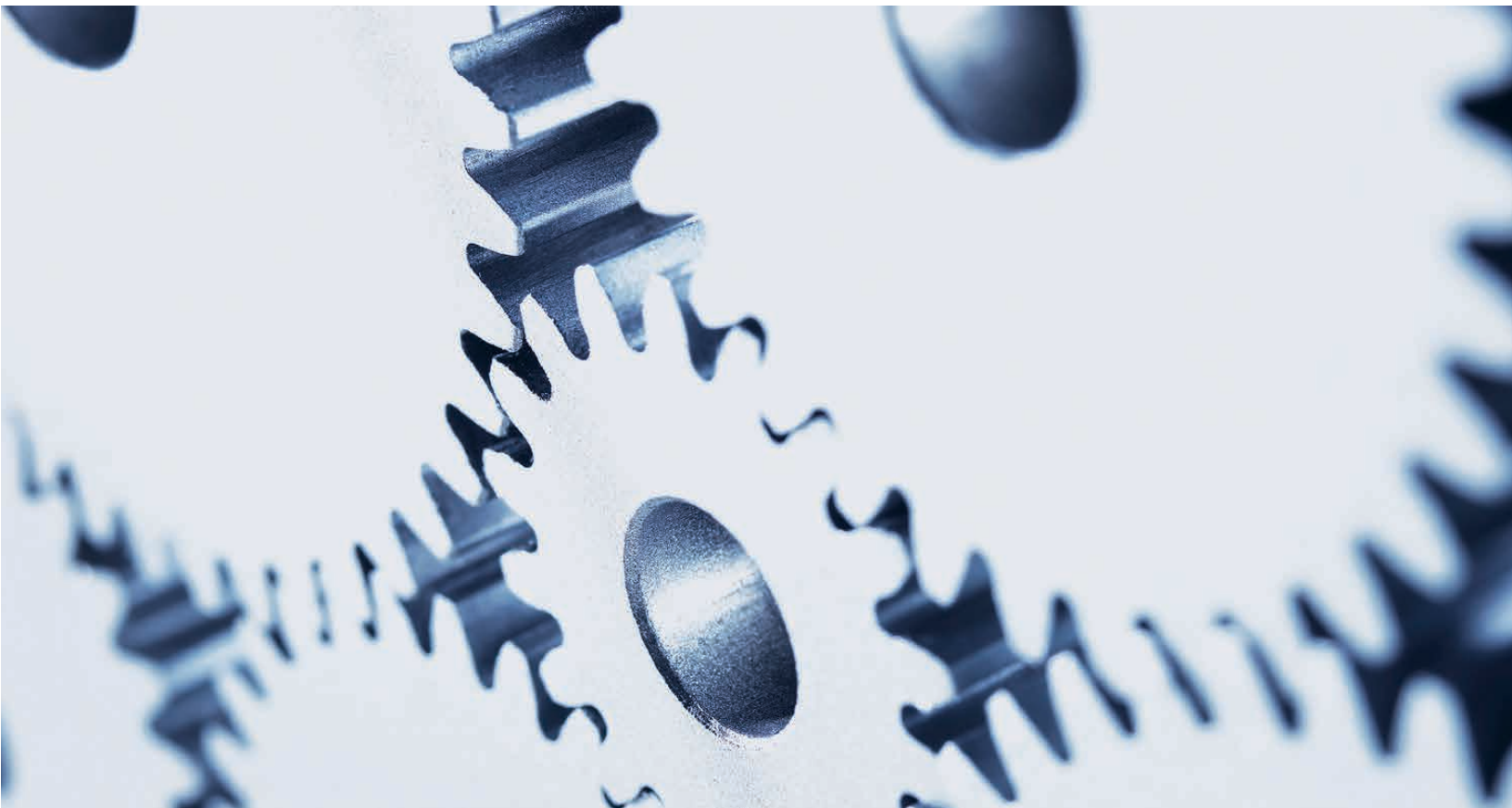
The authors wish to thank Grace Liou, Peter Noteboom, Luca Pancaldi, Ishanaa Rambachan, and Kayvaun Rowshankish for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

# The compliance function at an inflection point

McKinsey's benchmarking survey of leading banks helped identify five steps toward transforming the efficiency and effectiveness of the compliance function.

*by Oliver Bevan, Piotr Kaminski, Ida Kristensen, Thomas Poppensieker, and Azra Pravdic*



© Adam Gault/Getty Images

**The 2008 financial crisis** brought compliance into sharp focus. At financial institutions worldwide, failures related to compliance led to fines and losses topping \$300 billion in the ensuing years—damage approaching the proportions of crisis-induced credit losses. Compliance woes have not gone away since. Recent McKinsey research indicates that most senior managers feel more comfortable with their credit-risk management than with their control of compliance risk. The reason for the discomfort is the inchoate state of compliance standards. Best practices for compliance risk are still emerging, few agree on the most effective organizational approach, and business ownership of compliance risk is weak.

Institutions have heavily invested in compliance over the past ten years. Costs increased to unsustainable levels, so banks are now seeking to improve the efficiency as well as the effectiveness of their compliance departments. With standards still emerging, however, tracking developments and comparing compliance performance with peers have proved difficult.

To address this gap, McKinsey launched a compliance benchmarking effort in 2017, with 22 leading institutions from Asia, Europe, and North America participating. We updated this effort in 2018, with 24 leading institutions. Both global systemically important banks (G-SIBs) and non-G-SIBs participated. What follows is a report on our latest findings, along with insights from our discussions with executives at the banks that took part. Our aim is to provide a robust fact base for institutions exploring the potential for enhancing their compliance function.

## **Compliance-spending growth is slowing**

In response to regulatory feedback and industry-wide failures, many institutions have expanded

the mandate and size of their compliance function over the past decade. However, this growth seems to have peaked. While nearly half our sample of banks saw their costs rise by more than 20 percent during 2014–16, that share fell to one-quarter for the 2015–17 period (Exhibit 1). Three-quarters of respondents expect compliance costs either to stabilize or fall in the coming year.

Despite the cost pressures many banks face, only six responding institutions expect to reduce the size of their compliance function this year. The two banks that said their compliance costs would rise by more than 10 percent were special exceptions, as the extra spending is needed in one case for a major regulatory remediation and for building out a previously underdeveloped function in the other.

## **Size and effectiveness are not yet in balance**

The proportional size and budgets of compliance functions vary significantly from bank to bank, an indication that compliance has yet to establish a recognized, sustainable balance between size and effectiveness (Exhibit 2). McKinsey's 2018 survey revealed that the share of resources dedicated to regulatory compliance alone in an average compliance department is 0.79 percent of total full-time equivalents and 0.4 percent of total revenue.<sup>1</sup>

The banks with the largest compliance functions tend to be those under strict regulatory scrutiny, whether because of their position in the financial crisis or recent compliance failures (such as rogue-trader incidents or market abuses). The survey results also reveal that G-SIBs spend more and maintain relatively higher levels of compliance resources than other banks, likely because they too are under greater regulatory scrutiny. One conclusion we were unable to draw, however, either from the survey results or from our conversations

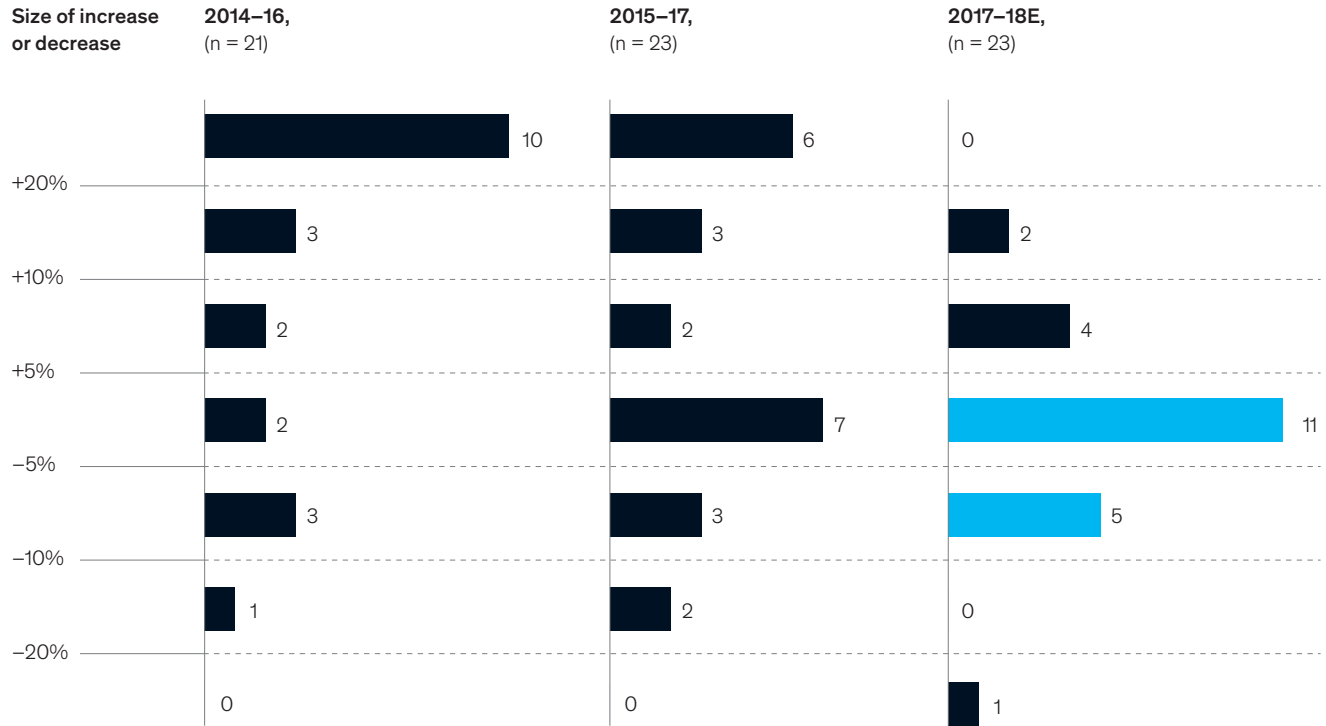
---

<sup>1</sup> That is, exclusive of financial-crimes-related compliance activities.

Exhibit 1

**In McKinsey’s 2018 compliance benchmarking survey, most banks reported compliance costs would remain at or near 2017 levels.**

**Change in compliance costs by size of increase or decrease, number of respondents**



Source: McKinsey Compliance 360 Benchmarking Survey 2018

with executives, was the correlation, if any, between size and effectiveness in compliance functions.

In conducting the survey, we observed considerable variation in the ease with which banks were able to provide the information we sought. At some banks, the information on head count and spending was readily available; at others significant resources had to be devoted to finding it. In general, the banks that had greater control of this information also performed better in the compliance maturity self-assessment described in the next section. The variations highlight the importance of professionalizing the compliance function. One step in this direction that larger

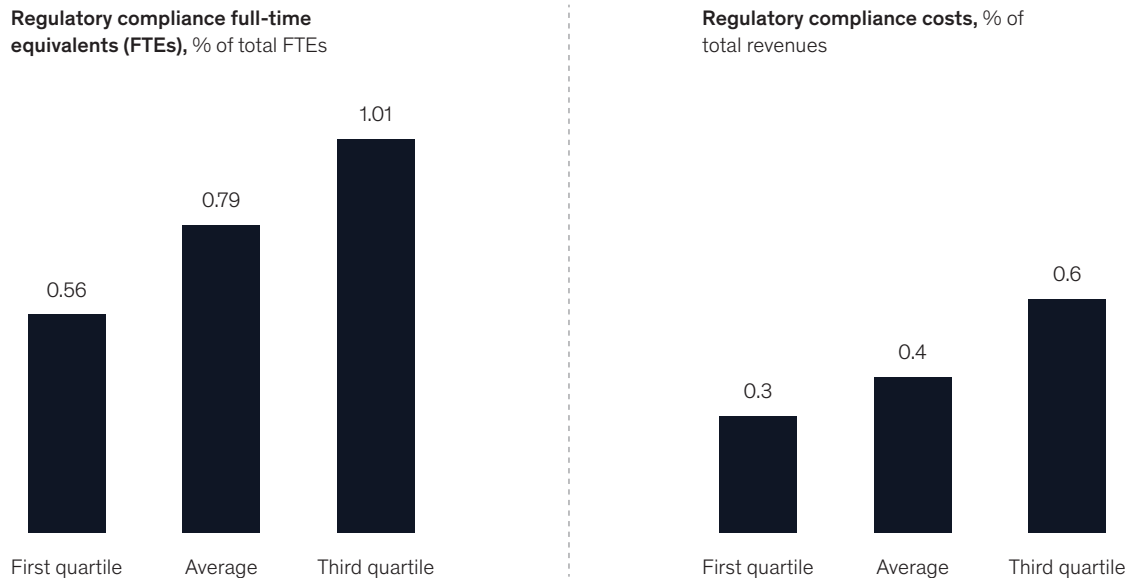
institutions could take is to appoint a chief financial officer for compliance. For smaller banks, a chief of staff responsible for managing the function’s infrastructure would be more appropriate.

**Banks assess the maturity of their compliance function**

As part of the survey, respondents were asked to assess compliance maturity in five areas: foundational capabilities, core policies and oversight, critical business and management processes, personnel, and control systems. The results are illustrated in Exhibit 3. The profile of

## The size and costs of compliance functions vary significantly among banks.

### Change in compliance costs by size of increase or decrease<sup>1</sup>



<sup>1</sup>Data compiled from 20 respondents.

Source: McKinsey Compliance 360 Benchmarking Survey 2018

compliance-function capabilities that emerged from the assessment was a varied one. Most banks scored low in areas relating to control systems, including automation, monitoring and assessment, reporting and management-information systems, and analytics. In line with these results, the executives we spoke with were keen to explore how best to use data, analytics, and technology to improve the compliance function and capture untapped potential.

Some non-G-SIBs are enhancing their more basic compliance expertise. Along with some G-SIBs, many non-G-SIBs reported challenges in integrating compliance management within their broader management of risk. Challenges include the need to build a robust risk taxonomy and control library and to integrate compliance within enterprise risk management. The chief

compliance officers (CCOs) at non-G-SIBs reported that they were struggling to strengthen core capabilities without making their compliance functions much larger. They were doubtful that following G-SIBs in significantly expanding their function's size and spending would be an appropriate approach for them.

### Automation and analytics remain a challenge

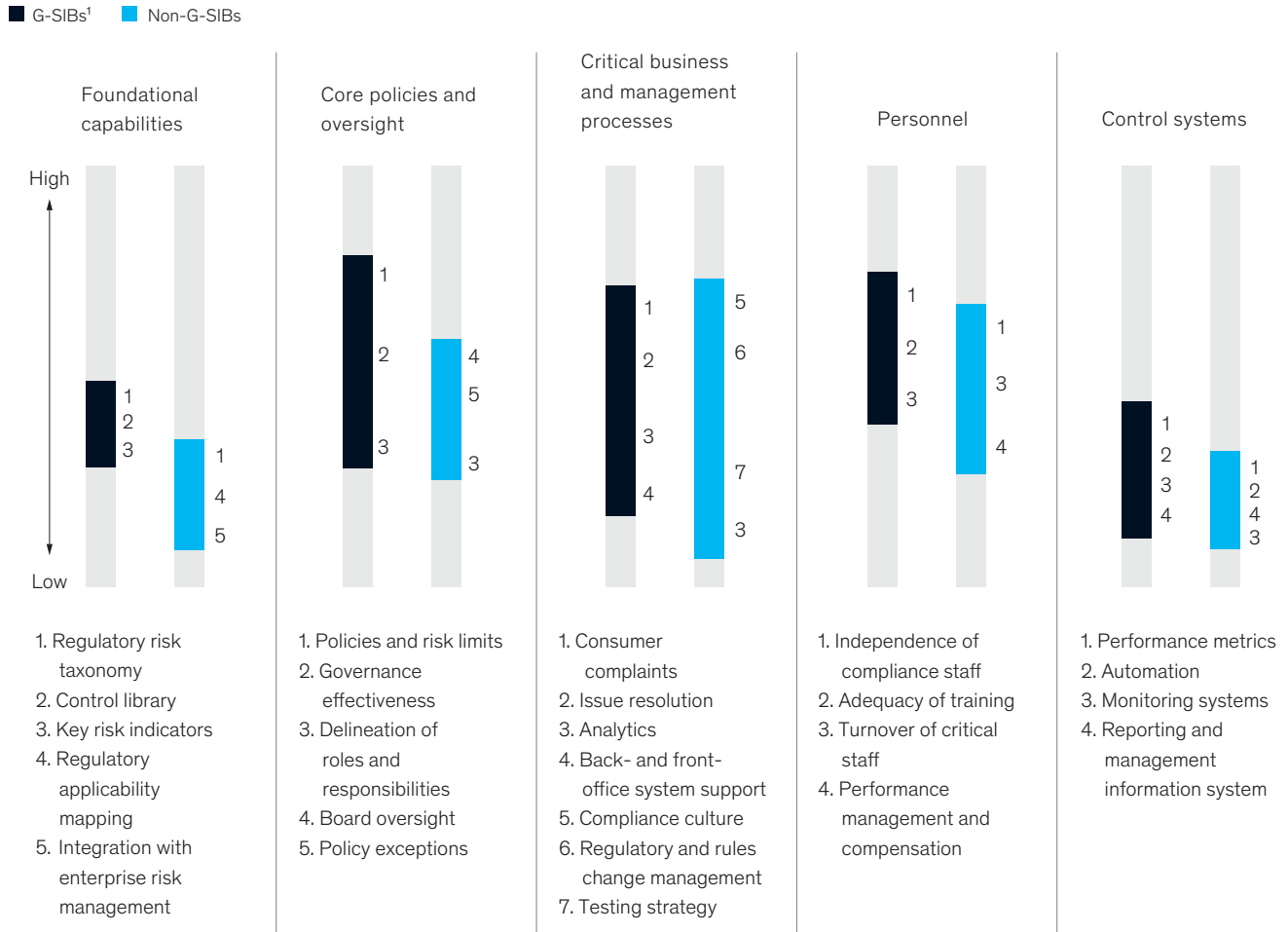
Few banks have cracked the code on applying automation and analytics effectively. Many CCOs reported a sense of frustration that much of the investment in technology was going into end-user tools that required constant attention or quickly became obsolete. The result is that resources are being drained as banks do little more than maintain the status quo.



Exhibit 3

## The maturity of compliance functions varies by category.

Compliance maturity by capability area and category



<sup>1</sup> Global systemically important banks.

Source: McKinsey Compliance 360 Benchmarking Survey 2018

Another source of frustration, according to respondents, was the absence of a technology strategy or perspective on how to drive digital change in compliance. Although CCOs were constantly approached by vendors offering technological solutions to various problems, these executives struggled to articulate what they wanted or to indicate use cases that would allow them to start unlocking value. Many had seen several proofs of concept but no real impact or scale was ever achieved.

### Spending more on technology does not guarantee maturity

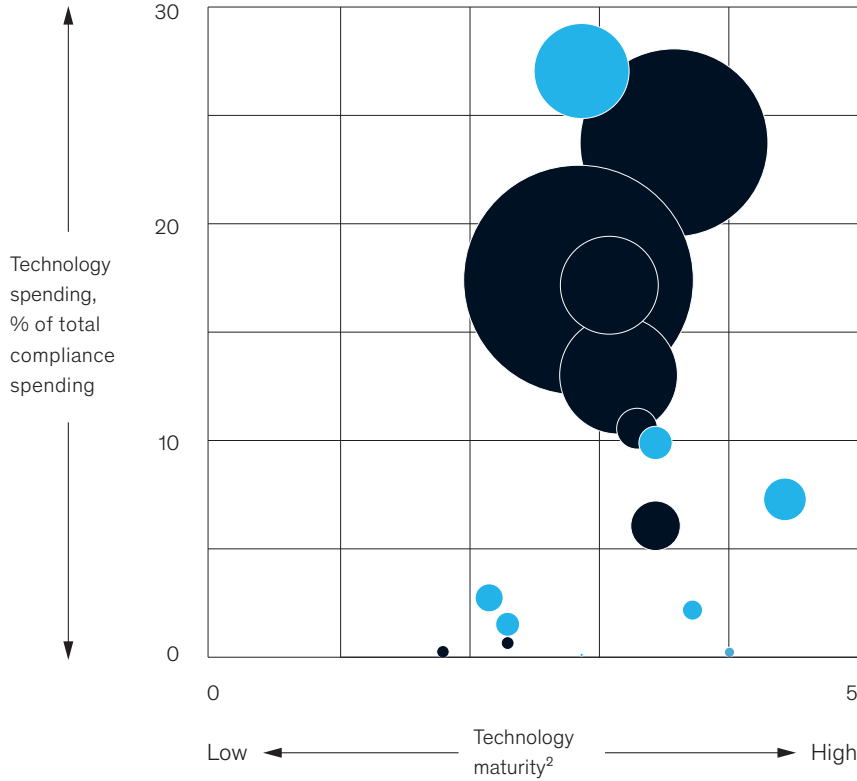
The difficulties of automation and analytics underscore a key finding from the survey: that the scale of a bank's spending on technology is not a reliable indicator of the level of maturity attained in the application of technology in compliance (Exhibit 4).

Exhibit 4

**The attainment of technological maturity in compliance is not simply a function of higher spending.**

Total spending on technology, \$ million (bubble size)

● G-SIBs<sup>1</sup> ● Non-G-SIBs



<sup>1</sup> Global systemically important banks.

<sup>2</sup> Average rating (out of 5) for control systems, analytics, and front- and back-office systems.

Source: McKinsey Compliance 360 Benchmarking Survey 2018

Some banks were spending in excess of \$50 million a year on technology to support compliance without seeing much progress in its mature application. Among the banks surveyed, the average share of technology in overall compliance costs was only 9 percent, but this share varied among individual banks, from around 1 percent to above 20 percent. The great bulk of compliance spending (79 percent) remains devoted to personnel costs (Exhibit 5).

Survey respondents are exploring the use of advanced analytics and technology in fraud

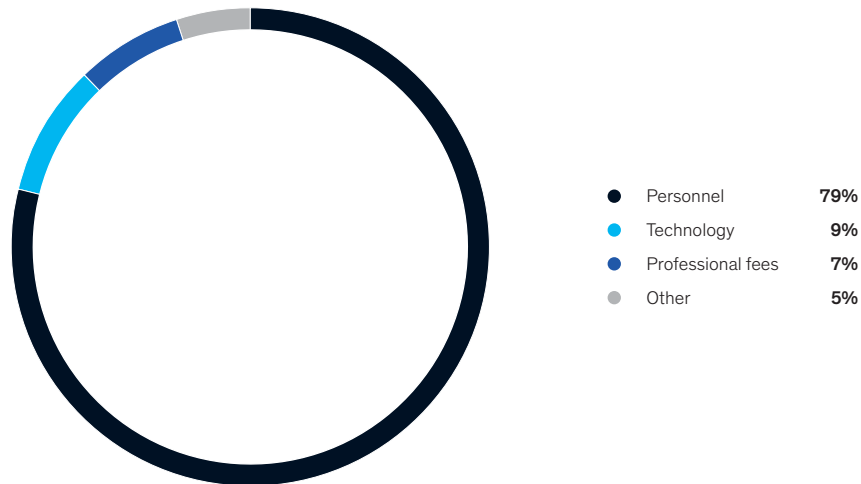
detection, transaction monitoring and screening, “know your customer” (KYC) processes, and trade surveillance. Compliance and business stakeholders are also evaluating approaches to streamlining and automating banks’ monitoring and testing processes, since these processes involve about one-fifth of compliance employees on average across our sample.

Representatives from both the first and second lines of defense reported difficulties in developing an efficient operating model for monitoring and testing, one that would ensure clear roles and

Exhibit 5

## Personnel accounts for more than three-quarters of compliance costs.

Compliance costs: industry average, % share



Source: McKinsey Compliance 360 Benchmarking Survey 2018

responsibilities, eliminate overlaps, and increase effectiveness. However, some banks reported early successes in using robotic process automation and natural-language processing to support monitoring and testing. All respondents agreed that the adoption of continuous monitoring with automated controls should reduce the need for traditional sample-based testing.

### Where next for compliance?

Our survey results and discussions with executives suggest that compliance has reached an inflection point. As regulatory pressures intensify, competition increases, and costs are squeezed, banks need to make their compliance risk management more efficient and effective. We see five actions as critical to achieving this goal.

#### 1. Getting the fundamentals right

Most survey respondents are still filling gaps in basic compliance capabilities. Needs include controls, key risk indicators (KRIs), integration with enterprise risk

management (ERM), and regulatory applicability. Many banks are now working to develop cohesive ERM frameworks and ensure the alignment of risk and control taxonomies, policies and procedures, monitoring and testing, risk assessment, and roles and responsibilities across all control functions. Some banks are integrating parts of their risk functions, such as regulatory and financial-crime compliance, as well as integrating operational and compliance risk more broadly. They are starting to adopt more forward-looking, sophisticated KRIs that support active real-time risk management. They are also exploring how to use advanced analytics in conduct risk, trade, communications surveillance, and other areas. Large banks are beginning to rationalize, automate, and streamline their controls. Better controls improve the effectiveness not only of risk mitigation but of monitoring and testing as well.

#### 2. Strengthening risk ownership in the first line

Risk management and oversight depend on the first line playing its role, but with the more recent view of compliance as a risk rather than a legal obligation,

business ownership of compliance is still lacking. The culture of compliance management needs to be strengthened in the first line through role modeling, an aspiration and tone set from the top. Banks then need to adopt formal mechanisms such as performance evaluation while ensuring that the right skills and tools are in place.

### 3. Streamlining compliance processes

Compliance requirements are often added to existing business and functional processes instead of being treated as complete end-to-end processes in their own right. This approach can lead to multiple handoffs and a lack of clarity over roles and requirements, as is often seen in KYC processes during customer onboarding. In addition, many compliance processes are highly manual or supported by outdated tools. All this means that there is ample scope to optimize compliance processes. The best method involves streamlining these processes from beginning to end across functions as a first step, and only then looking at opportunities for automation and digitization.

### 4. Adopting a dynamic technology-enabled approach to risk management

Our survey results indicate that compliance functions are in need of a technological overhaul to enhance systems and tools in management information, reporting, monitoring, and assessment. Adopting next-generation governance, risk, and control solutions is one option. Banks are already applying advanced analytics in areas such as transaction monitoring, trade and communications surveillance, and monitoring and testing. To help prevent the

proliferation of proofs of concept that will be difficult to expand to scale, banks should establish a robust process for challenging analytics and automation use cases. Only those that can be implemented practically and are likely to have the most impact should be approved. Banks can then build minimum viable products and expand to scale, taking care to map each opportunity to specific process steps and requirements. Other key success factors include a two-tier IT structure, a dedicated data lake, and a cross-functional and agile way of working.

### 5. Building compliance talent

Talent is a crucial enabler of any compliance transformation. Most banks have already begun to approach compliance with a risk-manager mind-set, eschewing earlier, more legalistic approaches. The next wave of change, already visible, is toward a data-driven and analytically enabled function. Leading banks are now beginning to set up talent academies to enhance the data-and-analytics capabilities of their employees.

---

Rising compliance demands in the wake of the financial crisis led banks to expand their compliance functions year after year. With further growth largely unsustainable, compliance is now at an inflection point. Greater efficiency and effectiveness are needed and automation and advanced analytics offer powerful methods and tools to help banks meet this need. Those institutions that move quickly will reap the rewards and help set the standard for the next-generation compliance function.

**Oliver Bevan** is an associate partner in McKinsey's Chicago office; **Piotr Kaminski** is a senior partner in the New York office, where **Ida Kristensen** is a partner; **Thomas Poppensieker** is a senior partner in the Munich office; and **Azra Pravidic** is an associate partner in the Brussels office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Confronting the risks of artificial intelligence

With great power comes great responsibility. Organizations can mitigate the risks of applying artificial intelligence and advanced analytics by embracing three principles.

*by Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari*

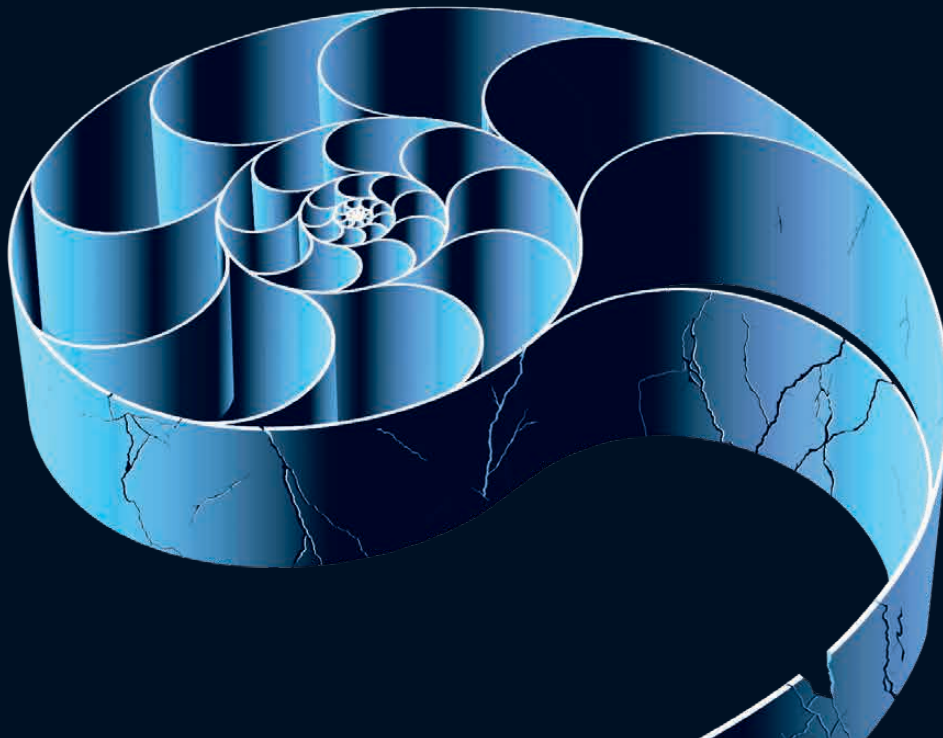


Illustration by Daniel Hertzberg

**Artificial intelligence (AI)** is proving to be a double-edged sword. While this can be said of most new technologies, both sides of the AI blade are far sharper, and neither is well understood.

Consider first the positive. These technologies are starting to improve our lives in myriad ways, from simplifying our shopping to enhancing our healthcare experiences. Their value to businesses has also become undeniable: nearly 80 percent of executives at companies that are deploying AI recently told us that they're already seeing moderate value from it. Although the widespread use of AI in business is still in its infancy and questions remain open about the pace of progress, as well as the possibility of achieving the holy grail of "general intelligence," the potential is enormous. McKinsey Global Institute research suggests that by 2030, AI could deliver additional global economic output of \$13 trillion per year.<sup>1</sup>

Yet even as AI generates consumer benefits and business value, it is also giving rise to a host of unwanted, and sometimes serious, consequences. And while we're focusing on AI in this article, these knock-on effects (and the ways to prevent or mitigate them) apply equally to all advanced analytics. The most visible ones, which include privacy violations, discrimination, accidents, and manipulation of political systems, are more than enough to prompt caution. More concerning still are the consequences not yet known or experienced. Disastrous repercussions—including the loss of human life, if an AI medical algorithm goes wrong, or the compromise of national security, if an adversary feeds disinformation to a military AI system—are possible, and so are significant challenges for organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust.

Because AI is a relatively new force in business, few leaders have had the opportunity to hone

their intuition about the full scope of societal, organizational, and individual risks, or to develop a working knowledge of their associated drivers, which range from the data fed into AI systems to the operation of algorithmic models and the interactions between humans and machines. As a result, executives often overlook potential perils ("We're not using AI in anything that could 'blow up,' like self-driving cars") or overestimate an organization's risk-mitigation capabilities ("We've been doing analytics for a long time, so we already have the right controls in place, and our practices are in line with those of our industry peers"). It's also common for leaders to lump in AI risks with others owned by specialists in the IT and analytics organizations ("I trust my technical team; they're doing everything possible to protect our customers and our company").

Leaders hoping to avoid, or at least mitigate, unintended consequences need both to build their pattern-recognition skills with respect to AI risks and to engage the entire organization so that it is ready to embrace the power and the responsibility associated with AI. The level of effort required to identify and control for all key risks dramatically exceeds prevailing norms in most organizations. Making real progress demands a multidisciplinary approach involving leaders in the C-suite and across the company; experts in areas ranging from legal and risk to IT, security, and analytics; and managers who can ensure vigilance at the front lines.

This article seeks to help by first illustrating a range of easy-to-overlook pitfalls. It then presents frameworks that will assist leaders in identifying their greatest risks and implementing the breadth and depth of nuanced controls required to sidestep them. Finally, it provides an early glimpse of some real-world efforts that are currently under way to tackle AI risks through the application of these approaches.

---

<sup>1</sup> See "Notes from the AI frontier: Modeling the impact of AI on the world economy," McKinsey Global Institute, September 2018, McKinsey.com.

Before continuing, we want to underscore that our focus here is on first-order consequences that arise directly from the development of AI solutions, from their inadvertent or intentional misapplication, or from the mishandling of the data inputs that fuel them. There are other important consequences, among which is the much-discussed potential for widespread job losses in some industries due to AI-driven workplace automation. There also are second-order effects, such as the atrophy of skills (for example, the diagnostic skills of medical professionals) as AI systems grow in importance. These consequences will continue receiving attention as they grow in perceived importance but are beyond our scope here.

### Understanding the risks and their drivers

When something goes wrong with AI, and the root cause of the problem comes to light, there is often a great deal of head shaking. With the benefit of hindsight, it seems unimaginable that no one saw it coming. But if you take a poll of well-placed executives about the *next* AI risk likely to appear, you're unlikely to get any sort of a consensus.

Leaders hoping to shift their posture from hindsight to foresight need to better understand the types of risks they are taking on, their interdependencies, and their underlying causes. To help build that

missing intuition, we describe below five pain points that can give rise to AI risks. The first three—data difficulties, technology troubles, and security snags—are related to what might be termed enablers of AI. The final two are linked with the algorithms and human-machine interactions that are central to the operation of the AI itself. Clearly, we are still in the early days of understanding what lies behind the risks we are taking on, whose nature and range we've also sought to catalog in Exhibit 1.

#### Data difficulties

Ingesting, sorting, linking, and properly using data have become increasingly difficult as the amount of unstructured data being ingested from sources such as the web, social media, mobile devices, sensors, and the Internet of Things has increased. As a result, it's easy to fall prey to pitfalls such as inadvertently using or revealing sensitive information hidden among anonymized data. For example, while a patient's name might be redacted from one section of a medical record that is used by an AI system, it could be present in the doctor's notes section of the record. Such considerations are important for leaders to be aware of as they work to stay in line with privacy rules, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), and otherwise manage reputational risk.

Exhibit 1

## Artificial intelligence and advanced analytics offer a host of benefits but can also give rise to a variety of harmful, unintended consequences.

Who could be affected and what's at risk

Individuals	Organizations	Society
Physical safety Privacy and reputation Digital safety Financial health Equity and fair treatment	Financial performance Nonfinancial performance Legal and compliance Reputational integrity	National security Economic stability Political stability Infrastructure integrity

### Technology troubles

Technology and process issues across the entire operating landscape can negatively affect the performance of AI systems. For example, one major financial institution ran into trouble after its compliance software failed to spot trading issues because the data feeds no longer included all customer trades.

### Security snags

Another emerging issue is the potential for fraudsters to exploit seemingly nonsensitive marketing, health, and financial data that companies collect to fuel AI systems. If security precautions are insufficient, it's possible to stitch these threads together to create false identities. Although target companies (that may otherwise be highly effective at safeguarding personally identifiable information) are unwitting accomplices, they still could experience consumer backlash and regulatory repercussions.

### Models misbehaving

AI models themselves can create problems when they deliver biased results (which can happen, for example, if a population is underrepresented in the data used to train the model), become unstable, or yield conclusions for which there is no actionable recourse for those affected by its decisions (such as someone denied a loan with no knowledge of what they could do to reverse the decision). Consider, for example, the potential for AI models to discriminate unintentionally against protected classes and other groups by weaving together zip code and income data to create targeted offerings. Harder to spot are instances when AI models are lurking in software-as-a-service (SaaS) offerings. When vendors introduce new, intelligent features—often with little fanfare—they are also introducing models that could interact with data in the user's system to create unexpected risks, including giving rise to hidden vulnerabilities that hackers might exploit. The implication is that leaders who believe they are in the clear if their organization has not purchased or built AI systems, or is only experimenting with their deployment, could well be mistaken.

### Interaction issues

The interface between people and machines is another key risk area. Among the most visible are challenges in automated transportation, manufacturing, and infrastructure systems. Accidents and injuries are possible if operators of heavy equipment, vehicles, or other machinery don't recognize when systems should be overruled or are slow to override them because the operator's attention is elsewhere—a distinct possibility in applications such as self-driving cars. Conversely, human judgment can also prove faulty in overriding system results. Behind the scenes, in the data-analytics organization, scripting errors, lapses in data management, and misjudgments in model-training data can easily compromise fairness, privacy, security, and compliance. Frontline personnel also can unintentionally contribute, as when a sales force more adept at selling to certain demographics inadvertently trains an AI-driven sales tool to exclude certain segments of customers. And these are just the *unintended* consequences. Without rigorous safeguards, disgruntled employees or external foes may be able to corrupt algorithms or use an AI application to engage in malfeasance.

## AI risk management: Three core principles

In addition to providing a flavor of the challenges ahead, the examples and categorization above are useful for identifying and prioritizing risks and their root causes. If you understand where risks may be lurking, ill understood, or simply unidentified, you have a better chance of catching them before they catch up with you.

But you'll need a concentrated, enterprise-wide effort to move from cataloging risks to rooting them out. The experiences of two leading banks help illustrate the clarity, breadth, and nuanced rigor that's needed. The first, a European player, has been working to apply advanced-analytics and AI capabilities to call-center optimization, mortgage decision making, relationship management, and treasury-management initiatives. The second is a global leader, seeking to apply a machine-learning model to its customer-credit decisions.

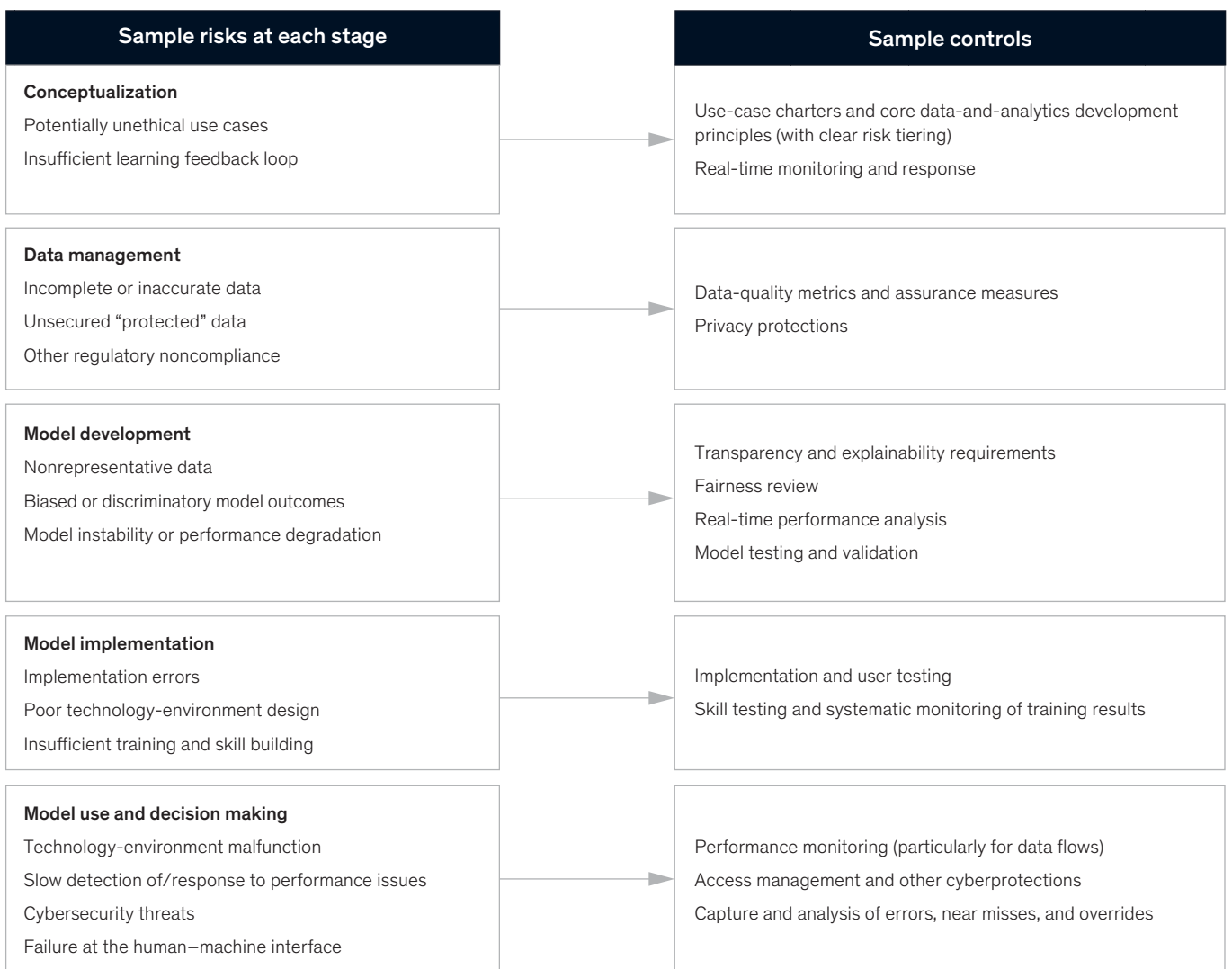


These banks, like many others in the financial-services sector, have been applying some form of advanced analytics for a number of years, dating back to their early use in credit-card fraud detection and equity trading. They also are subject to a high degree of regulatory oversight and therefore have long been applying and making transparent a wide range of protocols and controls for mitigating the related risks—including cybersecurity risk, where they are frequently on the front lines given the obvious attractiveness of their assets to attackers.

Nonetheless, these banks' stories illustrate only a subset of the risk-specific controls organizations should be considering. Exhibit 2 presents a more complete list of potential controls, spanning the entire analytics process, from planning to development to subsequent use and monitoring. Our hope is that taken together, the tool and examples will help leaders who must confront a wide range of issues—from avoiding bias in recommendation engines to eliminating personal-identity risk to better tailoring the responses of customer-service bots to the needs of specific customers, and many more beyond.

Exhibit 2

**Artificial-intelligence risks can crop up at any stage of development, but controls can help mitigate them.**



**Clarity: Use a structured identification approach to pinpoint the most critical risks**

The European bank's COO started by assembling leaders from business, IT, security, and risk management to evaluate and prioritize its greatest risks. Inputs to this exercise included a clear-eyed look at the company's existing risks and how they might be exacerbated by AI-driven analytics efforts under consideration, and at new risks that AI enablers, or the AI itself, could create. Some were obvious, but others less so. One that unexpectedly neared the top of the list was the delivery of poor or biased product recommendations to consumers. Such flawed recommendations could result in a significant amount of harm and damage, including consumer losses, backlash, and regulatory fines.

What the bank's leaders achieved through this structured risk-identification process was clarity about the most worrisome scenarios, which allowed them to prioritize the risks encompassed, to recognize controls that were missing, and to marshal time and resources accordingly. Those scenarios and prioritized risks will naturally vary by industry and company. A food manufacturer might prioritize contaminated-product scenarios. A software developer might be particularly concerned about disclosure of software code. A healthcare organization might focus on issues such as patient misdiagnosis or inadvertently causing harm to patients. Getting a diverse cross-section of managers focused on pinpointing and tiering problematic scenarios is a good way both to stimulate creative energy and to reduce the risk that narrow specialists or blinkered thinking will miss major vulnerabilities. Organizations need not start from scratch with this effort: over the past few years, risk identification has become a well-developed art, and it can be directly deployed in the context of AI.

**Breadth: Institute robust enterprise-wide controls**

Sharpening the organization's thinking about show-stopping risks is only a start. Also crucial is the application of company-wide controls to guide

the development and use of AI systems, ensure proper oversight, and put into place strong policies, procedures, worker training, and contingency plans. Without broad-based efforts, the odds rise that risk factors such as those described previously will fall through the cracks.

Concerned with the potential risk from poor or biased product recommendations, the European bank began adopting a robust set of business principles aimed at detailing how and where machines could be used to make decisions affecting a customer's financial health. Managers identified situations where a human being (for example, a relationship manager or loan officer) needed to be "in the loop" before a recommendation would be delivered to the customer. These workers would provide a safety net for identifying if a customer had special circumstances, such as the death of a family member or financial difficulties, that might make a recommendation ill timed or inappropriate.

The bank's oversight committee also conducted a gap analysis, identifying areas in the bank's existing risk-management framework that needed to be deepened, redefined, or extended. Thorough and consistent governance at the bank now ensures proper definition of policies and procedures, specific controls for AI models, core principles (supported by tools) to guide model development, segregation of duties, and adequate oversight. For example, model-development tools ensure that data scientists consistently log model code, training data, and parameters chosen throughout the development life cycle. Also adopted were standard libraries for explainability, model-performance reporting, and monitoring of data and models in production. This governance framework is proving invaluable both for in-house AI-development efforts and for evaluating and monitoring third-party AI tools such as an SaaS fraud model the bank had adopted.

In addition, bank policies now require all stakeholders, including the sponsoring business executives, to conduct scenario planning and create a fallback plan in case AI model

performance drifts, data inputs shift unexpectedly, or sudden changes, such as a natural disaster, occur in the external environment. These fallback plans are included in the bank's regular risk-review process, giving the board's risk committee visibility into the steps being taken to mitigate analytics-driven and AI-related risks.

Worker training and awareness are also prominent in the bank's risk-mitigation efforts. All affected employees receive comprehensive communications about where AI is being used; the steps the bank is taking to ensure fair and accurate decisions and to protect customer data; and how the bank's governance framework, automated technology, and development tools work together. Additionally, business sponsors, risk teams, and analytics staff receive targeted training on their role in identifying and minimizing risks. For instance, business sponsors are learning to request explanations on model behavior, which they are using to provide feedback on business assumptions behind the model. Meanwhile, the risk team has been trained on how to better identify and mitigate legal and regulatory-compliance issues, such as potential discrimination against protected groups or compliance with GDPR.

Monitoring AI-driven analytics is an ongoing effort, rather than a one-and-done activity. As such, the bank's oversight groups, including the board's risk committees, regularly review the program to stay on top of new risks that might have emerged as a result of regulatory changes, industry shifts, legal interpretations (such as emerging GDPR case law), evolving consumer expectations, and rapidly changing technology.

**Nuance: Reinforce specific controls depending on the nature of the risk**

Important as enterprise-wide controls are, they are rarely sufficient to counteract every possible risk. Another level of rigor and nuance is often needed, and the requisite controls will depend on

factors such as the complexity of the algorithms, their data requirements, the nature of human-to-machine (or machine-to-machine) interaction, the potential for exploitation by bad actors, and the extent to which AI is embedded into a business process. Conceptual controls, starting with a use-case charter, sometimes are necessary. So are specific data and analytics controls, including transparency requirements, as well as controls for feedback and monitoring, such as performance analysis to detect degradation or bias.

Our second example sheds valuable light on the application of nuanced controls. This institution wanted visibility into how, exactly, a machine-learning model was making decisions for a particular customer-facing process. After carefully considering transparency requirements, the institution decided to mitigate risk by limiting the types of machine-learning algorithms it used. Disallowing certain model forms that were overly complex and opaque enabled the institution to strike a balance with which it was comfortable. Some predictive power was lost, which had economic costs. But the transparency of the models that were used gave staff higher confidence in the decisions they made. The simpler models also made it easier to check both the data and the models themselves for biases that might emerge from user behavior or changes in data variables or their rankings.

As this example suggests, organizations will need a mix of risk-specific controls, and they are best served to implement them by creating protocols that ensure they are in place, and followed, throughout the AI-development process. The institutions in our examples implemented those protocols, as well as enterprise-wide controls, at least in part, through their existing risk infrastructure. Companies that lack a centralized risk organization can still put these AI risk-management techniques to work using robust risk-governance processes.

There is much still to be learned about the potential risks that organizations, individuals, and society face when it comes to AI; about the appropriate balance between innovation and risk; and about putting in place controls for managing the unimaginable. So far, public opinion and regulatory reaction have been relatively tempered.

But this is likely to change if more organizations stumble. As the costs of risks associated with AI rise, the ability both to assess those risks and to engage workers at all levels in defining and implementing controls will become a new source of competitive advantage. On the horizon for many organizations

is a reconceptualization of “customer experience” to encompass the promise as well as the pitfalls of AI-driven outcomes. Another imperative is to engage in a serious debate about the ethics of applying AI and where to draw lines that limit its use. Collective action, which could involve industry-level debate about self-policing and engagement with regulators, is poised to grow in importance as well. Organizations that nurture those capabilities will be better positioned to serve their customers and society effectively; to avoid ethical, business, reputational, and regulatory predicaments; and to avert a potential existential crisis that could bring the organization to its knees.

**Benjamin Cheatham** is a senior partner in McKinsey’s Philadelphia office and leads QuantumBlack, a McKinsey company, in North America; **Kia Javanmardian** is a senior partner in the Washington, DC, office; and **Hamid Samandari** is a senior partner in the New York office.

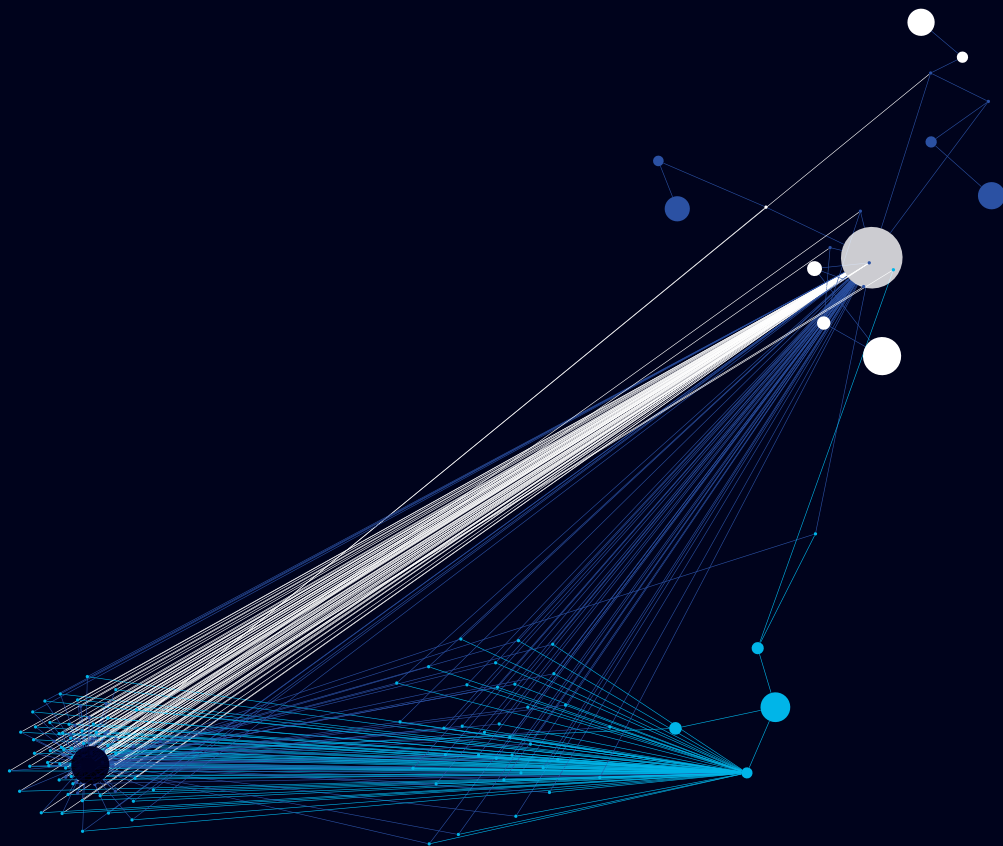
The authors wish to thank Roger Burkhardt, Liz Grennan, Nicolaus Henke, Pankaj Kumar, Marie-Claude Nadeau, Derek Waldron, and Olivia White for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Derisking machine learning and artificial intelligence

The added risk brought on by the complexity of machine-learning models can be mitigated by making well-targeted modifications to existing validation frameworks.

*by Bernhard Babel, Kevin Buehler, Adam Pivonka, Bryan Richardson, and Derek Waldron*



**Machine learning and artificial intelligence** are set to transform the banking industry, using vast amounts of data to build models that improve decision making, tailor services, and improve risk management. According to the McKinsey Global Institute, this could generate value of more than \$250 billion in the banking industry.<sup>1</sup>

But there is a downside, since machine-learning models amplify some elements of model risk. And although many banks, particularly those operating in jurisdictions with stringent regulatory requirements, have validation frameworks and practices in place to assess and mitigate the risks associated with traditional models, these are often insufficient to deal with the risks associated with machine-learning models.

Conscious of the problem, many banks are proceeding cautiously, restricting the use of machine-learning models to low-risk applications, such as digital marketing. Their caution is understandable given the potential financial, reputational, and regulatory risks. Banks could, for example, find themselves in violation of antidiscrimination laws, and incur significant fines—a concern that pushed one bank to ban its HR department from using a machine-learning résumé screener. A better approach, however, and ultimately the only sustainable one if banks are to reap the full benefits of machine-learning models, is to enhance model-risk management.

Regulators have not issued specific instructions on how to do this. In the United States, they have stipulated that banks are responsible for ensuring that risks associated with machine-learning models are appropriately managed, while stating that existing regulatory guidelines, such as the Federal Reserve’s “Guidance on Model Risk Management” (SR11-7), are broad enough to serve as a guide.<sup>2</sup>

Enhancing model-risk management to address the risks of machine-learning models will require policy decisions on what to include in a model inventory,

as well as determining risk appetite, risk tiering, roles and responsibilities, and model life-cycle controls, not to mention the associated model-validation practices. The good news is that many banks will not need entirely new model-validation frameworks. Existing ones can be fitted for purpose with some well-targeted enhancements.

### **New risks, new policy choices, new practices**

There is no shortage of news headlines revealing the unintended consequences of new machine-learning models. Algorithms that created a negative feedback loop were blamed for the 6 percent “flash crash” of the British pound in 2016, for example, and it was reported that a self-driving car failed to properly identify a pedestrian walking her bicycle across the street, with tragic consequences.

The cause of the risks that materialized in these machine-learning models is the same as the cause of the amplified risks that exist in all machine-learning models, whatever the industry and application: increased model complexity. Machine-learning models typically act on vastly larger data sets, including unstructured data such as natural language, images, and speech. The algorithms are typically far more complex than their statistical counterparts and often require design decisions to be made before the training process begins. And machine-learning models are built using new software packages and computing infrastructure that require more specialized skills.

The response to such complexity does not have to be overly complex, however. If properly understood, the risks associated with machine-learning models can be managed within banks’ existing model-validation frameworks, as the exhibit on the next page illustrates.

Highlighted in the exhibit are the modifications made to the validation framework and practices employed by Risk Dynamics, McKinsey’s model-validation

---

<sup>1</sup> For the purposes of this article, machine learning is broadly defined to include algorithms that learn from data without being explicitly programmed, including, for example, random forests, boosted decision trees, support-vector machines, deep learning, and reinforcement learning. The definition includes both supervised and unsupervised algorithms. For a full primer on the applications of artificial intelligence, see “An executive’s guide to AI,” on McKinsey.com.

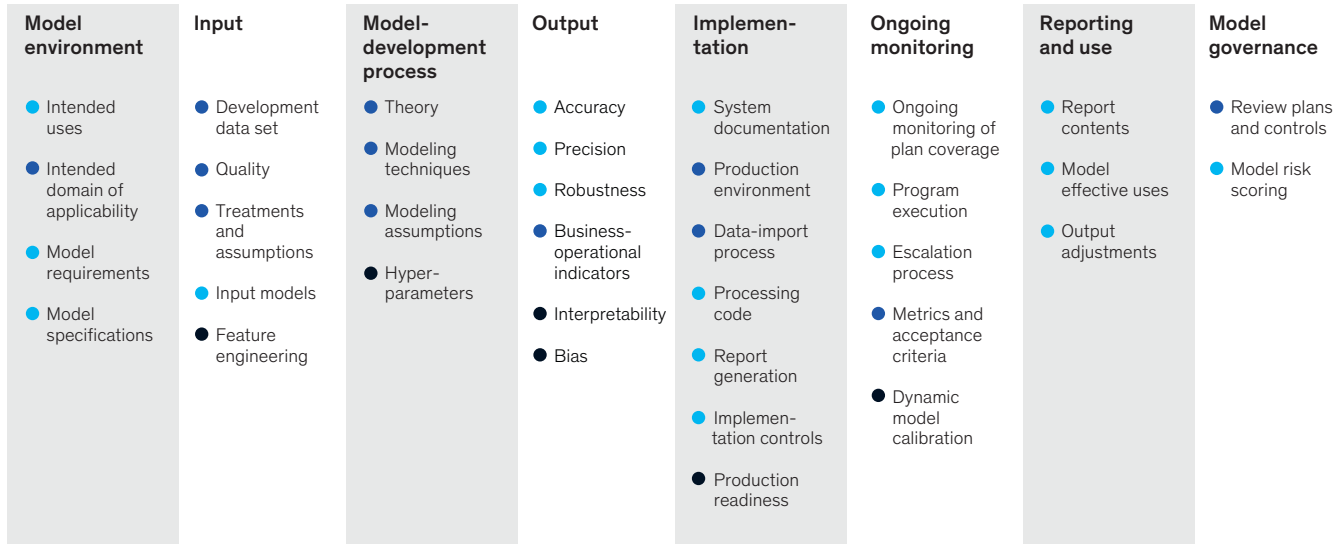
<sup>2</sup> Lael Brainard, *What are we learning about artificial intelligence in financial services?*, Fintech and the New Financial Landscape, Philadelphia, PA, November 13, 2018, [federalreserve.gov](https://www.federalreserve.gov).

Exhibit

## Existing validation frameworks can address machine-learning-model risk with some well-targeted enhancements.

### Similarity to traditional validation

● New ● Modified ● No change



arm. This framework, which is fully consistent with SR11-7 regulations and has been used to validate thousands of traditional models in many different fields of banking, examines eight risk-management dimensions covering a total of 25 risk elements. By modifying 12 of the elements and adding only six new ones, institutions can ensure that the specific risks associated with machine learning are addressed.

### The six new elements

The six new elements—interpretability, bias, feature engineering, hyperparameters, production readiness, and dynamic model calibration—represent the most substantive changes to the framework.

#### Interpretability

Machine-learning models have a reputation of being “black boxes.” Depending on the model’s architecture, the results it generates can be hard to understand or explain. One bank worked for months on a machine-learning product-recommendation

engine designed to help relationship managers cross-sell. But because the managers could not explain the rationale behind the model’s recommendations, they disregarded them. They did not trust the model, which in this situation meant wasted effort and perhaps wasted opportunity. In other situations, acting upon (rather than ignoring) a model’s less-than-transparent recommendations could have serious adverse consequences.

The degree of interpretability required is a policy decision for banks to make based on their risk appetite. They may choose to hold all machine-learning models to the same high standard of interpretability or to differentiate according to the model’s risk. In the United States, models that determine whether to grant credit to applicants are covered by fair-lending laws. The models therefore must be able to produce clear reason codes for a refusal. On the other hand, banks might well decide that a machine-learning model’s recommendations to place a product

advertisement on the mobile app of a given customer poses so little risk to the bank that understanding the model's reasons for doing so is not important.

Validators also need to ensure that models comply with the chosen policy. Fortunately, despite the black-box reputation of machine-learning models, significant progress has been made in recent years to help ensure their results are interpretable. A range of approaches can be used, based on the model class:

- **Linear and monotonic models (for example, linear-regression models):** linear coefficients help reveal the dependence of a result on the output.
- **Nonlinear and monotonic models, (for example, gradient-boosting models with monotonic constraint):** restricting inputs so they have either a rising or falling relationship globally with the dependent variable simplifies the attribution of inputs to a prediction.
- **Nonlinear and nonmonotonic (for example, unconstrained deep-learning models):** methodologies such as local interpretable model-agnostic explanations or Shapley values help ensure local interpretability.

### **Bias**

A model can be influenced by four main types of bias: sample, measurement, and algorithm bias, and bias against groups or classes of people. The latter two types, algorithmic bias and bias against people, can be amplified in machine-learning models.

For example, the random-forest algorithm tends to favor inputs with more distinct values, a bias that elevates the risk of poor decisions. One bank developed a random-forest model to assess potential money-laundering activity and found that the model favored fields with a large number of categorical values, such as occupation, when fields with fewer categories, such as country, were better able to predict the risk of money laundering.

To address algorithmic bias, model-validation processes should be updated to ensure appropriate algorithms are selected in any given context. In some cases, such as random-forest feature selection, there are technical solutions. Another approach is to develop “challenger” models, using alternative algorithms to benchmark performance.

To address bias against groups or classes of people, banks must first decide what constitutes fairness. Four definitions are commonly used, though which to choose may depend on the model's use:

- **Demographic blindness:** decisions are made using a limited set of features that are highly uncorrelated with protected classes, that is, groups of people protected by laws or policies.
- **Demographic parity:** outcomes are proportionally equal for all protected classes.
- **Equal opportunity:** true-positive rates are equal for each protected class.
- **Equal odds:** true-positive and false-positive rates are equal for each protected class.

Validators then need to ascertain whether developers have taken the necessary steps to ensure fairness. Models can be tested for fairness and, if necessary, corrected at each stage of the model-development process, from the design phase through to performance monitoring.

### **Feature engineering**

Feature engineering is often much more complex in the development of machine-learning models than in traditional models. There are three reasons why. First, machine-learning models can incorporate a significantly larger number of inputs. Second, unstructured data sources such as natural language require feature engineering as a preprocessing step before the training process can begin. Third, increasing numbers of commercial machine-learning packages now offer so-called AutoML, which generates large numbers of complex features to test many transformations of the data. Models produced using these features run the risk of being



unnecessarily complex, contributing to overfitting. For example, one institution built a model using an AutoML platform and found that specific sequences of letters in a product application were predictive of fraud. This was a completely spurious result caused by the algorithm's maximizing the model's out-of-sample performance.

In feature engineering, banks have to make a policy decision to mitigate risk. They have to determine the level of support required to establish the conceptual soundness of each feature. The policy may vary according to the model's application. For example, a highly regulated credit-decision model might require that every individual feature in the model be assessed. For lower-risk models, banks might choose to review the feature-engineering process only: for example, the processes for data transformation and feature exclusion.

Validators should then ensure that features and/or the feature-engineering process are consistent with the chosen policy. If each feature is to be tested, three considerations are generally needed: the mathematical transformation of model inputs, the decision criteria for feature selection, and the business rationale. For instance, a bank might decide that there is a good business case for using debt-to-income ratios as a feature in a credit model but not frequency of ATM usage, as this might penalize customers for using an advertised service.

#### **Hyperparameters**

Many of the parameters of machine-learning models, such as the depth of trees in a random-forest model or the number of layers in a deep

neural network, must be defined before the training process can begin. In other words, their values are not derived from the available data. Rules of thumb, parameters used to solve other problems, or even trial and error are common substitutes. Decisions regarding these kinds of parameters, known as hyperparameters, are often more complex than analogous decisions in statistical modeling. Not surprisingly, a model's performance and its stability can be sensitive to the hyperparameters selected. For example, banks are increasingly using binary classifiers such as support-vector machines in combination with natural-language processing to help identify potential conduct issues in complaints. The performance of these models and the ability to generalize can be very sensitive to the selected kernel function.

Validators should ensure that hyperparameters are chosen as soundly as possible. For some quantitative inputs, as opposed to qualitative inputs, a search algorithm can be used to map the parameter space and identify optimal ranges. In other cases, the best approach to selecting hyperparameters is to combine expert judgment and, where possible, the latest industry practices.

#### **Production readiness**

Traditional models are often coded as rules in production systems. Machine-learning models, however, are algorithmic, and therefore require more computation. This requirement is commonly overlooked in the model-development process. Developers build complex predictive models only to discover that the bank's production systems cannot support them. One US bank spent considerable

**An institution built a model using an AutoML platform and found that specific sequences of letters in a product application were predictive of fraud—a spurious result.**

resources building a deep learning–based model to predict transaction fraud, only to discover it did not meet required latency standards.

Validators already assess a range of model risks associated with implementation. However, for machine learning, they will need to expand the scope of this assessment. They will need to estimate the volume of data that will flow through the model, assessing the production–system architecture (for example, graphics–processing units for deep learning), and the run time required.

### **Dynamic model calibration**

Some classes of machine–learning models modify their parameters dynamically to reflect emerging patterns in the data. This replaces the traditional approach of periodic manual review and model refresh. Examples include reinforcement–learning algorithms or Bayesian methods. The risk is that without sufficient controls, an overemphasis on short–term patterns in the data could harm the model’s performance over time.

Banks therefore need to decide when to allow dynamic recalibration. They might conclude that with the right controls in place, it is suitable for some applications, such as algorithmic trading. For others, such as credit decisions, they might require clear proof that dynamic recalibration outperforms static models.

With the policy set, validators can evaluate whether dynamic recalibration is appropriate given the intended use of the model, develop a monitoring plan, and ensure that appropriate controls are

in place to identify and mitigate risks that might emerge. These might include thresholds that catch material shifts in a model’s health, such as out–of–sample performance measures, and guardrails such as exposure limits or other, predefined values that trigger a manual review.

---

Banks will need to proceed gradually. The first step is to make sure model inventories include all machine learning–based models in use. You may be surprised to learn how many there are. One bank’s model risk–management function was certain the organization was not yet using machine–learning models, until it discovered that its recently established innovation function had been busy developing machine–learning models for fraud and cybersecurity.

From here, validation policies and practices can be modified to address machine–learning–model risks, though initially for a restricted number of model classes. This helps build experience while testing and refining the new policies and practices. Considerable time will be needed to monitor a model’s performance and finely tune the new practices. But over time banks will be able to apply them to the full range of approved machine–learning models, helping companies mitigate risk and gain the confidence to start harnessing the full power of machine learning.

**Bernhard Babel** is a partner in McKinsey’s Cologne office; **Kevin Buehler** is a senior partner in the New York office, where **Adam Pivonka** is an associate partner and **Derek Waldron** is a partner; **Bryan Richardson** is a senior expert in the Vancouver office.

The authors wish to thank Roger Burkhardt, Pankaj Kumar, Ryan Mills, Marc Taymans, Didier Vila, and Sung-jin Yoo for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Going digital in collections to improve resilience against credit losses

With delinquencies on the rise, lenders need to transform their contact approaches now to suit customer preferences.

*by Matthew Higginson, Frédéric Jacques, Marta Matecsa, and Davide Tesini*



© Westend61/Getty Images

**Since the financial crisis**, losses at many lending institutions have been historically low. The period of economic recovery after 2008 to 2009 was defined by accommodative monetary policies, strong demand from a burgeoning Chinese economy, and a massive increase in cross-border trade. The financial markets took off. Credit growth returned—faster in North America, more moderately in Europe. In the low-interest-rate environment, lenders adjusted their lending policies to acquire more customers again.

Perhaps not surprisingly, institutions allowed their collections capabilities and recovery operations (at least for unsecured loans) to languish during the long up cycle. But now household debt is at an all-time high, delinquencies have been rising, and forward-looking macroeconomic indicators are softening. As a result, lenders are reexamining their capacities for handling delinquencies. Part of that reevaluation for heads of collections involves taking into account changes in the consumer landscape. For example, consumers increasingly communicate with financial-services providers through text messaging and prefer self-service digital channels. They do not respond to repetitive collections phone calls—an approach further complicated by stricter regulations against harassment.

As the evidence for a deteriorating credit cycle mounts along with increasing losses, lenders can take steps to increase institutional resilience. By strengthening collections capabilities and embracing digital communications, they will be better prepared to address any further increase in delinquencies that may occur.

### **The canary in the coal mine?**

Do rising credit delinquencies foreshadow economic down cycles? Are collections departments the “canary in the coal mine” of an economy, indicating by upticks in demand an approaching slowdown?

Household delinquencies in the United States hovered at historically low levels through 2016. They began to climb in 2017, however, rising steadily across home-equity and auto loans, as well as credit cards. By the fourth quarter of 2018, delinquencies had reached their highest point in seven years. Over the last 18 months, both delinquent balances and losses have risen for nearly every unsecured lending product in North America. Credit cards in 90-plus days’ delinquency, for example, have risen by 5.3 percent, while auto loans in this category have ballooned by 14 percent.<sup>1</sup> Whether recent trends signal a return to “normal” or the onset of a cyclical downturn remains to be seen.

Should signs of a slowing economy continue to gather, institutions will want to recall the experience of previous downturns. Economic slowdowns involve many industries and create effects that linger beyond the point when the macroeconomy begins to recover. The implications for collections departments will be experienced not only in financial services but also in utilities, healthcare, telecommunications, and the public sector. The recently expanded client base, accelerated by new online lenders, has created vulnerabilities for institutions: some of the new customers are riskier and will likely experience financial stress early in any down cycle. The pressure to lend to these customers can even rise as the economy slows, as attracting business from an increasingly conservative consumer sector becomes more difficult.

### **Is ‘right sizing’ now wrong?**

Even in an environment of average delinquency rates—for example, 4.6 percent for cards in the United States—collections operations today may be unprepared to address sudden demand. The history of credit losses is bimodal, with persistent low losses punctuated by sudden spikes; in other words, normalcy involves periods in which delinquency rates are substantially higher than average (Exhibit 1).

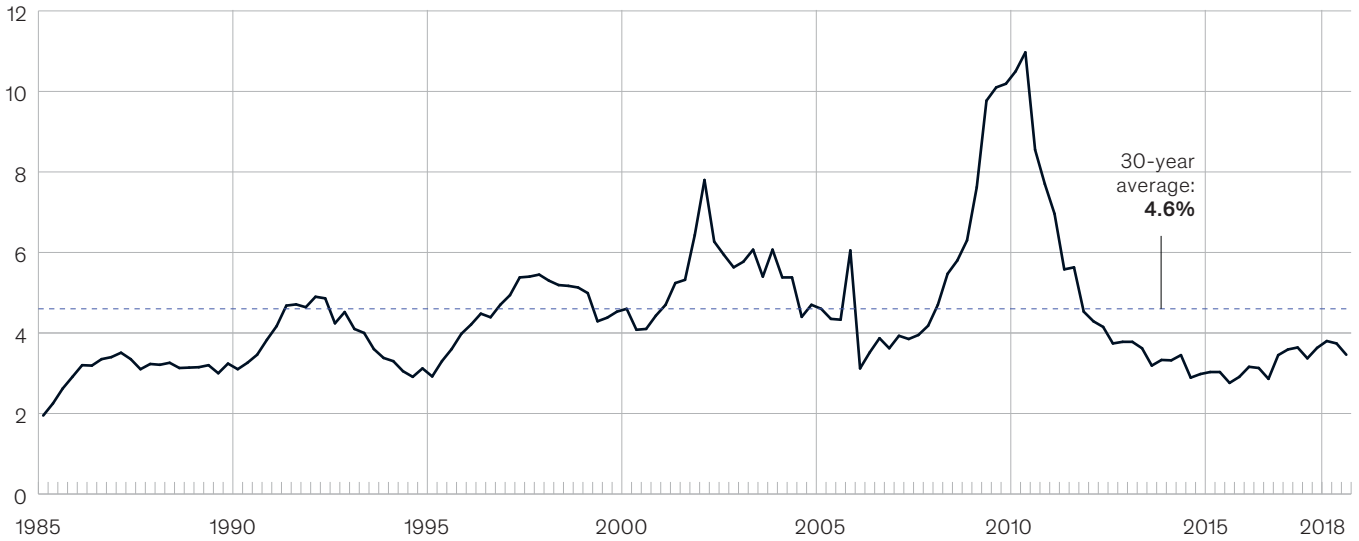
---

<sup>1</sup> *Quarterly report household debt and credit*, Federal Reserve Bank of New York, fourth quarter 2018, [newyorkfed.org](http://newyorkfed.org).

Exhibit 1

## In the United States after the financial crisis, credit-card charge-off rates quickly fell below historical averages.

US credit-card charge-off rate, %



Source: US Federal Reserve

During the long recovery from the financial crisis, lenders closed tens of millions of accounts of risky customers, causing a flight to a new marketplace of online lenders using innovative peer-to-peer (P2P) platforms. Then, as interest revenues fell, major incumbent lenders began expanding their customer base again, while hoping that advanced analytics would enable them to avoid borrowers at the greatest risk of default. Between 2011 and 2015, for example, the average credit score of auto-loan customers in the United States fell by more than 25 points, sufficient to shift some lenders' focus from prime to near prime.<sup>2</sup> Credit has not been scarce. Total household consumer debt in the United States has risen steadily for the past seven years and stands at almost \$14 trillion. With strong employment and buoyant equities and

real-estate prices, this debt could be maintained. Any sustained reversal of economic conditions, however, could trigger an avalanche of losses, with the most marginal customers no longer able to service their debts. And higher losses in secured borrowing could trigger a fire sale of collateral and create contagion in the markets.

This could present a serious challenge to institutions that in recent years have adjusted to loss rates that were 30 percent below historical averages. The approach they took, of cost cutting in collections through head-count reductions and a focus on efficiency, has left little spare capacity. Now that delinquencies are growing, institutions need the capabilities to address the new demand for their services.

<sup>2</sup> As calculated by Fair Isaac Corporation, or FICO, a private analytics company.

## Changing consumer habits: The digital generation

In addition to the likelihood that collections units are understaffed, their traditional collections methods have become less helpful. An unintended effect of ubiquitous smartphone use has been to dilute the potency of outbound calling as a way to reach customers. Despite the fact that nearly every delinquent customer has a phone, they typically do not answer calls, preferring instead to communicate (and pay) in their own time, on their own terms. They are quite adept at using smarter call-screening technology. Regulatory pressure has also blunted the usefulness of the outbound dialing tool: many card issuers have received compliance notices since 2012, making them especially sensitive to any attempt to increase contact frequency that could be perceived as customer harassment.

Despite the trend, many lenders are still focusing on the old ways of doing things. During the last recession, some firms even added staff to make more calls. Now a digital approach is needed.

### How customers experience delinquency contact

A recent McKinsey survey highlighted this mismatch between the contact strategies employed by most issuers and the contact preferences of their delinquent customers. In late 2018, we asked questions of credit-card customers who recently fell into delinquency. The objectives were to understand how they experienced outreach from their card issuer, how they prefer to be contacted, and the respective outcomes of these two approaches. Based on their responses, we were able to plot the relationship between institutional contact strategies, customer preferences, and outcomes (Exhibit 2).

The three main lessons of the survey can be summarized as follows:

- Most issuers still pursue traditional contact strategies based on the delinquent customer's balance, risk profile, and days delinquent. The strong preference of lenders is to prioritize
- outbound phone calls and letters, especially in later delinquency. Digital contact channels, including email, text messaging, and online chat are more commonly used by institutions in early delinquency but after 30 days are largely abandoned as too passive an approach. Evidently, fewer than half of the major issuers have a true multichannel contact strategy in collections.
- Delinquent customers expressed a preference to be contacted primarily by email and text message. They also report that issuers mainly use traditional contact channels nonetheless. Lower-risk customers in particular prefer alerts and notifications via voice mail or email, and to take action in their own time. These “digital first” customers are identifiable by simple characteristics like demographic data, balance, payment behavior, channel of acquisition, and use of online banking and apps. They represent a significant portion of the total delinquent population and vastly outnumber those who say they prefer traditional channels.
  - In responding to issuers' contact strategies, digital-first and traditional-channel customers behave very differently. The digital-first segment is 12 percent more likely to make a payment when contacted by the bank through a preferred digital channel in early delinquency. In late delinquency, this likelihood rises to 30 percent. The proportion of these customers who pay in full also doubles when they are contacted through digital channels. A small minority of customers still prefer phone and letter contact, a distinct population that typically pays in full.

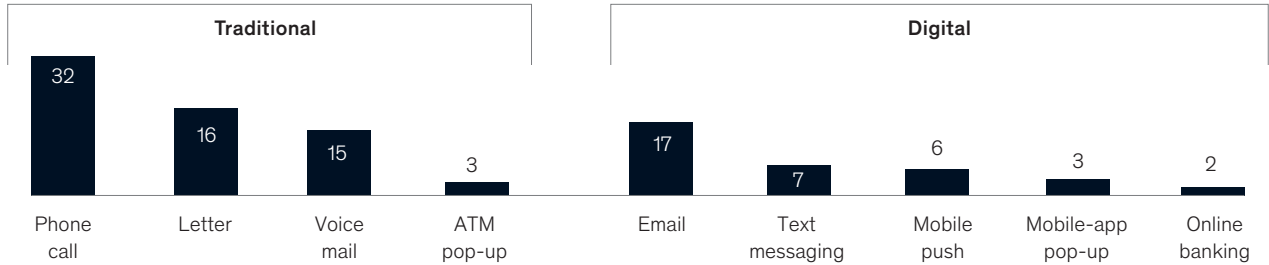
### Lenders are using the least effective rather than the most effective channels

As Exhibit 2 makes clear, the channels favored by lenders for contacting delinquent customers—phone, letter, and voice mail—are now the least effective in eliciting payments. Conversely, the channels that lenders use less often—email, text messaging, and pop-up notifications—are the most favored by customers today and yield the

Exhibit 2

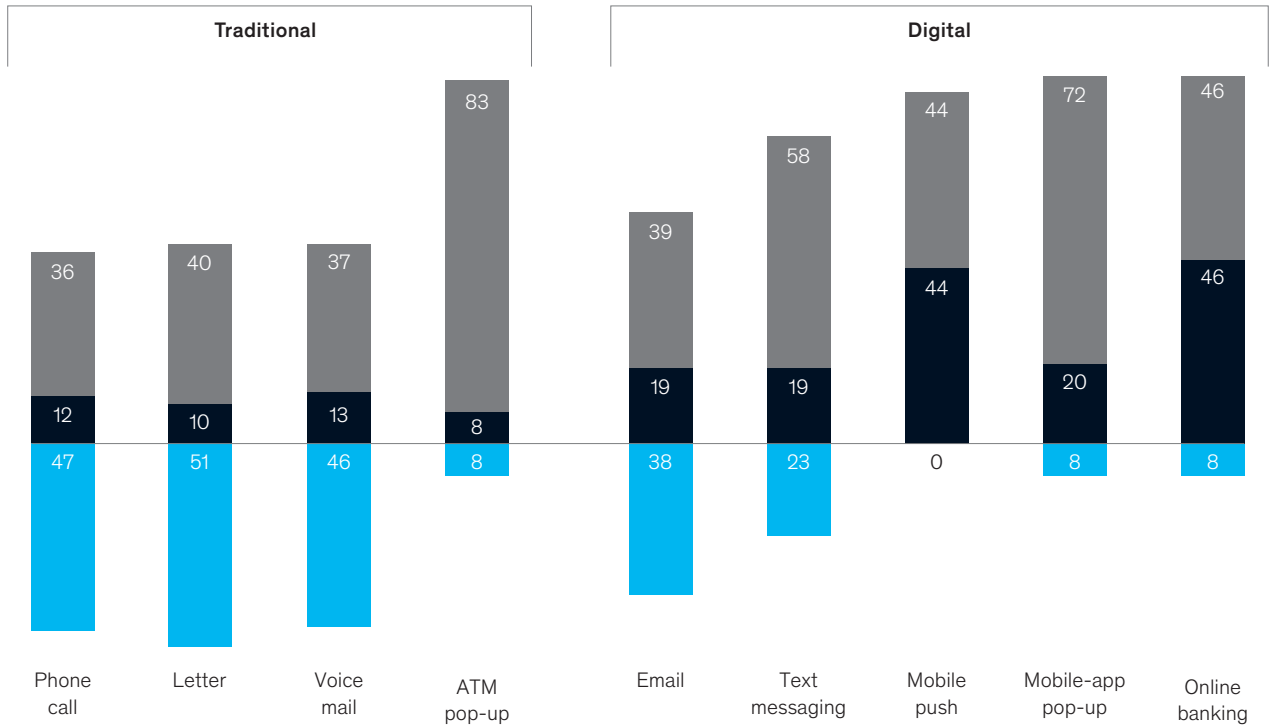
**According to a recent survey, banks are not using the channels that lead to the best customer outcomes.**

Method of last-contact channel for accounts 30+ days past due, % of total respondents



Payment action, by last-contact channel, for accounts 30+ days past due, % of total respondents

■ Full payment   ■ Partial payment   ■ No action



Note: Figures may not sum to 100%, because of rounding and omission of an inconsequential category ("Other").

Source: McKinsey survey of credit-card customers at North American financial institutions, 2018

best results (Exhibit 3). Lenders, in other words, are using the least effective rather than the most effective contact channels, while customers clearly prefer digital-first contact.

Whether this mismatch is due to rapidly shifting customer preferences, a lack of digital capabilities among the issuing banks, or a resistance to change among risk-averse collections managers, the implications are the same: customers are not responding. They expect and prefer to communicate digitally, whether their financial institutions understand this or not. These expectations have already been demonstrated in other dimensions of banking operations (such as service to sales). Those banks that continue to ignore customer preferences will suffer the consequences in losses higher than those experienced by more responsive peers.

Such a competitive disadvantage could become profound in an economic slowdown. During and following the last recession, many issuers were served with enforcement actions for unfair or deceptive lending practices, including fines for harassment of delinquent customers. Of particular concern was the intimidating language used by collectors and the obnoxious frequency at which

they were calling individual customers (in some cases as often as 20 times per day). As a result, many collections operations have drastically reduced their calling frequency and focused on using compliant language and noninvasive collector behaviors. Many issuers have taken away performance-related employee compensation, and punish collectors who tell customers that they must make a payment.

To avoid both harassment complaints and unwanted costs, many banks are phoning lower-risk customers less frequently—once per day or a few times per week. Lower-frequency calling is the norm for customers that have not consented to banks' calling their mobile phones through an automated dialer. Despite rising losses, furthermore, many collections units fail to raise contact rates due to internal-risk rulings. Interestingly, recent research by the US Consumer Financial Protection Bureau indicates that most issuers fall far short of their own self-imposed call-frequency caps.<sup>3</sup>

Banks should be able to increase contact frequency and achieve better customer outcomes if they switch to a coordinated multichannel approach, with smarter dialing practices and

<sup>3</sup> *The consumer credit card market*, US Consumer Financial Protection Bureau, December 2017, [consumerfinance.gov](http://consumerfinance.gov).

### Exhibit 3

## Customers prefer email, text messaging, and mobile channels for contact, finding traditional channels little engaging.

**65%**

of issuer-initiated contact is with traditional channels (phone, voice mail, letter) despite poor response rates

**89–92%**

payment rates can be achieved by using digital channels—online banking or mobile

Source: McKinsey survey of credit-card customers at North American financial institutions, 2018



better text messaging. Newer entrants into the recovery business report higher response and recovery rates after they abandon outbound dialing completely. Their approaches focus on tailored digital messages that bypass spam filters and contain language that resonates with delinquent customers. Higher response rates have been achieved with tailored landing pages, account-specific text alerts, and email content that educates and gives hope rather than depresses customers. Surely there are lessons here for pre-charge-off collections as well.

## **The collections transformation journey**

In response to rising delinquencies, shifting consumer preferences, and the current regulatory environment, leading financial institutions have begun a journey of digital transformation in collections. Borrowing heavily from successful approaches used in other parts of the business, they are investing in advanced analytics, digital channels, advanced collector capabilities, and next-generation collections strategies. Recognizing that it takes time to design, build, test, and implement such strategies, these leaders have inaugurated transformation efforts with 12 months or more set aside for completion. We have observed four effective constituent actions.

### **1. Strengthen segmentation capabilities with advanced analytics**

With rising delinquencies and resource limitations, institutions need better segmentation and fewer customers referred for personal attention. As institutions perfect their enterprise data warehouse and advanced-analytics capabilities, they are discovering that more can be done with what they already have in the meantime. Regulators have lately welcomed analytics applications that allow issuers to improve customer differentiation and tailor contact and collections strategies. The approach has generated better outcomes for customers. Issuers can maximize the number of customers that pay on their own initiative (self-cure) with analytics-based targeted digital campaigns for those in early delinquency or even predelinquency, while using the customers' preferred digital contact channels. Furthermore, unresponsive accounts that fit the

profile for fraud can be filtered out more rigorously and sent to a separate treatment queue.

### **2. Develop effective omnichannel orchestration**

Digital-first customers inhabit an app-based world. They expect to address their delinquency in their own time, through easy-to-use self-serve channels. The growth of online bill payment points the way for issuers. With an integrated collections platform, customers would have self-serve access to the exact same payment plans and treatment solutions as those that issuers offer over the phone. Customers should also be able, through the online self-service channel, to schedule automated future payments ("autopay").

These digital-first customers should also continue to be contacted through an orchestrated omnichannel digital contact strategy, even if they are delinquent beyond 30 days. With active-response models, business rules can be introduced such that outliers that have not responded digitally after a reasonable amount of time are passed to agents for skip tracing and personal assistance.

### **3. Optimize messaging used in all customer contacts**

Examples abound of delinquent customers responding positively to empathetic messages from their issuers. Instead of sending generic or passive-aggressive notices of collections, issuers can use language that highlights options for solutions and payments. Many institutions have had success with this approach. Leading issuers are also using more client-specific language in alerts, to avoid the appearance of spamming or phishing. By training and empowering collectors to have intelligent conversations using "words that work" according to customer needs—rather than standardized scripts—collections managers create a higher likelihood of finding a sustainable solution for customers.

### **4. Restructure the operating model to serve customer needs**

The collections operating model should be structured to allocate collectors in proportion to customer needs. Institutions can better anticipate these needs by improving segmentation, as discussed previously. One step is to divert low-risk

and self-serve customers away from live calling and toward digital-first solutions. For higher-risk customers, collectors can be trained to identify their needs more closely by assessing their ability and willingness to pay. These parameters help enable more effective negotiations and better outcomes. Another step is to shift staff to more personalized “ownership” teams, whose members take ownership of a customer relationship, engaging in repeated conversations with particular high-risk customers to craft personalized and sustainable solutions.

### **Prioritize and act now**

In our experience, collections executives are never short of ideas for improvement but sometimes fail to prioritize their agenda. As advocated in a book by our colleagues, *Strategy Beyond the Hockey Stick: People, Probabilities, and Big Moves to Beat the Odds* (John Wiley & Sons, 2018), a top team will create far greater impact by focusing on five to ten major initiatives than by trying to implement 50 to 100 minor ones. Operational agility will be critically important; priority initiatives should include both quick wins to build momentum as well as the longer-term capability goals. The collections initiatives we are proposing require the introduction of new approaches, such as a digital self-service platform, that will quickly become self-funding.

Many collections heads encounter resistance to modernizing their departments while losses hover around historical averages. Indeed, many report that collections has been largely neglected as product revenues have expanded. We argue that this state of affairs must change. From “trough to peak,” losses rose 250 percent in the 24 months after the fourth quarter of 2007. At many institutions, meanwhile, implementing a major IT project (such as a collections transformation) can take 12 to 18 months. Even with a sound plan of action (such as that described previously), many institutions will lack implementation capabilities, leaving collections operations extremely vulnerable. By failing to digitize their collections operations, these institutions risk potentially crippling losses in a future downturn. But if they start now, they could have a largely transformed shop within 12 months.

---

The global economy has been emitting mixed signals of late, prompting a fair amount of analyst speculation about an impending downturn. One need not guess at the “estimated time of arrival” of a recession, however, before investing in a smart, digital-forward collections transformation. The sooner institutions act, the sooner they will reap near-term rewards and be prepared for future uncertainties.

**Matt Higginson** is a partner in McKinsey’s Boston office, **Frédéric Jacques** is a partner in the Montréal office, **Marta Matecsa** is an associate partner in the Budapest office, and **Davide Tesini** is an associate partner in the New York office.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Bubbles pop, downturns stop

Economic downturns are impossible to predict, and sure as sunrise. Build resistance now, because when the sun comes up, you'd better be moving.

*by Martin Hirt, Kevin Laczkowski, and Mihir Mysore*



Illustration by Daniel Hertzberg

**Waste no time** trying to predict the next economic cycle. The running joke is that “experts” correctly anticipated seven out of the last three macroeconomic events. Unfortunately, it is unlikely that the hit rate will be any better next time around.

Geopolitics, economic cycles, and many other forces that can have substantial effects on the fortunes of your business are inherently uncertain. Higher volatility in our business environment has become the “new normal” for many. And while scenario analysis is a worthwhile exercise to rationally assess some of the uncertainties you are facing, there is no guarantee for getting it right.

So, if you are concerned about the economic outlook, and if you get challenging questions from your board about the resilience of your business performance, how do you best respond?

It turns out that in times of crisis and in times of economic slowdown, not everybody fares the same. When we traced the paths of more than 1,000 publicly traded companies, we found that during the last downturn, about 10 percent of those companies fared materially better than the rest. We called those companies “resilients”—and we were intrigued. What made them different? Was it sector related? Did they simply get lucky?

As we investigated more deeply, we found some noteworthy characteristics in how resilients weathered the storms: how they prepared for them, how they acted during tougher periods, and how they came out of them.

We will share some of the more specific findings with you below, but let’s start with the core insight right here: Resilients moved early, ahead of the downturn. They entered ahead, they dipped less, and they came out of it with guns blazing.

In short, your business context is and will remain uncertain. But if you get moving now, you can ride the waves of uncertainty instead of being overpowered by them.

## How the resilients performed

In our book, *Strategy Beyond the Hockey Stick: People, Probabilities, and Big Moves to Beat the Odds* (John Wiley & Sons, 2018), we researched more than 2,000 companies over two decades to show that corporate performance follows a power curve. A small number of companies capture the lion’s share of global economic profit, while the vast majority return just slightly above their cost of capital. Moving up the power curve requires big moves: dynamic resource reallocation, disciplined M&A, and dramatic productivity improvement. Those findings held across economic cycles.

Our latest research focused squarely on what specifically helps companies thrive through downturns. The focal point of our analysis was a group of approximately 1,100 publicly traded companies, across a wide range of industries and geographies, with revenue exceeding \$1 billion. We found that between 2007 and 2011, in each of 12 economic sectors analyzed, there also was a power curve of corporate performance, measured in terms of total returns to shareholders (TRS) or excess TRS growth during that period, relative to the sector median. The top quintile of companies in each sector—the resilients—delivered TRS growth that was structurally higher than the median in their sector (see Exhibit 1 for a representative analysis in the technology, media, and telecommunications sector).

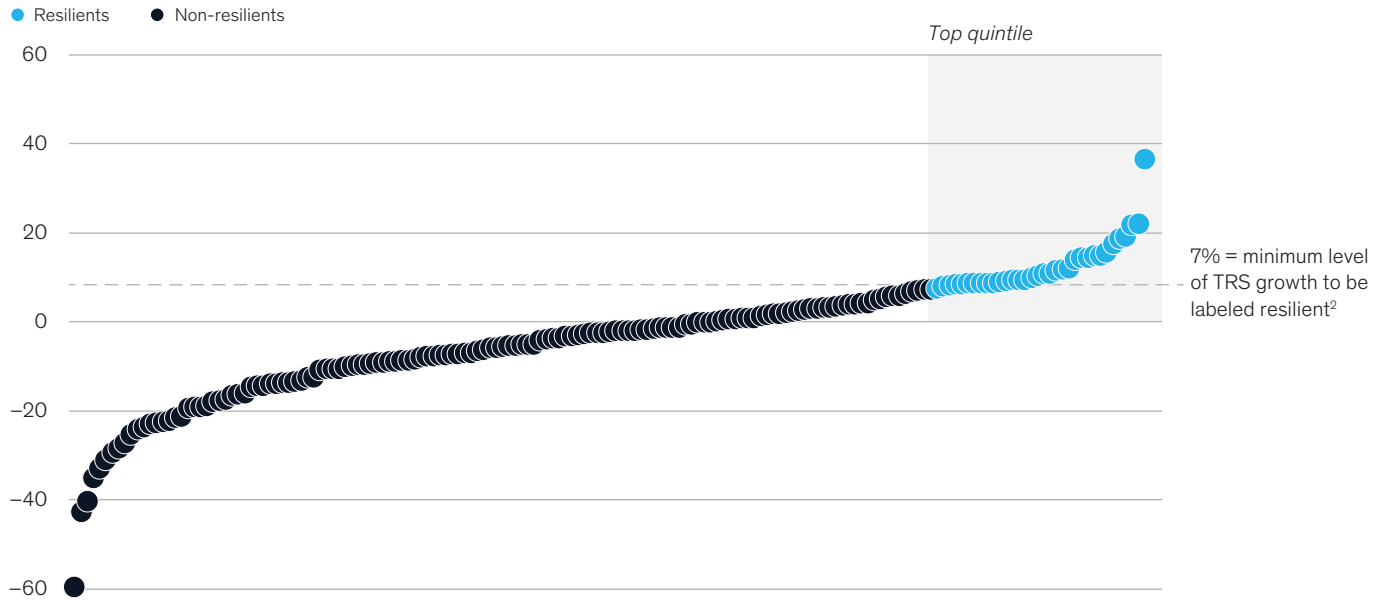
In the three boom years before 2007, the resilients actually underdelivered slightly on TRS. However, they opened up a slight TRS lead relative to their sector peers during the downturn and extended this lead through the recession (Exhibit 2). By 2017, the cumulative TRS lead of the typical resilient had grown to more than 150 percentage points over the non-resilients. This lead was tough to reverse: nearly 70 percent of the resilients remained top-quintile performers in their sector, with just a small fraction of the non-resilients joining them.

When the economy started heading south, what distinguished the resilients was earnings, not revenue. Barring a few sectors that were

Exhibit 1

**While the last downturn was severe, some companies flourished.**

Compound annual TRS growth rate for companies in technology, media, and telecom sector,<sup>1</sup> 2007–11, %



<sup>1</sup> TRS = total returns to shareholders; n = 171; results are representative of analyses done for 11 other sectors, for a total of 1,144 companies.

<sup>2</sup> That is, 7% more compound annual TRS growth from 2007 to 2011.

Source: S&P Capital IQ; McKinsey analysis

exceptions, resilient companies lost nearly as much revenue as industry peers during the early stages of the slowdown. However, by the time the downturn reached its trough in 2009, the earnings of resilient companies, measured as earnings before interest, taxes, depreciation, and amortization (EBITDA), had risen by 10 percent, while industry peers had lost nearly 15 percent.

**What the resilient companies did**

Resilient companies did three things to create this earnings advantage:

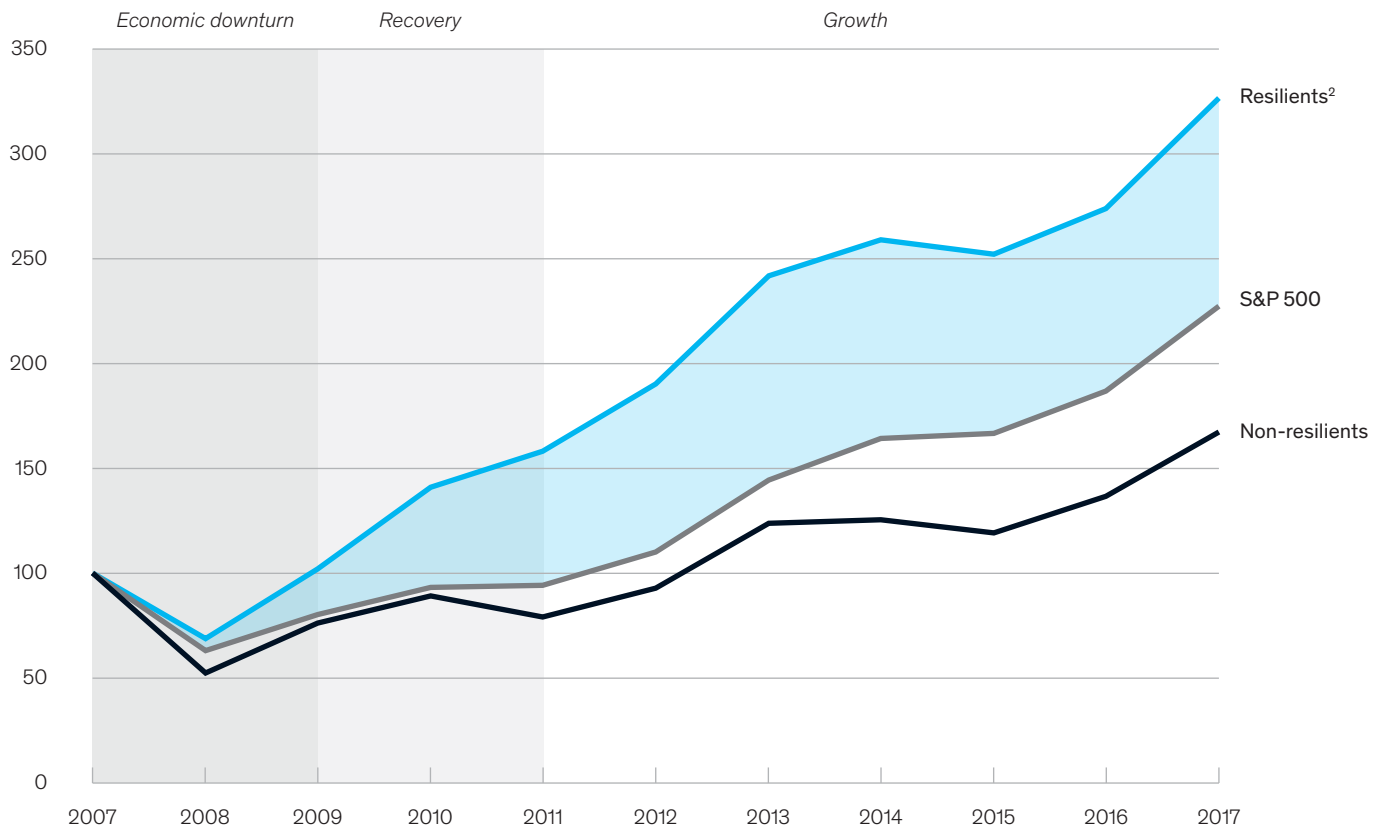
**1. Resilient companies created flexibility—a safety buffer.** They did this by cleaning up their balance sheets before the trough, which helped them be more acquisitive afterward. In particular, resilient companies were deleveraging during 2007: they reduced their debt by more than \$1 for every dollar of total capital on their balance sheet, while peers added more than \$3 of debt. They accomplished this partly by divesting underperforming businesses 10 percent faster than their peers. The upshot was that

resilient companies entered the trough with more financial flexibility. At the first sign of economic recovery, the resilient companies shifted to M&A, using their superior cash levels to acquire assets that their peers were dumping in order to survive. Overall, the resilient companies were about 10 percent more acquisitive early in the recovery. They accelerated when the economy was stuck in low gear.

**2. Resilient companies cut costs ahead of the curve.** There is little evidence to suggest that the resilient companies were better at timing the market. However, it is quite clear that they prepared earlier, moved faster, and cut deeper when recessionary signs were emerging. One such warning came in the summer of 2007, when the global financial markets briefly seized up before settling back down. By the first quarter of 2008, the resilient companies already had cut operating costs by 1 percent compared with the year before, even as their peers' year-on-year costs were growing by a similar amount. The resilient companies maintained and expanded their cost lead as the recession moved toward its trough, improving their operating edge

## Resilient companies did better at the outset of the downturn and after.

### Cumulative TRS performance<sup>1</sup>



<sup>1</sup> TRS = total returns to shareholders; calculated as average of subsectors' median performance within resilient and non-resilient categories; n = 1,140 companies; excludes financial companies and real-estate investment trusts.

<sup>2</sup> Resilient companies defined as top quintile in TRS performance by sector.

Source: S&P Capital IQ; McKinsey analysis

in seven out of the eight quarters during 2008 and 2009. In doing so, the resilient companies appear to have focused primarily on operational effectiveness, reducing their cost of goods sold, while maintaining selling, general, and administrative costs roughly in line with sales.

**3. Resilient companies in countercyclical sectors focused on growth, even if it meant incurring costs.** There were three sectors in the last recession that behaved very differently from the rules above, primarily because they saw little impact to their revenues and only slightly slower growth as an industry. Oil and gas was in the middle of a commodity supercycle in the early part of the recession, with prices reaching as high as \$120 per barrel. Meanwhile, demand

for healthcare and pharmaceuticals proved relatively inelastic. For these growth sectors, the rule book was quite different. Their resilient companies actually overdelivered significantly on revenue, while taking on higher costs.

### What's different now

Invaluable as the lessons of history are, we also must be cognizant of changes in the external environment. Consider first costs: reducing them, faster and deeper, in the way that the resilient companies did during 2008–09, is likely to be difficult. That's partly because competition in global markets, and the relentless pressure of activist shareholders, have left businesses with less fat to trim than in previous cycles. We recently asked a group of

CEOs at the World Economic Forum in Davos, as well as at a similar forum in New York, whether their companies had a lot of potential for large cost cuts. Two-thirds of them were dubious.

Although, when push comes to shove, it starts seeming more feasible to realize challenging savings—these days, across-the-board cost cuts can create more problems than they solve. For starters, there's the risk of undercutting digitization efforts by underinvesting in mission-critical talent. There are also the wider social costs of layoffs, which companies are starting to feel in the form of backlash from communities, customers, politicians, and workers.

Digital and analytics-driven productivity improvements may be an important alternative to conventional cost cuts or cross-border labor-cost arbitrage. Our work with major manufacturing businesses across a range of sectors over the past two years suggests that for many companies, cost-reduction opportunities using “traditional” levers amount to only about 2 percent of costs, whereas those applying digital and analytics tools can reduce costs by a further 5 percent. In general, accelerating digitization has widened the gap in capabilities and performance between digital leaders and laggards—a gap that is likely to grow during any downturn.

### **A robust resilience playbook**

These environmental differences don't mean you should forget about costs in the next recession; the ability of the resilient to drive earnings growth despite top-line challenges was a critical differentiator. But it does point toward a resilience playbook (Exhibit 3) emphasizing more balanced performance interventions, as well as faster decision making enabled by a resilience “nerve center” and a well-prepared organization.

### **Balanced performance interventions**

Getting past the limitations of traditional performance approaches oriented around head count and cost will require fresh thinking about boosting productivity. A large electrical-equipment manufacturer, for example, found that adopting

robotic-arc welding led to a 30 percent decrease in manufacturing costs, a 50 percent improvement in production time, higher quality, and better process control. Production costs fell to levels similar to those in China, and the manufacturer decided against further offshoring, expanding manufacturing in the United States instead. This example shows that the economic logic of advanced technologies and automation cuts in multiple directions, with robots creating and saving some jobs even as they displace others. Working through this nuance, and communicating it to relevant stakeholders, will be an important part of leaders' roles moving forward.

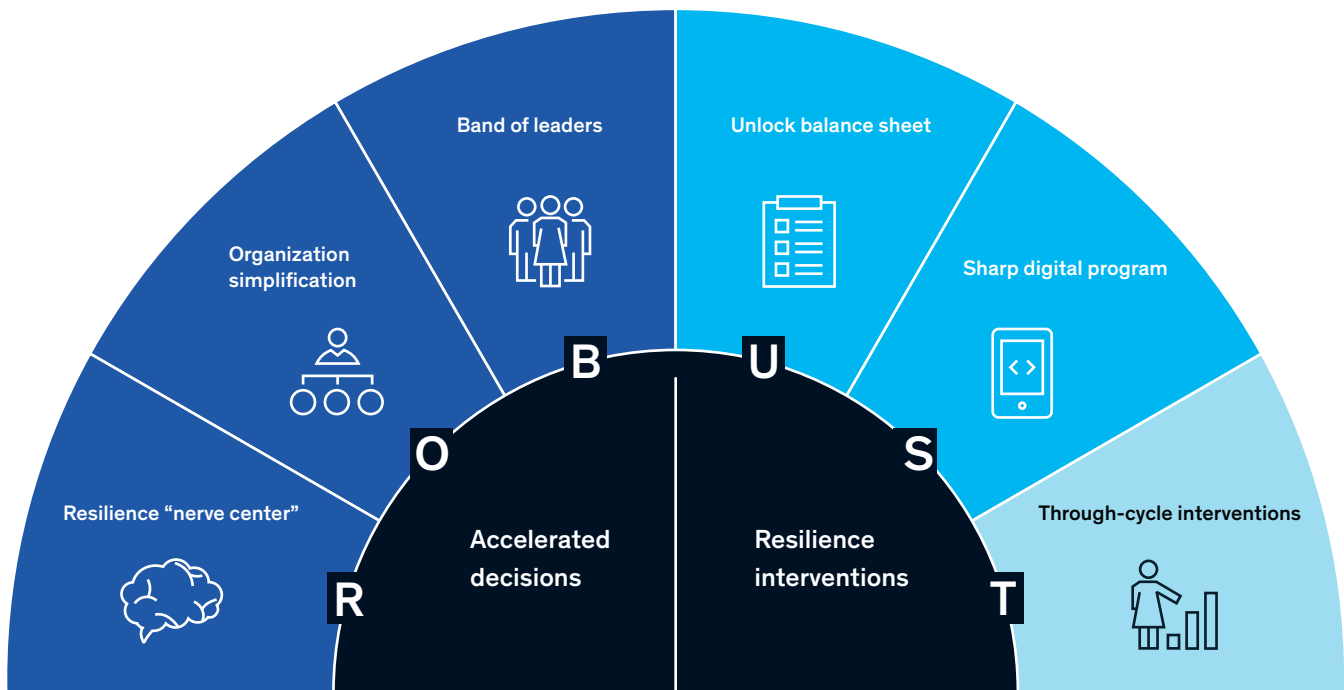
Although the resilient's earnings edge rested primarily on cost savings, they were also better at locking in post-cycle growth, partly through the use of emerging tools that enabled them to better serve higher-value customer segments. A specialized cargo airline, for instance, developed a new system for categorizing customers in its micromarkets based on demand, flight availability, and capacity per flight. It then rewarded customers that contributed most to its tough-to-fill routes and negotiated price with large customers based on their route-by-route volume. This increased the carrier's share of wallet as high as 20 percent with key customers.

These performance interventions need to be balanced with creating flexibility—either operational or financial. Financial flexibility is achieved partly by unlocking your balance sheet, or by divesting noncore assets early, before the fire sales start. Operational flexibility may be created through variable contracts and more diverse supply sources and platforms that share components across product lines and parts, among other levers, as new McKinsey Global Institute research shows. Toyota has been on such a journey, investing billions to ensure its factories can shift seamlessly between different body styles and power trains.

### **Sharp digital discipline**

As advanced technologies and analytics create performance opportunities, they're reshaping competitive dynamics in far-reaching ways. Our

**A new resilience playbook is emerging.**



colleagues have shown in separate research that those further along the digital journey are realizing 7-plus percent more revenue growth than industry peers, and nearly 6 percent more EBITDA growth. This digital divide, combined with the tendency for downturns to drive a sustained wedge in performance, could mean a long-lasting bifurcation among digital “haves” and digital “have-nots.” The digital haves will connect better with loyal customers; provide a frictionless, private customer experience; serve them at a lower cost; absorb price hits; and avoid expensive IT upgrades at a vulnerable time. Digital have-nots, on the other hand, may feel a need to retrench, making catch-up elusive, even when economic conditions improve.

Future resilientists will likely have a clear view of which critical processes should be digitized to drive near-term value and which initiatives (such as creating new offerings or investing to extend customer reach) are critical to remaining competitive. An auto insurer, for example, might

safeguard an initiative aimed at using analytics and machine learning to create claims estimates without sending an inspector to look at a damaged car, because of its transformational potential. It might also stay the course with the development of a new pricing system that has significant near-term potential. On the other hand, a process-redesign effort whose full potential will be difficult and time-consuming to capture as a result of regulatory and reporting differences across geographies might get moved off the priority list.

Most advanced technology efforts require engaging people in multiple parts of the organization—analytics experts, customer-experience specialists, operators skilled at robotic process automation, lean-operations gurus, and the like. Breaking down organizational silos to engage all these people often requires special attention. Australian insurer IAG, for example, created an “accelerator” that, according to chief digital officer Mark Drasutis, looks “across all



the activities to understand and direct priorities, [and bring] together expertise across the business . . .”<sup>1</sup> The challenge during a downturn is that near-term cost pressures and traditional organizational reporting lines sometimes yield efforts to “lean things out” function by function, with each executive or manager told to “make cuts in what’s in your control.” This approach becomes outmoded fast in the horizontal, cross-functional world of digital innovation and execution. Instead, companies should get important digital work done through agile operating units, deployed flexibly against value-creation opportunities.

### **The resilience nerve center**

A resilience nerve center aims to do three things well:

- **Monitor** a small number of material risks and use stress tests to orient the company, early, toward downturn-related economic impacts.
- **Decide** how the organization will manage these impacts faster.
- **Execute** by organizing teams into agile, cross-functional units that drive toward clear outcomes, create forums for faster executive decision making, and monitor the results through value-based initiative tracking.

The art of effective resilience monitoring starts with a recognition that any effort to identify an economic scenario precisely will inevitably miss something that turns out to be important, while creating a deafening cacophony of risks that leaves leaders overwhelmed and unable to act. It is far better, in our experience, to agree on a small number of representative major threats and for each to define a clear leading indicator, as well as triggers for escalating the threat to decision makers. Thinking this through ahead of time is great preparation for tackling unexpected threats when they emerge.

The next step is to incorporate these material threats into a map, like the one devised by an oil and gas company we know, that focuses on the potential timing, sequencing, magnitude (confirmed by stress-test modeling of financial impact under different scenarios), and second-order effects associated with various hazards. This map becomes the basis for big strategic moves. If a particular idea will not help neutralize one of the issues spelled out in the threat map, it may not be bold enough to make the company resilient.

All of this work ends up being a theoretical exercise unless it leads to quick decisions and then action—which in our experience starts with forming cross-functional, highly autonomous teams with well-defined objectives.

### **Preparing your organization, your leaders—and yourself**

The fast-moving teams that support nerve-center activities, and also are intertwined with many digitization and operational-improvement efforts, may sound a lot like agile squads. That’s no accident, because more and more organizations are embracing agile approaches.

Leaders should certainly use resilience planning to build on those initiatives, but as part of a much wider effort to simplify the organization and prepare for uncertainty. A full-scale reorganization is tough to pull off anytime, and particularly so in the throes of a major downturn, so a recluster of activities may help. This is best done in the flow of ongoing strategic dialogue about portfolio priorities, particularly divestiture and acquisition opportunities whose urgency could rise with swings in the macroeconomy. The recluster can be dramatic, approaching a zero-based “clean sheet” approach, or something more incremental.

Simultaneously, you can identify, using an analytical approach, the skills and people needed to carry the business through turbulence. Most

---

<sup>1</sup> See “Scaling and accelerating a digital transformation,” February 2019, McKinsey.com.

companies shed people during a recession, but resilient players are just as conscious of investing in the skills needed to win in the recovery. Know your key roles. Then look at how your top talent is arrayed against them and what you need to do about any mismatches (which might include, for example, retaining or acquiring digital skills, or rethinking the outsourcing of IT talent).

All this will require a leadership team that is itself agile and resilient, able to make effective decisions quickly in an atmosphere of uncertainty and stress. Many superstars imploded under pressure during the last recession, and most of their equivalents today have not been tested in the cauldron of a serious downturn. Resilient executives will likely display a more comfortable relationship with uncertainty that allows them to spot opportunities and threats and rise to the occasion with equanimity. Now is also the time to develop a plan spelling out who will be involved, and how often, in making and communicating key decisions, ideally empowering those employees closest to the work.

Particular attention should be focused on a process to ensure that “big bet” strategic decisions—those like divestments and acquisitions—are the outcome of a healthy and well-informed debate rather than made on the fly.

---

Underlying the priorities we’ve been describing is a bias toward action—an urgency that reminds us of a quote: “Every morning in Africa, a gazelle wakes up. It knows it must run faster than the fastest lion or it will be killed. Every morning a lion wakes up. It knows it must outrun the slowest gazelle or it will starve to death. It doesn’t matter whether you are a lion or a gazelle: when the sun comes up, you’d better be running.”<sup>2</sup>

Are you a lion or a gazelle?

Or, put differently: If you are concerned about the resilience of your business, are you already moving?

---

<sup>2</sup> “Lions or gazelles?” in “The other dimension: Technology and the City of London—A survey,” *Economist*, July 6, 1985. For more on this quote, which has been attributed to a variety of individuals, see “The fable of the lion and the gazelle,” Quote Investigator, [quoteinvestigator.com](http://quoteinvestigator.com).

**Martin Hirt** is a senior partner in McKinsey’s Taipei office, **Kevin Laczkowski** is a senior partner in the Chicago office, and **Mihir Mysore** is a partner in the Houston office.

The authors wish to thank Cindy Levy, Mary Meaney, Philipp Radtke, Kirk Rieckhoff, Hamid Samandari, and Sven Smit for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

# Fighting back against synthetic identity fraud

Digging deep into the data trails people leave behind can help banks detect whether their customers are real or not and stem losses from this fast-growing financial crime.

*by Bryan Richardson and Derek Waldron*



© Reinhard Krull/Getty Images

### **Banks have become much more effective**

at preventing many types of fraud thanks to their investments in technology, but criminality has evolved in response. Rather than using a stolen credit card or identity (ID), many fraudsters now use fictitious, synthetic IDs to draw credit. Indeed, by our estimates, synthetic ID fraud is the fastest-growing type of financial crime in the United States, accounting for 10 to 15 percent of charge-offs in a typical unsecured lending portfolio.<sup>1</sup> Instances of synthetic ID fraud have also recently been reported in other geographies.<sup>2</sup> More worrying still, much bigger losses are building up behind these IDs like hidden time bombs.

That risk is because of the way the fraudsters typically operate. Over months, if not years, they build up a good credit record with synthetic IDs. Only when the credit lines are maximized do repayments cease—or, in the jargon of the business, do the synthetic IDs “bust out.” Fraud rings sometimes establish thousands of synthetic IDs, all waiting to default. The largest synthetic ID ring detected to date racked up losses for banks of \$200 million from 7,000 synthetic IDs and 25,000 credit cards.<sup>3</sup>

To date, there has been no efficient way of uncovering synthetic ID fraud. To crack down on it, every customer seeking credit would have to undergo even more rigorous ID checks than they do already. This article proposes a new approach that, with the help of machine learning, digs deep into vast amounts of third-party data to gauge whether the basic information given by an applicant matches that of a real person, thereby weeding out the small proportion of those likely to be using a synthetic ID. It is on this group that banks, or indeed any organization wanting to stop synthetic ID fraud, can focus their ID checks without inconveniencing other customers.

### **The scam**

Synthetic IDs are created by applying for credit using a combination of real and fake, or sometimes entirely fake, information. The application is typically rejected because the credit bureau cannot match the name in its records. However, the act of applying for credit automatically creates a credit file at the bureau in the name of the synthetic ID, so the fraudster can now set up accounts in this name and begin to build credit. The fact that the credit file looks identical to those of many real people who are just starting to build their credit record—that is, there is limited or no credit history—makes the scam nearly impossible to detect.

The question that springs to mind is: Why do financial institutions fail to conduct additional, more rigorous screening to identify synthetic IDs when onboarding new customers? In the United States, a large part of the problem is that there is no efficient government process to confirm whether a Social Security number, date of birth, or name is real. And although the government is developing a service to address this, the release date and precise capabilities remain unclear.<sup>4</sup>

The sophisticated technology that has helped detect other types of fraud is not of much assistance. Machine-learning techniques such as deep neural networks that find patterns associated with fraud are of little use, because so few cases of synthetic ID fraud have been uncovered on which to train models. Unsupervised machine-learning techniques that look for anomalies in data also struggle, because there are few, if any, differences between real and synthetic IDs at the time of application.

This leaves financial institutions having to conduct their own additional—and sometimes intrusive—

---

<sup>1</sup> AnnaMaria Andriotis and Peter Rudegeair, “The new ID theft: Millions of credit applicants who don’t exist,” *Wall Street Journal*, March 6, 2018, wsj.com.

<sup>2</sup> “Synthetic’ identity fraud costs Canada \$1B a year,” CBC/Radio-Canada, October 11, 2017, cbc.ca.

<sup>3</sup> “Eighteen people charged in international \$200 million credit card fraud scam,” US Department of Justice, February 5, 2013, justice.gov.

<sup>4</sup> The US government is building an application that will verify Social Security numbers, names, and dates of birth as part of the Economic Growth, Regulatory Relief, and Consumer Protection Act (S.2155).

checks, slowing an already complex onboarding process. The danger becomes that banks deter not only the fraudsters but also the very customers they wish to attract, who may well turn to competitors instead.

### **How extra data helps**

An approach to identifying synthetic IDs that entails leveraging third-party data can be a powerful tool. It is grounded in the fact that real people have real histories, evidence of which they scatter behind them in dozens of different data systems, physical and digital. These trails are hard to fake. They have depth—that is, large amounts of data that stretch back years. For example, a real teacher might have a student loan taken out ten years ago, a social-media account, a cell-phone record, a couple of past employers, several previous addresses, an email account set up years ago, and property records. The trails of real people are also consistent: the same address, email account, and phone number crop up in various databases. Synthetic IDs tend to be inconsistent, because although the applicant may give some real details (perhaps a name that reoccurs in various data systems), others are fabricated, so they will not reoccur. In cases in which the synthetic ID is entirely fabricated, the ID may be too consistent—that is, there are no changes at all to the address, email account, and other data over several years.

### **A rich demonstration**

By evaluating the depth and consistency of information available about applicants in third-party data systems, institutions can determine whether the applicants are real or not. McKinsey undertook research to demonstrate the efficacy of this approach. While adhering to all applicable privacy regulations, we used a sample of 15,000 profiles gathered from a consumer-marketing database (exhibit):

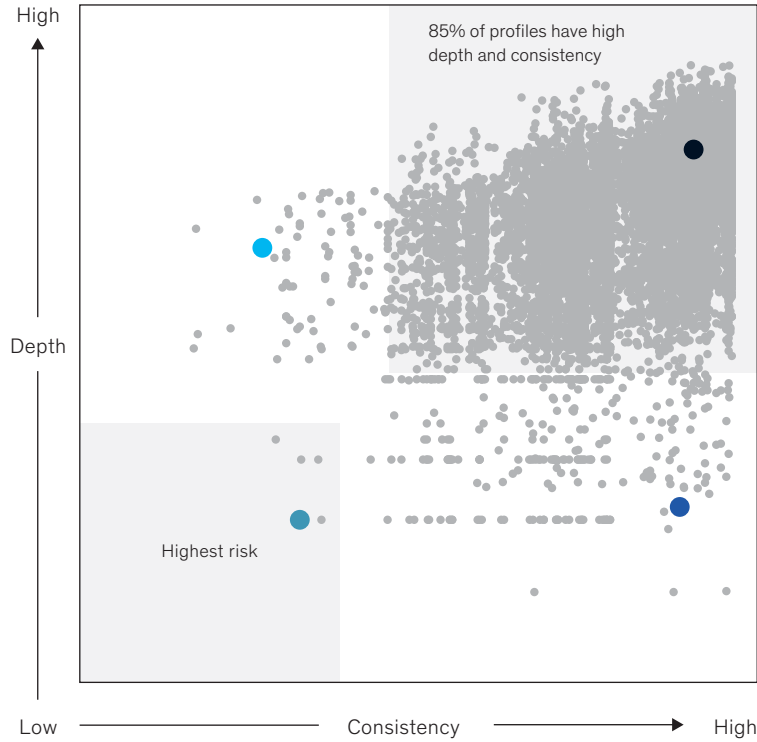
- We used nine external data sources to check and augment the data in each profile, looking at social-media accounts, email addresses, mobile-phone and landline numbers, financial behavior, property records, and other information. The nine sources chosen were those with the most digital and nondigital information that matched our sample group. The sources yielded more than 22,000 unique fields of information.
- We then identified some 150 features that served as measures of a profile's depth and consistency that could be applied to all 15,000 people. (The fact that there were so many suitable measures illustrates the wealth of relevant external data available.) The features related to depth included the age of a first loan, age of the oldest recorded nondigital event (a vehicle registration, for example), and age of an email address. Features related to consistency included matches of unique names with the


## **Why do financial institutions fail to conduct additional, more rigorous screening to identify synthetic IDs when onboarding new customers?**

Exhibit

From nine sources of external data, McKinsey researchers determined the likely authenticity of identities based on data depth and consistency.

Matrix for scoring profile depth and consistency





**Arturo**  
High consistency,  
high depth



**Cheryl**  
Low consistency,  
high depth



**Maria**  
High consistency,  
low depth



**John**  
Low consistency,  
low depth

Consistency				
Unique names	1	2	1	2
Unique numbers	1	1	1	2
Suspicious indicators?	No	No	No	Yes
Depth				
Age of nondigital data	25 years	8 years	15 years	<1 year
Nondigital data	12 records	5 records	1 record	0 records
Email age	9 years	9 months	<1 year	<3 months

Note: Under consistency and depth, only top three features are listed.

same data in many sources, as well as reverse matches of particular data points (such as addresses and phone numbers) leading back to the same name.

- An overall depth and consistency score was then calculated for each ID. The lower the score, the higher the risk of a synthetic ID.
- For some identities, low depth or consistency scores clearly did not indicate high-risk profiles. Someone fresh out of school may well have a new email address, for example. A suite of machine-learning models was used to take account of such anomalies and adjust overall scores accordingly.
- The final results of our demonstration showed that 85 percent of the profiles we examined had high depth and consistency, and a further 10 percent fell just outside the normal range. The remaining 5 percent, as depicted in the lower left-hand quadrant of the exhibit, were profiles that would raise suspicions. “John,” for example, has two different names linked to the same phone number, his email is fewer than three months old, and the age of his oldest nondigital record is less than a year.

If armed with similar scoring systems, banks could ascertain whether an applicant’s profile looked real. They could then instantly extend credit, perhaps limited, to those applicants with high depth and consistency scores. They could even offer higher initial credit limits than would normally be the case for first loans, since low-risk applicants could be distinguished from high-risk ones.

Very limited credit, or none, would be extended to high-risk applicants while their IDs were reviewed more thoroughly with the help of a range of processes, such as in-person verification of documents and third-party income verification, as well as increasingly sophisticated tools. These tools include biometric screening that matches a face to a photo on a driver’s license or passport, voice

identification that assigns the unique voiceprint of a customer to a Social Security number, and geospatial technology that confirms whether a customer’s application was made from the stated address. Some checks are less obtrusive than others, and it may be wise to conduct these first. That said, many customers understand and appreciate banks’ efforts to reduce fraud.

Importantly, banks could also review existing accounts to avoid any further buildup of debt through synthetic IDs. High-risk accounts would require extra ID checks; in the meantime, additional credit would be denied or limited.

### **Next steps**

Chances are, if your onboarding processes for customers applying for credit do not include in-person verification of documents or biometric screening, you are exposed to synthetic ID fraud. The extent of that exposure is harder to gauge, as even the most sophisticated banks struggle to know whether an unpaid debt is a result of synthetic ID fraud, another type of fraud, or simply a customer who cannot pay. One approach is to look for charge-offs that resemble synthetic ID fraud—for example, those that occurred fewer than two years after the account was opened, had minimal account activity, and for which there was no customer contact once credit limits were reached. The results are likely to spur you to further action.

If so, assemble a team of data scientists, compliance experts, and fraud experts to gather third-party data and develop a synthetic ID risk model. A good one will be built from external data sources that have a good match rate. For example, an online bank will likely find plenty of additional information on applicants in social-media data. Banks whose customers have an older demographic will find information on property ownership helpful. The model will also have good-quality data, and all data will adhere to privacy regulations. So test multiple external data providers. Remember, too, that while

machine learning can help sort through the data and formulate models, risk-model managers need to validate them. If the models and data introduce bias or incorrect information, they can be riskier than the fraud that companies seek to mitigate.

Finally, when it comes to deployment, test any changes you choose to make to the customer-onboarding process as a result of the model's findings on a sample of customers. You may find, for example, that the extra time it adds to the application process is unacceptably long, so you would have to rethink the design.

Fraud will continue to evolve to evade detection. However, by mining the growing number of third-party data sources available, banks can deepen their understanding of their customers. This knowledge can help banks enhance risk controls and stem losses associated with synthetic ID fraud—all without burdening the vast majority of honest customers with ever-more intrusive and time-consuming ID checks.

---

**Bryan Richardson** is a senior knowledge expert in McKinsey's Vancouver office, and **Derek Waldron** is a partner in the New York office.

The authors wish to thank DemystData, a comprehensive data-access company, for helping provide the data used in this article. The authors also wish to thank Kevin Buehler, Mark Hookey, Ivan Pyzow, and Shoan Joshi for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.



# Critical infrastructure companies and the global cybersecurity threat

How the energy, mining, and materials industries can meet the unique challenges of protecting themselves in a digital world.

*by Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallace*



© Milko Marchetti/Getty Images

**Whether they generate or distribute power,** or extract or refine oil, gas, or minerals, heavy industrial companies comprise critical infrastructure for the global economy. As a result, they are attractive targets for cybercrimes. Already by 2018 nearly 60 percent of relevant surveyed organizations had experienced a breach in their industrial control (ICS) or supervisory control and data-acquisition (SCADA) systems.<sup>1</sup>

Heavy industrials face unique cybersecurity challenges, given their distributed, decentralized governance structures and large operational technology (OT) environment—an environment that does not lend itself readily to traditional cybersecurity controls.<sup>2</sup> Furthermore, many heavy industrials have invested in becoming “cyber mature,” as have other at-risk industries, such as financial services and healthcare. The investment gap has left most heavy industrials insufficiently prepared for the mounting threats.

As awareness of the threat environment grows, however, many top executives at these companies are now sharpening their focus on cybersecurity. They are asking important questions such as: What does it take to transform our cybersecurity capabilities? What investments will address the most risk? How much should we be spending? Leading companies are now rethinking their cybersecurity organizations and governance models. Some are taking advantage of new security tools for OT offered by innovative start-ups. Most are adopting a risk-based approach to security—identifying their critical assets and seeking appropriate controls based on risk levels (see sidebar, “A cybersecurity transformation in oil and gas”).

## Evolution of the threat landscape

Several factors underlie the growing threat landscape for the heavy industrial sector. One is the rise in geopolitical tensions, which has led to attacks targeting critical national infrastructure. Heavy industrials can become collateral damage in

broader attacks even when they are not the target, given IT security gaps and OT networks connected to IT networks through new technologies. Obviously, these threats have become a major concern for top managers, boards, and national government bodies.

## Attacks on national infrastructure

Among the most significant attacks on critical national infrastructure of the past few years are these:

- In 2014, a Western European steel mill suffered serious damage in its operational environment from a phishing attack used first to penetrate its IT network and then its OT network, where attackers gained control of plant equipment.
- The 2015 to 2016 attacks on an Eastern European power-distribution grid cut power to 230,000 people. In this case, attackers compromised a third-party vendor’s network, which was connected to an energy company’s OT network, allowing the attackers to make changes to the control system.
- In 2017, attackers gained access to a Middle Eastern petrochemical plant’s ICS and attempted to sabotage operations and trigger an explosion.

Recent discoveries in the networks of electrical-distribution companies based in the European Union and the United States indicate that threat actors established vantage points within OT networks from which to launch attacks at a future date. An example of this is the Dragonfly syndicate, which has been blamed for the breach of EU and US electrical companies to gather intelligence and build cyber capabilities to compromise OT systems.

Groups like Dragonfly are increasingly procuring private-sector offensive tools, enabling them to deliver highly sophisticated cyberattacks. Given the sensitivity of the targets, this has quickly become a matter of national security involving government bodies and intelligence agencies.

<sup>1</sup> Forrester consulting study commissioned and published by Fortinet, May 2018.

<sup>2</sup> Operational-technology systems include centralized, human-interface control systems such as supervisory control and data-acquisition systems (SCADA), industrial control systems (ICS), distributed control systems (DCS), industrial Internet of Things (IIoT) devices that send and receive feedback from machinery, and programmable logic controllers (PLC) that relay commands between SCADA and IIoT field devices.

## A cybersecurity transformation in oil and gas

---

A large state-owned oil and gas company was facing frequent cyberattacks, even as it was undertaking a digital transformation that increased the exposure of its critical systems. A successful attack on its assets would harm the economy of an entire nation.

Over 18 months, this multibillion-dollar organization was able to protect its assets and improve its overall digital resilience by transforming its cybersecurity posture. The transformation engaged 30,000 employees across 450 sites in addressing security issues every day. This experience offers a good example of how a critical-infrastructure company can meet the global cybersecurity threat and commit to the cyber-resilience journey.

The company operates across the industry value chain, upstream, midstream, and downstream. It had suffered attacks on both its IT and operational technology (OT) systems, which, as in most companies, were siloed from each other. Attacks hit IT network security and the supervisory control and data-acquisition (SCADA) systems.

The company suffered a ransomware attack, email phishing campaigns, and defacement of its website. As the company was digitizing many systems, including critical controllers, massive amounts of data were exposed to potential manipulation that could trigger disastrous accidents. The company focused on three important steps.

First, it defined and protected its “crown jewels”: its most important assets. It comprehensively mapped its business assets and identified the most critical, from automated tank gauges that manage pressure and oil levels on oil rigs to employee health records and customer credit-card information. The company created a library of controls to protect these crown-jewel assets, which are now being brought on line.

Second, the company focused on rapidly building capabilities. To address siloed IT and OT operations, it created an integrated cybersecurity organization under a chief security officer aligned with the risk function (see Exhibit 1 in this article). The

company also tailored industrial security standards to the oil and gas industry and its regional context. A security operation center was established to monitor and react to threats, and a data-loss-prevention program was set up to avoid leaks.

Third, the company outlined its plan for a holistic cybersecurity transformation, including a three-year implementation program with prioritized initiatives, estimated budget, and provisions to integrate cybersecurity into the digitization effort. To ensure that effort did not create new vulnerabilities, the company developed the new digital systems to be “secure by design,” creating secure coding guidelines and principles.

The achievements were impressive. The cybersecurity organization is now fully built, with a focus on improving resilience daily. The company is on its way to ensuring that it can continue to reliably supply the energy its nation needs, supporting a major share of the country’s GDP growth.

### Collateral damage in nonspecific attacks

The electricity, oil and gas, and mining sectors have been rapidly digitizing their operational value chains. While this has brought them great value from analysis, process optimization, and automation, it has also broadened access to previously isolated ICS and SCADA devices by users of the IT network and third parties with physical and/or remote access to the OT network. In many cases, this digitization has allowed access to these OT devices from the wider internet, as well. According to an analysis of production OT networks by CyberX, an industrial cybersecurity company, 40 percent of industrial sites have at least one direct connection to the

public internet, and 84 percent of industrial sites have at least one remotely accessible device.<sup>3</sup> In response to the danger, ICS manufacturers can analyze USB-born threats to detect and neutralize those that could seriously disrupt operations.

Ransomware poses an additional threat. One well-known example was WannaCry, which disrupted 80 percent of gas stations of a major Chinese oil company by exploiting a vulnerability in a dated and unsupported version of Windows. NotPetya was far more devastating. This malware wiped IT devices around the world, affecting about 25 percent of all oil-and-gas companies.

---

<sup>3</sup> CyberX report on global industrial control systems and Internet of Things risk (2018).

More recently, botnets with the ability to detect and infect SCADA systems have been discovered, and those targeting Internet of Things (IoT) devices have become pervasive. The past year has also seen the massive growth of crypto-mining malware targeting ICS computers, severely affecting productivity by increasing load on industrial systems.

These types of sweeping, nontargeted attacks disproportionately affect industries, including heavy industrial companies with less cyber maturity and many devices to protect. Moreover, heavy industrials have the dual challenge of protecting against new digital threats while maintaining a largely legacy OT environment. Most companies still operate with their founding cybersecurity initiatives like patch management and asset compliance. More than half of OT environments tested in one study had versions of Windows for which Microsoft is no longer providing security patches. Fully 69 percent had passwords traversing OT networks in plain text.<sup>4</sup>

### Unique security challenges facing heavy industrials

Electricity, mining, and oil and gas companies have revealed four unique security challenges that are less prevalent in industries of greater cyber maturity, such as financial services and technology. One challenge stems from the digital transformations that many energy and mining companies are undertaking. Others relate to their distributed footprint, their large OT environment, and exposure to third-party risk.

#### The overlooked costs of security in digital transformations

Most heavy industrials are undergoing major digital transformations or have recently completed them. When building the business case for these transformations, leaders often overlook the cost of managing the associated security risks. Security is not often a central part of the transformation, and security architects are brought in only after a new digital product or system has been developed. This security-as-afterthought approach increases the cost of digitization, with delays due to last-minute

security reviews, new security tools, or increases in the load on existing security tools. For example, instead of building next-generation security stacks in the cloud, most enterprises are still using security tools hosted on premise for their cloud infrastructure, limiting the cloud's cost advantages.

Additionally, security capabilities that are bolted on top of technology products and systems are inherently less effective than those built in by design. Bolt-on security can also harm product usability, causing friction between developers and user-experience designers on one side, and security architects on the other. This sometimes results in users circumventing security controls, where possible.

#### Protecting the 'crown jewels'

The expansive geographical footprint typical for these heavy industrials can harm their cybersecurity efforts in several ways. It limits their ability to identify and protect their key assets—their “crown jewels.” They may have difficulty managing vulnerabilities across end devices. And while they tend to have a good handle on IT assets managed centrally, they have little or no visibility over assets managed by business units or third parties. Examples of crown-jewel assets include IT, OT, and management assets:

- *information technology*: network diagrams, system logs, and network access directory
- *operational technology*: programmable logic controllers, SCADA protocols, and system-configuration information
- *management assets*: internal strategy documents, executive and board communications, customer and employee personal information

Governance structures typically leave central security leaders without responsibility for security in the business units or operations. Many heavy industrials we surveyed could not identify a party responsible for OT security. The chief information-security officer (CISO) may set policy and develop

---

<sup>4</sup> Ibid.

security standards but often has no responsibility for implementing OT security in the operations, or for auditing adherence to it. At the same time, many operational units have no clear security counterpart responsible for deploying, operating, and maintaining OT security controls at the plant level. Therefore, they often neglect OT security.

### **Challenges of protecting operational technology**

Most of today's OT networks consist of legacy equipment originally designed to be perimeter protected ("air gapped") from unsecure networks. Over time, however, much of it has become connected to IT networks. Most security efforts to protect OT involve network-based controls such as firewalls that allow data to leave the OT network for analysis, but do not allow data or signals to enter it. Although important, these perimeter controls are ineffective against attacks originating from within the OT network, such as malware on removable devices. Additionally, malware has been discovered that exploits vulnerabilities in virtual private networks (VPNs) and network-device software.

Many traditional security tools cannot be applied to the OT environment. In some cases, these tools can harm the sensitive devices that control plant equipment. Even merely scanning these devices for vulnerabilities has led to major process disruptions. Applying security patches (updates) to address known vulnerabilities in high-availability systems presents yet another operational risk, as few sites

have representative backup systems on which to test the patches. Because of these risks of disruption, operational-unit leaders are hesitant to allow changes in their OT environment. This requires security teams to implement workarounds that are far less effective in managing risk. Adding even more risk and complexity are newer technologies such as industrial IoT devices, cloud services, mobile industrial devices, and wireless networking.

Beyond technology is the human factor, as many industries face a shortage in cybersecurity skills. The problem is worse for heavy industrials, which need to staff both IT and OT security teams and to attract talent to remote operational locations. In a 2017 report on the global information-security workforce, the cybersecurity professional organization (ISC)<sup>2</sup> predicted that the gap between qualified IT professionals and unfilled positions will grow to 1.8 million by 2022. OT security expertise is even more specialized and difficult to acquire, making it particularly expensive to staff.

### **Exposure to third-party risk**

Compared with IT, the OT environment is highly customized, as it supports a process specific to a given operation. The proprietary nature of OT equipment means that companies rely on the OEM to maintain it and make changes. This equipment is often a "black box" to its owner, which has no visibility into security features or levels of vulnerability. Furthermore, companies

# Many traditional security tools cannot be applied to the operational technology environment.

are increasingly outsourcing maintenance and operation of OT, or adopting build-operate-transfer contracts. These types of relationships require third parties to gain physical access to OT networks. Where remote maintenance is required, the owner needs to establish connections to the OEM networks. These remote connections are mostly unsupervised by the owner organizations, introducing a blind spot. Several heavy industrials have reported that third parties frequently connect laptops and removable storage devices directly into the OT network without any prior cybersecurity checks, despite the obvious dangers of infection.

Vendor assessments and contracts for OEMs often fail to include a cybersecurity review. This failure prevents companies from enforcing security standards without renegotiating contracts. Where they do conduct precontract security assessments, results are rarely pursued. OEM vendors that do have security features in their products report that operational buyers rarely want them. In some cases, even if security features are included by default, or at no additional cost, the buyer does not use them.

## Emerging solutions

Considering the complexity of these challenges, companies in heavy industrial sectors have been slow to invest in cybersecurity programs that span both IT and OT, especially when compared with manufacturing and pharmaceutical companies. The only exception is the US electricity production and distribution grid, acting in response to emerging regulation in this sector. The good news is that solutions for heavy industrials are becoming more sophisticated. Several incumbent OEM providers, and a growing number of start-ups, have developed new approaches and technologies focused on protecting the OT environment.

Leaders that deploy these solutions must first carefully consider the unique challenges and process requirements they face. They can then combine the solutions with appropriate operational changes. Below we describe the challenges they will have to address along the way and the investments that will be needed, both internally and through OEMs and start-ups, to achieve cyber maturity.

## Integrate cybersecurity earlier, across OT and IT

As companies undergo digital transformation, leaders are integrating cybersecurity earlier, in both the OT and IT environments. If heavy industrials are to manage risk and avoid security-driven delays during their digital transformations, they will need to embed security earlier in the process, with investments in developer training and oversight. At the same time, these companies should expect increased convergence between their OT and IT systems. Therefore, their investments in cybersecurity-transformation programs should span both, while they more deeply integrate their security functions into both the OT and IT ecosystems.

One way to accomplish this is to create an integrated security-operations center that covers both OT and IT, housing detailed escalation protocols and incident response plans for OT-related attack scenarios. An example comes from Shell, which is working with some of its IT networking providers and some OT OEMs to develop a unified security-management solution for plant-control systems across 50 plants.<sup>5</sup> Solutions like these enable centralized asset management, security monitoring, and compliance, dynamically and in real time.

## Improving governance and accountability for security across IT and OT

The decentralized nature of heavy industries makes it particularly vital that they integrate security into all technology-related decisions across IT and OT, and deep into different functions and business units. This integration will become even more important as they become digital enterprises. Accomplishing this will require new governance models.

For instance, mature heavy industrials have established architecture-review committees to vet new technologies introduced into the IT or OT environments, and changes to existing technologies. Emerging as a second line of defense are teams that do information risk management (IRM), including strategy, compliance, and reporting. Additionally, some companies have enlisted their internal audit function as a truly independent third line of defense.

---

<sup>5</sup> "Shell Oil Strengthening Cybersecurity," ciab.com.

But few have reached such a level of maturity. A look at four typical approaches to IT and OT security reveals that only one approach integrates security under a chief security officer (CSO) aligned with the risk function (Exhibit 1). In the first three, accountabilities are insufficiently defined. But in the fourth approach, the CSO role spans both IT and OT. The CSO reports directly to the COO, thus protecting security from IT cost cutting, and preventing security from being sidestepped by IT programs.

In this optimal approach, the CSO sets policy, creates standards, and works with process engineers to create security architectures that

incorporate operational specifics. In an ideal scenario, deployment and operation of OT security resides in plant-level functions, staffed with OT experts who are cross-skilled in security. However, this separation between policy setting and deployment can lead to misunderstandings, perhaps allowing some risks to fall through the cracks. Companies can mitigate this by creating local security-review task forces, including tenured business-unit security officers who represent the security organization regionally or locally. Metrics and reporting structures can be managed by a company-wide cyber-governance committee that reports into the board.

Exhibit 1

**Of four approaches to IT and OT security, only one integrates them, using a CSO aligned with the risk function.**

**Distribution of responsibilities, by security approach**

● Primary responsibility    ○ Shared responsibility

OT security functions	Led by a CISO, <sup>1</sup> whose location will vary, typically within IT, risk, or security department												Led by a CSO <sup>2</sup>			
	No clear direction of OT <sup>3</sup> so defaults to operations				CISO advises and has oversight, operations directs				CISO is accountable but not responsible for execution in OT				Single accountability for IT, OT; cyber is part of risk agenda			
	CISO	Ops	IT	CRO <sup>4</sup>	CISO	Ops	IT	CRO	CISO	Ops	IT	CRO	CISO	Ops	IT	CRO
Policy setting		●			○	○			●				○			○
Standards creation		●							●				●			
Security architecture and engineering		●				●			○	○			○	○		○
Execution deployment		●				●				●					●	
Operations/maintenance (within perimeter)		●				●				●					●	
Operations/maintenance (perimeter/IT interface)		○	○			○	○				●				●	
Operations/maintenance (physical security)		●				●				●			○			○
Adherence		●			○	○			○	○		○	○		○	○

- Earliest stages of maturity; OT cybersecurity ownership defaults to business units
- Decentralized policy and standard setting

- CISO advises on security policy but has little influence over operations
- Execution, operations, and maintenance with operational units

- CISO determines policy and standards centrally
- Operational units responsible for execution and operations

- CSO spans IT and OT; owns security end to end
- Collaboration between security and CRO for policy setting, architecture, adherence

<sup>1</sup>Chief information-security officer.  
<sup>2</sup>Chief security officer.  
<sup>3</sup>Operational technology.  
<sup>4</sup>Chief risk officer.

### Emerging technical solutions

To overcome difficulties in OT security, consider emerging technical solutions. Several providers focused on protecting the OT environment are bringing new capabilities to tackle issues. Although several proofs of concept have resulted in successful, large-scale deployments, the technology is still evolving quickly. As companies compete to differentiate their solutions, winners have yet to emerge. Here, however, are some solutions to consider:

- ***Firewalls to limit attackers' ability to move across the network after one section is compromised.***

Enhancements in controls at the gateway between the OT and IT networks enable companies to inspect the traffic traversing that gateway. They also automate a system's ability to execute policy changes and block newly identified threats. Best practice also calls for placing critical assets and systems in separate zones to limit the impact from a compromise; for example, a fail-safe system in a separate zone from the SCADA. Incumbent firewall providers are tailoring their solutions for OT.

- ***Unified identity and access management.***

These tools allow the company to centralize adding, changing, and removing user access to OT systems and devices. This is linked to the organization's identity-management system, providing robust authentication. This approach, pervasive in IT, has been adopted as a standard in OT environments in the US electricity sector. It reduces the risk of attack by limiting "super-user" accounts. It allows the company to trace who has access to critical assets, and it helps identify sources of attack. It also has safety applications; a Chinese power plant, for instance, uses it to allow security administrators to remotely close facility doors for improved safety management.

- ***Asset inventory and device authorization.***

These tools help keep companies aware of all devices connected to their OT network. They can identify vulnerabilities in specific devices based on the device type, manufacturer, and version. They are also used for controlling authorizations of devices and communications.

In addition to security applications, these tools can optimize efficiency and identify faults in connected devices.

- ***OT network monitoring and anomaly detection.***

A plethora of passive OT network monitoring tools have emerged that monitor traffic in a noninvasive way. These tools use machine-learning algorithms to identify and alert known threats and anomalies.

- ***Decoys to deceive attackers.*** These relatively new IT tools, tailored for OT environments, create asset and user-credential decoys and fictitious OT devices, including SCADAs, to throw off attackers.

While all these tools are useful, the organizational issues mentioned above have thus far inhibited their adoption. For one thing, security buyers have little or no influence over the OT environment. Incumbent OT OEMs, which own the relationship with the operational decision makers, have made some plays directly, and through partnerships in some verticals. However, low cyber awareness among the decision makers has thus far limited the number of such deals.

### Third-party risk management

Cost and timing sometimes interfere with a company's responsibility to assess vendor security compliance, both before the contract and on a regular basis. Sector-specific collaboration groups such as information sharing and analysis centers (ISACs) have become important in reducing these costs. For instance, the health ISAC, which includes pharmaceutical and medical-device manufacturers with large OT contingents, has implemented a tool that automates evidence collection and sector-specific risk assessments, to measure third-party vendors for security and data risk. This ISAC has also created a standardized vendor repository for evidence collected by others.

### Enablers to drive progress

Given the investment required to achieve digital resilience, and the increasing calls from business executives to get there, we have identified some important enabling factors that will help drive progress. These include increased cybersecurity



regulation (by industry groups or government), higher and smarter investments in digital resilience programs, and greater industry-level collaboration.

**Evolving cybersecurity regulations**

Among heavy industries, cybersecurity regulation is now quite limited. One potential model is emerging in the United States. An electrical-industry agency, the North American Electric Reliability Corporation (NERC), is empowered under federal law to set standards known as Critical Infrastructure Protection (CIP). These standards regulate technical and procedural controls. NERC issued 12 penalties in 2017, totaling more than \$1.7 million, and stepped up its work in 2018, issuing millions of dollars in penalties that year. One serious violation resulted in a penalty of \$2.7 million against an electric utility for data exposure by a vendor. Existing and emerging EU and UK regulations for critical infrastructure are a first step to creating consistency at an industry-wide level. However, most heavy industrial companies are struggling to develop their own standards for IT and OT security, patching them

together from numerous industry standards. As attacks on critical infrastructure continue, more regulation in this sector is likely to follow, either from industry, government, or both. This will bring a much-needed mandate for CISOs and CSOs to take action, and create a clearer path to setting consistent standards across industries.

**Higher and smarter investment in cybersecurity programs**

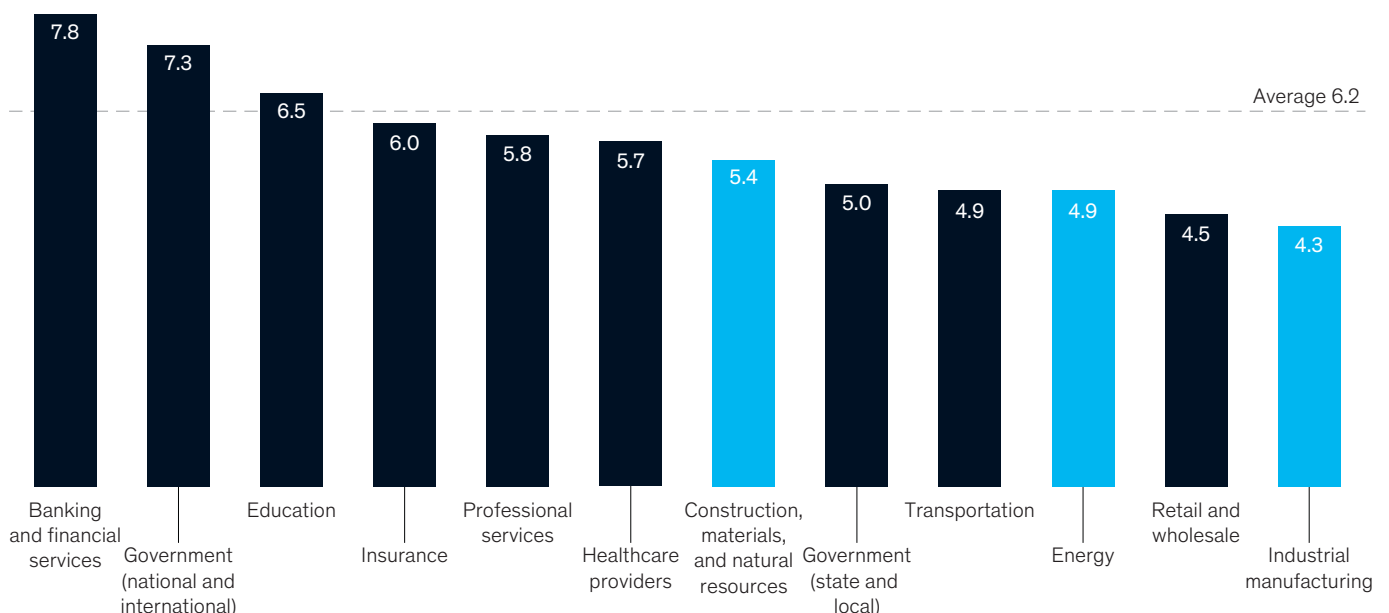
The average electrical-energy company spends just 4.9 percent of its IT budget on security, with mining coming in at 5.4 percent. This is compared with an all-industries average of 6.2 percent and financial services at 7.8 percent (Exhibit 2).

Cybersecurity-spending benchmarks are not the only factor to consider when deciding on what investment is required for a particular company. At the early stages of a cybersecurity transformation, program costs may spike before the company can reach a steady state. Spending mix is another important factor to consider. Companies at lower maturity levels tend to spend most of their cyber

Exhibit 2

**Heavy industrial companies lag behind most sectors in IT security spending.**

IT security spending as a % of all IT spending, 2017



Source: IT Key Metrics Data 2018: Key IT Security Measures: By Industry, Gartner.com, 2018

budget on compliance-driven, reactive activities. This mix changes substantially as companies mature, spending far more on forward-looking, proactive activities such as threat intelligence, hunting, and deception. Companies that conduct a comprehensive assessment of their current cyber maturity and sources of vulnerability can drive smarter long-term spending.

### **Greater industry-wide collaboration**

Knowledge-sharing initiatives have started to emerge across heavy industrial sectors, but much more can be done. Some good examples come from ISACs and other regional and sector-specific groups, which have supported rapid maturity building through information sharing, resource pooling (such as shared vendor assessments), and capability building (such as cross-sector crisis simulations). Although a few ISACs exist for heavy industrials, companies have much more to do to establish the high levels of collaboration and value seen in other sectors. Being part of a digitized, connected economy, organizations can be successful only if they apply the power of cooperation within and across sectors. Other industries such as financial services, insurance, and healthcare have built robust networks of

security professionals, using roundtables and other collaborations to address common threats and build a more secure industry for all.

Finally, it is worth noting that neither spending nor regulatory compliance are reliable indicators of digital resilience. Using the frameworks and tools we have identified in this article, companies can build that resilience by consistently applying a risk-based approach—identifying their critical assets and applying controls appropriately based on risk levels. This can then help them create cyber-transformation programs that buy down risk to tolerable levels and prioritize the activities that address the most risk per dollar spent.

---

As senior leaders set the stage for cyber transformation, they must ensure collaboration and buy-in from both security and risk professionals and the businesses. With such cooperation, companies will be truly able to transform cybersecurity, which will help keep them out of harm's way in a digital world.

**Adrian Booth** is a senior partner in McKinsey's San Francisco office, **Aman Dhingra** is an associate partner in the Singapore office, **Sven Heiligtag** is a senior partner in the Hamburg office, **Mahir Nayfeh** is a partner in the Abu Dhabi office, and **Daniel Wallance** is a consultant in the New York office.

The authors wish to thank Rhea Naidoo and Rolf Riemenschnitter for their contributions to this article.

Copyright © 2019 McKinsey & Company. All rights reserved.

**Risk Practice leadership**

Cindy Levy  
*Global*  
Cindy\_Levy@McKinsey.com

Fritz Nauck  
*Americas*  
Frederic\_Nauck@McKinsey.com

Philipp Härle  
*Western Europe*  
Philipp\_Haerle@McKinsey.com

Gabriel Vigo  
*Asia*  
Gabriel\_Vigo@McKinsey.com

Gökhan Sari  
*Eastern Europe, Middle East, North Africa*  
Gokhan\_Sari@McKinsey.com

Kevin Buehler  
*Risk Advanced Analytics*  
Kevin\_Buehler@McKinsey.com

Marco Piccitto  
*Risk People*  
Marco\_Piccitto@McKinsey.com

Holger Harreis, Olivia White  
*Risk Knowledge*  
Holger\_Harreis@McKinsey.com  
Olivia\_White@McKinsey.com

Thomas Poppensieker  
*Chair, Global Risk Editorial Board;  
Corporate Risk*  
Thomas\_Poppensieker@McKinsey.com

**In this issue:**

Transforming risk efficiency and effectiveness  
The compliance function at an inflection point  
Confronting the risks of artificial intelligence  
Derisking machine learning and artificial intelligence  
Going digital in collections to improve resilience against credit losses  
Bubbles pop, downturns stop  
Fighting back against synthetic identity fraud  
Critical infrastructure companies and the global cybersecurity threat

June 2019

Designed by Global Editorial Services

Copyright © McKinsey & Company

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

Printed in the United States of America.

