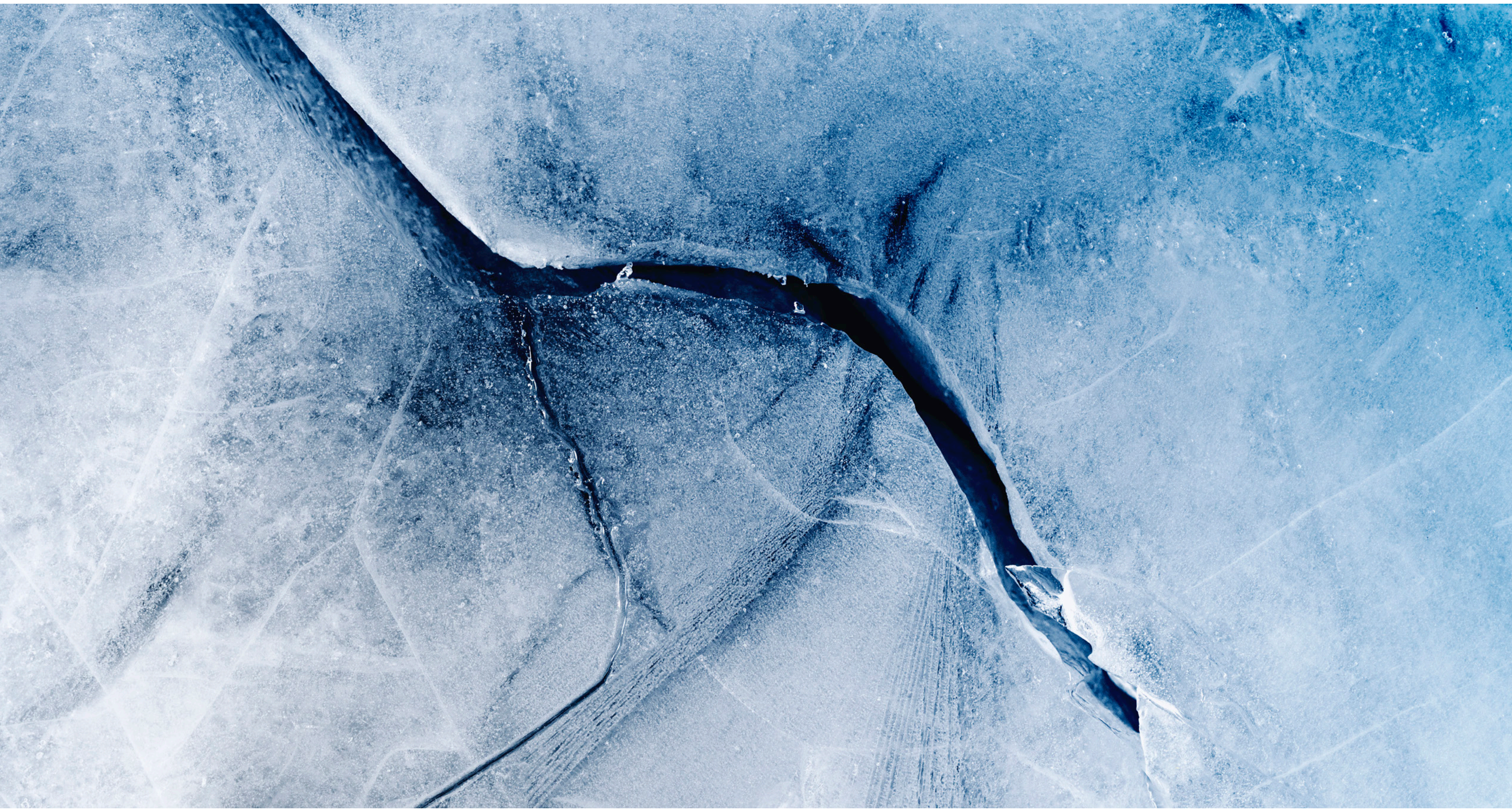
McKinsey
& Company

Risk Practice

The future of operational-risk management in financial services

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

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



© Jose A. Bernat Bacete/Getty Images

April 2020

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

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

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

The current state

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

Intrinsic difficulties

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

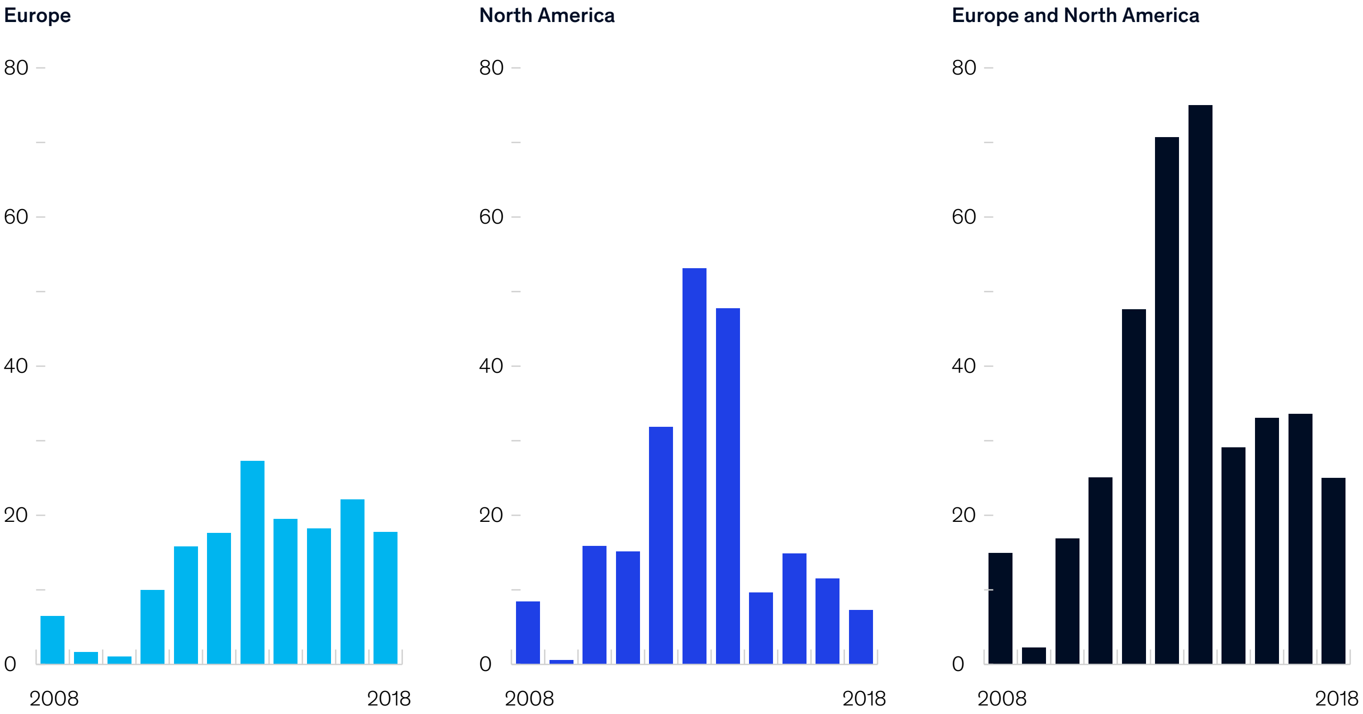
This last constraint has been lifted in recent years: granular data and measurement on operational processes, employee activity, customer feedback,

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

Exhibit 1

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

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



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

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

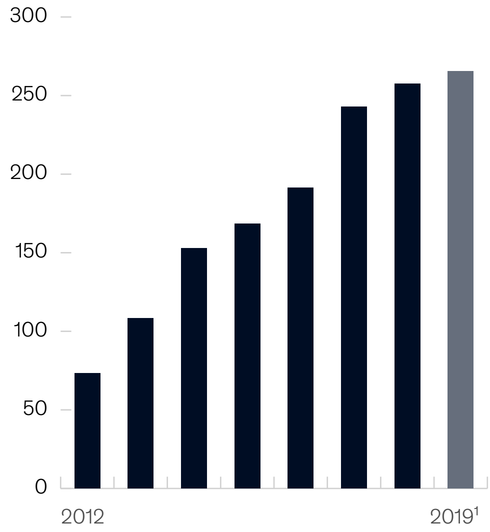
At the same time, digitization and automation have been changing the nature of work, reducing traditional human errors but creating new change-management risks; fintech partnerships create cyberrisks and produce new single points of failure; the application of machine learning and artificial intelligence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

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

Exhibit 2

Indicators of operational-risk levels continue to rise.

Complaints filed annually with Consumer Financial Protection Bureau, thousands



[1] 1st half of 2019 annualized.

Source: Consumer Financial Protection Bureau database; McKinsey analysis

Looking ahead

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

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

Defining next-generation operational-risk management

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

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

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

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

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

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

— *Map processes, risks, and controls.* Map the processes, along with associated risks and controls, including overall complexity, number of handoffs involved, and automation versus reliance on manual activities (particularly when the danger is high for negative customer outcomes or regulatory mistakes). This work will ideally be done in conjunction with systemic controls embedded in the process; end-to-end process ownership minimizes handoffs and maximizes collaboration.

— *Identify supporting technology.* Identify and understand the points where processes rely on technology.

— *Monitor risks and controls.* Create mechanisms and metrics (such as higher-than-normal volumes) to enable the monitoring of risk levels and control effectiveness, in real time wherever possible.

— *Link resource planning to processes.* Link resource planning to the emergent understanding of processes and associated needs. Be ready to scale capacity up or down according to the results of process monitoring.

— *Reinforce needed behavior.* Ensure reinforcement mechanisms for personal conduct, using communications, training, performance management, and incentives.

— *Enable feedback.* Establish feedback mechanisms for flagging potential issues, undertaking root-cause analysis, and updating or revising processes as needed to address the causes.

— *Establish change management.* Establish systematic, ongoing change management to ensure the right talent is in place, test processes and capacity, and provide guidance, particularly for technology.

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

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

Operational-risk managers must therefore rethink their approaches to issue detection. Advances in data and analytics can help. Banks can now tap into large repositories of structured and unstructured data to identify risk issues across operational-risk categories, moving beyond reliance on self-assessments and subjective controls. These emerging detection tools might best be described in two broad categories:

- *Real-time risk indicators* include real-time testing of operational processes and controls and risk metrics that identify areas operating under stress, spikes in transaction volumes, and other determinants of risk levels.
- *Targeted analytics tools* can connect the data dots to detect potential risk issues (see sidebar "Targeted analytics tools"). By mining sales and customer data, banks can detect potentially unauthorized sales. Machine-learning models can detect cyberrisk levels, fraud, and potential money laundering. As long as all privacy measures are respected, institutions can use natural-language processing to analyze calls, emails, surveys, and social-media posts to identify spikes in risk topics raised by customers in real time.

Targeted analytics tools

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

- *Anti–money laundering.* Replacing rules-driven alerts with machine-learning models can reduce false positives and focus resources on cases that actually require investigation.
- *Conduct.* Analytics engines can identify suspicious sales patterns, connecting the dots across sales, product usage, incentives, and customer complaints (for example, increases in nonactivated deposits, accounts sold by a retail banker, or trades triggered by a wealth-management adviser as they approach compensation breakpoints). Trade-monitoring analytics can mine trading and communication patterns for potential markers of conduct risk.
- *Cyberrisk.* Machine learning can analyze sources of signals, identify emerging threats, replace existing rules-based triggers, and reduce false-positive alerts.
- *Fraud.* Machine learning, including unsupervised techniques, can identify fraudulent transactions and reduce false positives; synthetic-ID-fraud analytics use external, third-party data, in accordance with all local regulation, to analyze the depth and consistency in the identity profiles of new customers
- *Process quality and regulatory risks.* Automated call surveillance using natural-language processing can monitor adherence to disclosure requirements. Systemic quality-control touchpoints can check the accuracy of decisions, disclosures, and filings against customer-provided information and regulatory rules (for example, the accuracy of a bankruptcy filing against the system of record information).
- *Third-party risk.* Models can be developed that quantify the reliance on key third parties (including hidden fourth-party exposures) to drive better business-continuity planning and bring a risk-based perspective to vendor assessment and selection.

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

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

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

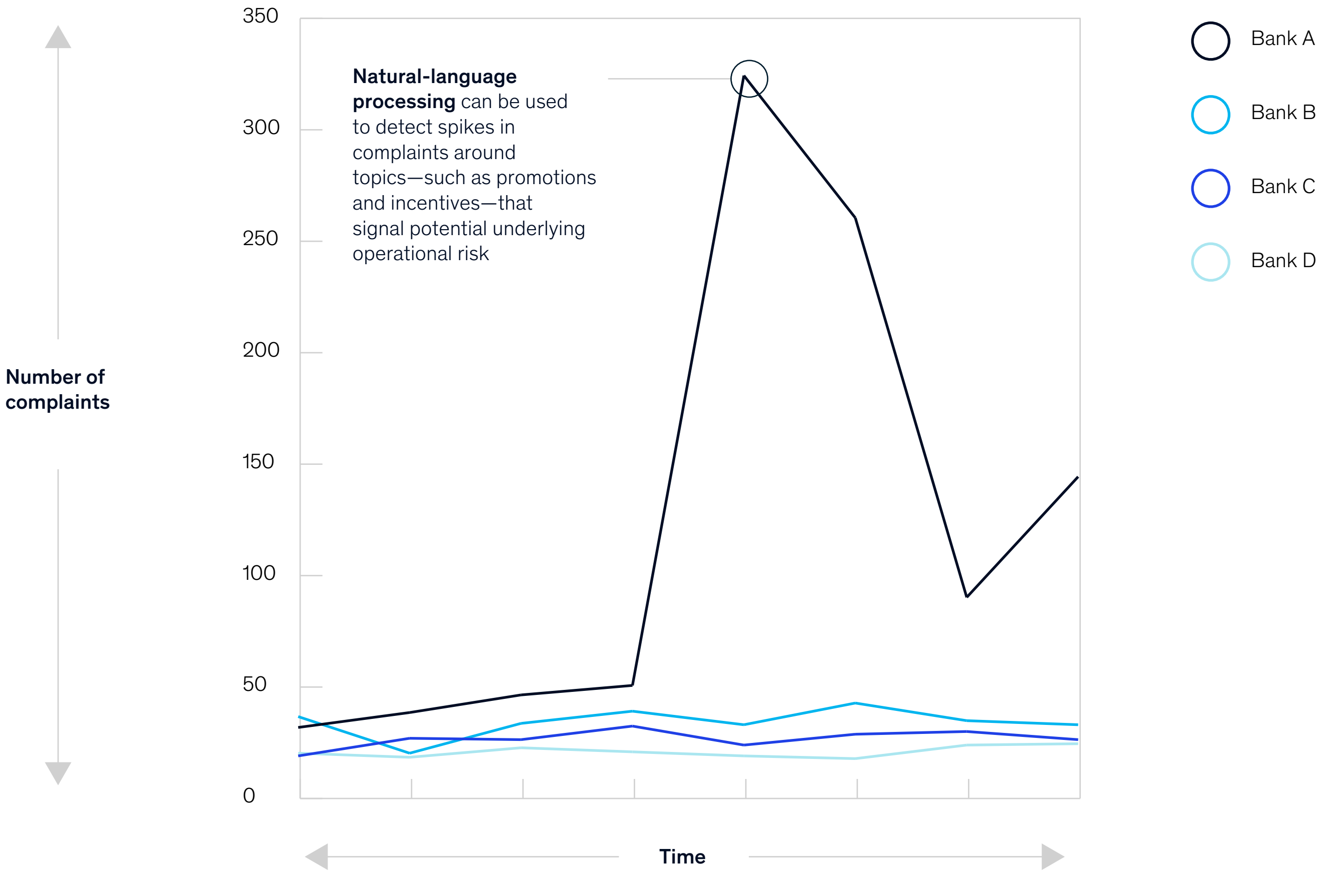
3. Develop talent and the tools to manage specialized risk types

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

Exhibit 3

Natural-language processing can help detect operational risk.

Customer complaints over time



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

Examples of specialized expertise

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

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

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

4. Manage human-factor risks

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

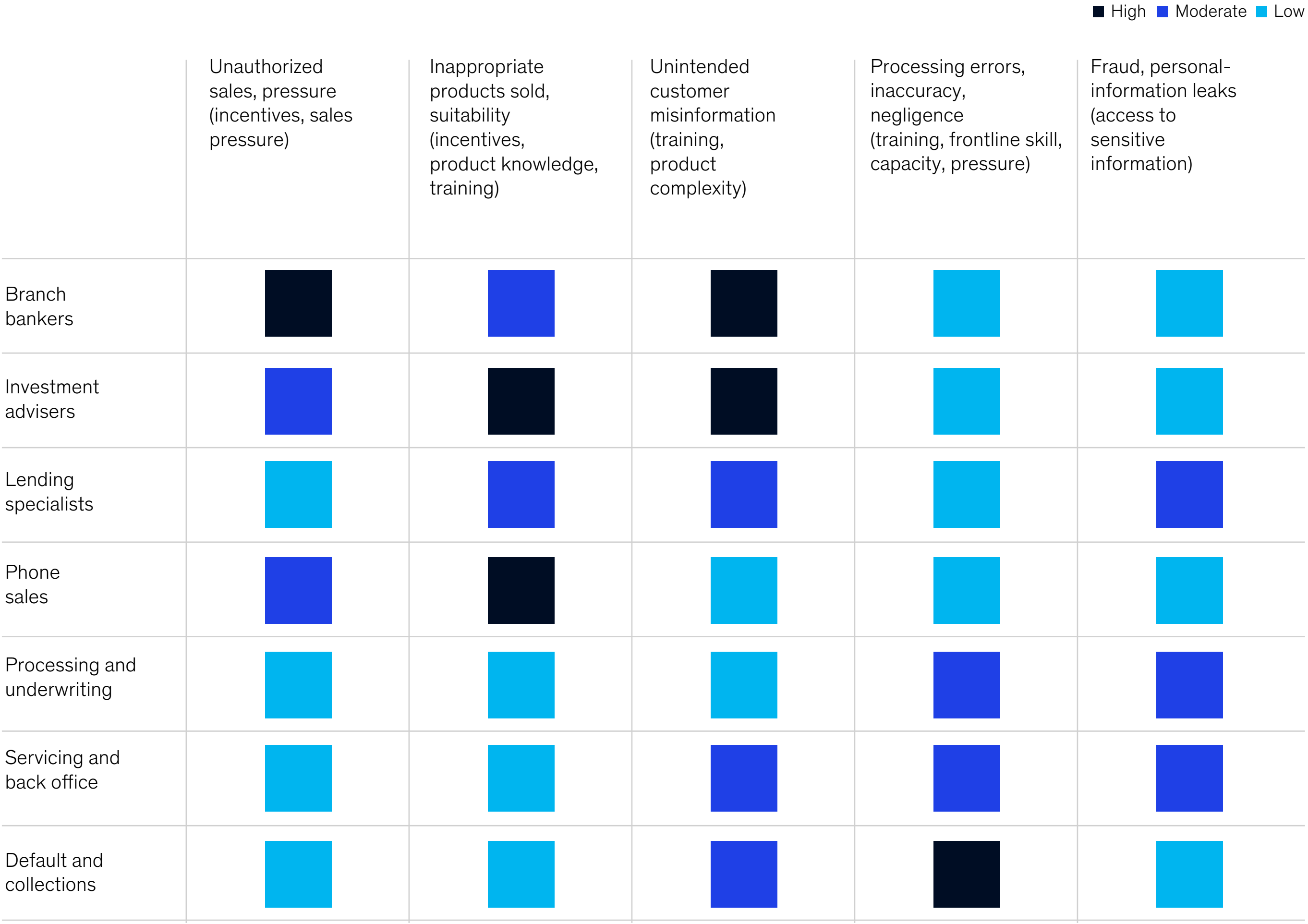
Developing effective risk-oversight frameworks for human-factor risks is not an easy task, as these risks are diverse and differ from many other operational-risk types. Some involve behavioral transgressions among employees; others involve the abuse of insider organizational knowledge and finding ways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

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

Exhibit 4

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

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



⬛ High 🟦 Moderate ◻ Low

	Unauthorized sales, pressure (incentives, sales pressure)	Inappropriate products sold, suitability (incentives, product knowledge, training)	Unintended customer misinformation (training, product complexity)	Processing errors, inaccuracy, negligence (training, frontline skill, capacity, pressure)	Fraud, personal-information leaks (access to sensitive information)
Branch bankers	⬛	🟦	⬛	◻	◻
Investment advisers	🟦	⬛	⬛	◻	◻
Lending specialists	◻	🟦	🟦	◻	🟦
Phone sales	🟦	⬛	◻	◻	◻
Processing and underwriting	◻	◻	◻	🟦	🟦
Servicing and back office	◻	◻	🟦	🟦	🟦
Default and collections	◻	◻	🟦	⬛	◻

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

A brighter future

Through the four-part transformation we have described, operational-risk functions can proceed to deepen their partnership with the business, joining with executives to derisk underlying processes and infrastructure. Historically, operational-risk management has focused on reporting risk issues, often in specialized forums removed from day-to-day assessment. Many organizations have thus viewed operational-risk activities as a regulatory necessity and of little business value. The function is accustomed to react to business priorities rather than involve itself in business decision making.

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

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

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

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

Designed by Global Editorial Services