McKinsey&Company

McKinsey on Risk

Highlights

The future of bank risk management

Nonfinancial risk: A growing challenge for the bank

'The ghost in the machine': Managing technology risk

Number 1, Summer 2016

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. Comments and requests for copies or for permissions to republish an article can be sent via email to McKinsey_Risk@McKinsey.com.

Cover photo:
© blackred/Getty Images

Editorial Board:
Kyra Blessing, Richard Bucci, Raul Galamba de Oliveira, Maria Martinez, Theodore Pepanides, Thomas Poppensieker, Kayvaun Rowshankish, Anthony Santomero, Himanshu Singh, Mark Staples

Manager of Risk External Relations: Kyra Blessing

Editors: Richard Bucci, Mark Staples

Contributing Editors:
Joanne Mason, Jonathan Turton

Art Direction and Design:
Leff Communications

Managing Editors:
Michael T. Borruso, Venetia Simcock

Editorial Production:
Runa Arora, Elizabeth Brown, Heather Byer, Torea Frey, Heather Hanselman, Katya Petriwsky, John C. Sanchez, Dana Sand, Sneha Vats

McKinsey Practice Publications

Editor in Chief:
Lucia Rahilly

Executive Editors:
Michael T. Borruso, Allan Gold, Bill Javetski, Mark Staples

Table of contents

Introduction

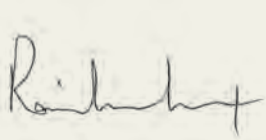
Welcome to the inaugural issue of *McKinsey on Risk*. In this compendium and those that will follow, we offer McKinsey's global perspective in the key risk areas that are affecting the performance of the world's leading companies—credit risk, enterprise risk management and risk culture, operational risk and compliance, regulation, trading and balance-sheet risk, data and technology, advanced analytics, and crisis preparedness and response.

In the aftermath of the financial crisis, companies have had to navigate business environments defined by sustained market volatility, rising regulatory levels, new technology risks, and complex geopolitical uncertainties, of which Brexit is the latest and one of the largest. On such terrain, effective risk-informed strategies become a major source of competitive advantage. To develop these strategies, top management needs a truly global and cross-functional view of risk issues. The articles in *McKinsey on Risk* will delve into the most compelling risk issues that companies in all sectors and geographies confront, presenting deep industry insights and structured risk-management approaches that have proved to be effective in lifting performance.

In this issue, we begin with an overview of the trends that are shaping the future of bank risk management; a second article looks into the management of nonfinancial risk—a risk discipline with critical implications for financial institutions. Two articles present strategies for tackling the tougher compliance environment; two more explore how banks can best manage credit risk in the face of an array of new challenges. Another article examines how enterprise-risk-management frameworks can be used to create real business value. Many of the articles analyze the risk implications of the data age; one specifically explores IT risk and the need to address it strategically, with wide organizational collaboration.

As industries and risk functions are challenged with problems of increasing technical complexity, the dangers of a siloed approach rise. A unifying theme of the insights presented in this issue of *McKinsey on Risk* is that risk is most effectively addressed in a structured way, based on an enterprise-wide view. The most successful companies are able to transform this approach into risk strategies that improve performance and create value.

We hope you enjoy these articles and find in them ideas worthy of your consideration. Let us know what you think at McKinsey_Risk@McKinsey.com. You can also view these articles, earlier articles on risk, and many others on McKinsey.com and on our McKinsey Insights app.



Raul Galamba de Oliveira
Senior partner
For McKinsey's Global Risk Practice

The future of bank risk management

Banks have made dramatic changes to risk management in the past decade—and the pace of change shows no signs of slowing. Here are six initiatives to help them stay ahead.

Philipp Härle, Andras Havas, and Hamid Samandari

Risk management in banking has been transformed over the past decade, largely in response to regulations that emerged from the global financial crisis and the fines levied in its wake. But important trends are afoot that suggest risk management will experience even more sweeping change in the next decade.

The change expected in the risk function's operating model illustrates the magnitude of what lies ahead. Today, about 50 percent of the function's staff are dedicated to risk-related operational processes such as credit administration, while 15 percent work in analytics. McKinsey research suggests that by 2025, these numbers will be closer to 25 and 40 percent, respectively.

No one can draw a blueprint of what a bank's risk function will look like in 2025—or predict all forthcoming disruptions, be they technological advances, macroeconomic shocks, or banking scandals. But the fundamental trends do permit a broad sketch of what will be required of the risk function of the future. The trends furthermore suggest that banks can take some initiatives now to deliver short-term results while preparing for the coming changes. By acting now, banks will help risk functions avoid being overwhelmed by the new demands.

Six trends

Six trends are shaping the role of the risk function of the future.

Trend 1: Regulation will continue to broaden and deepen

While the magnitude and speed of regulatory change is unlikely to be uniform across countries, the future undoubtedly holds more regulation—both financial and nonfinancial—even for banks operating in emerging economies.

Much of the impetus comes from public sentiment, which is ever less tolerant of bank failures and the use of public money to salvage them. Most parts of the prudential regulatory framework devised to prevent a repetition of the 2008 financial crisis are now in place in financial markets in developed economies. But the future of internal bank models for the calculation of regulatory capital, as well as the potential use of a standardized approach as a floor (Basel IV), is still being decided. The proposed changes could have substantial implications, especially for low-risk portfolios such as mortgages or high-quality corporate loans.

Governments are exerting regulatory pressure in other forms, too. Increasingly, banks are being required to assist in crackdowns on illegal and unethical financial transactions by detecting signs of money laundering, sanctions busting, fraud, and the financing of terrorism, and to facilitate the collection of taxes. Governments are also demanding that their banks comply with national regulatory standards wherever they operate in the world. Banks operating abroad must already adhere to US regulations concerning bribery, fraud, and tax collection, for example. Regulations relating to employment practices, environmental standards, and financial inclusion could eventually be applied in the same way.

Banks' behavior toward their customers is also under scrutiny. The terms and conditions of contracts, marketing, branding, and sales practices are regulated in many jurisdictions, and rules to protect consumers are likely to tighten. Banks will probably be closely examined for information asymmetries, barriers to switching banks, inappropriate or incomprehensible advice, and nontransparent or unnecessarily complex product features and pricing structures. The bundling and cross-subsidizing of products could also become problematic. In certain cases, banks might even be obliged to inform their customers of more suitable products with better terms than the ones they have—such as a lower remortgage rate. (Utility suppliers in some markets are already obliged to do this.)

This tightening regulatory environment makes unviable the traditional model to manage regulatory risks; the risk function will need to build even more robust regulatory and stakeholder-management capabilities. Risk functions must not only ensure compliance with existing rules but also review the entire sales-and-service approach through a broad, principle-based lens. In addition, the risk function will play a vital role in collaborating with other functions to reduce risk—for example, by working more closely with the business to integrate and automate the correct behaviors and to eliminate human interventions. The risk function's tasks will be to ensure that compliance considerations are always top of mind and not addressed perfunctorily by businesses after they have formulated their strategies or designed a new product.

Trend 2: Customer expectations are rising in line with changing technology

Technological innovation has ushered in a new set of competitors: financial-technology companies, or fintechs. They do not want to be banks, but they do want to take over the direct customer relationship and tap into the most lucrative part of the value chain—origination and sales. In 2014, these activities accounted for almost 60 percent of banks' profits. They also earned banks an attractive 22 percent

return on equity, much higher than the gains they received from the provision of balance sheet and fulfillment, which generated a 6 percent return on equity.[1]

The seamless and simple apps and online services that fintechs offer are beginning to break banks' heavy gravitational pull on customers. Most fintechs start by asking customers to transfer a single piece of their financial business, but many then steadily extend their services. If banks want to keep their customers, they will have to up their game, as customers will expect intuitive, seamless experiences, access to services at any time on any device, personalized propositions, and instant decisions.

Banks' responses to higher customer expectations will be automated: an instant response to retail and corporate credit decisions, for example, and a simple, rapid online account-opening process. For banks to deliver at this level, they will have to be redesigned from the perspective of customer experience and then digitized at scale.

Fintechs such as Kabbage, a small-business lender that operates in the United Kingdom and the United States, set a high customer-service bar for banks—and present new challenges for their risk functions. Kabbage does not require loan applicants to fill out lengthy documents to establish credit-worthiness. Instead, it draws upon a wide range of customer information from data sources such as PayPal transactions, Amazon and eBay trade information, and United Parcel Service shipment volumes. While it remains to be seen how such fintechs perform in the longer term, banks are learning from them. Some are designing account-opening processes, for example, where most of the requested data can be drawn from public sources. The risk function will have to work closely with each business to meet these kinds of customer expectations while containing risk to the bank.

Technology also enables banks and their competitors to offer increasingly customized services. It may be possible eventually to create the "segment of one," tailoring prices and products to each individual. This degree of customization is expensive for banks to achieve because of the complexity of supporting processes. Regulatory constraints might well be imposed in this area, however, to protect consumers from inappropriate pricing and approval decisions.

To find ways to provide these highly customized solutions while managing the risk will be the task of the risk function, working jointly with operations and other functions. Risk management will need to become a seamless, instant component of every key customer journey.

Trend 3: Technology and advanced analytics are evolving

Technological innovations continuously emerge, enabling new risk-management techniques and helping the risk function make better risk decisions at lower cost. Big data, machine learning, and crowdsourcing illustrate the potential impact.

- *Big data.* Faster, cheaper computing power enables risk functions to use reams of structured and unstructured customer information to help them make better credit risk decisions, monitor portfolios for early evidence of problems, detect financial crime, and predict operational losses. An important question for banks is whether they can obtain regulatory and customer approval for models that use social data and online activity.

- *Machine learning.* This method improves the accuracy of risk models by identifying complex, nonlinear patterns in large data sets. Every bit of new information is used to increase the predictive power of the model. Some banks that have used models enhanced in this way have achieved promising early results. Since they

cannot be traditionally validated, however, self-learning models may not be approved for regulatory capital purposes. Nevertheless, their accuracy is compelling, and financial institutions will probably employ machine learning for other purposes.

- *Crowdsourcing.* The Internet enables the crowdsourcing of ideas, which many incumbent companies use to improve their effectiveness. Allstate Insurance Company hosted a challenge for data scientists to crowdsource an algorithm for new car-accident insurance claims. Within three months, they improved the predictive power of their model by 271 percent.[2]

Many of these technological innovations can reduce risk costs and fines, and they will confer a competitive advantage on banks that apply them early and boldly. However, they may also expose institutions to unexpected risks, posing more challenges for the risk function. Data privacy and protection are also important concerns that must be addressed with due rigor.

Trend 4: New risks are emerging

Inevitably, the risk function will have to detect and manage new and unfamiliar risks over the next decade. Model risk, cybersecurity risk, and contagion risk are examples that have emerged.

- *Model risk.* Banks' increasing dependence on business modeling requires that risk managers understand and manage model risk better. Although losses often go unreported, the consequences of errors in the model can be extreme. For instance, a large Asia–Pacific bank lost $4 billion when it applied interest-rate models that contained incorrect assumptions and data-entry errors. Risk mitigation will entail rigorous guidelines and processes for developing and validating models, as well as the constant monitoring and improvement of them.

- *Cybersecurity risk.* Most banks have already made protection against cyberattacks a top strategic priority, but cybersecurity will only increase in importance and require ever greater resources. As banks store an increasing amount of data about their customers, the exposure to cyberattacks is likely to further grow.

- *Contagion risk.* Banks are more vulnerable to financial contagion in a global market. Negative market developments can quickly spread to other parts of a bank, other markets, and other involved parties. Banks need to measure and track their exposure to contagion and its potential impact on performance. Measures to reduce a bank's total risk can reduce its capital requirements, as contagion risk is one of

If banks want to keep their customers, they will have to up their game, as customers will expect intuitive, seamless experiences, access to services at any time on any device, personalized propositions, and instant decisions.

the main drivers for classification as a global systemically important bank (G-SIB) and for G-SIB capital surcharges.

To prepare for new risks, the risk-management function will need to build a perspective for senior management on risks that might emerge, the bank's appetite for assuming them, and how to detect and mitigate them. And it will need the flexibility to adapt its operating models to fulfill any new risk activities.

Trend 5: The risk function can help banks remove biases

Behavioral economics has made great strides in understanding how people make decisions guided by conscious or unconscious biases. It has shown, for example, that people are typically overconfident—in a few well-known experiments, for example, enormous majorities of respondents rated their driving skills as "above average." Anchoring is another bias, by which people tend to rely heavily on the first piece of information they analyze when forming opinions or making decisions.

Business, too, is prone to bias. Business cases are almost always inflated, and if the first person to speak in a discussion argues in favor of an idea, the likelihood is high that most present, if not all, will agree.

Biases are highly relevant for bank risk-management functions, as banks are in the business of taking risk, and every risk decision is subject to biases. A credit officer might write on a credit application, for example, "While the management team only recently joined the company, it is very experienced." The statement may simply be true—or it may be an attempt to neutralize potentially negative evidence.

Leading academics and practitioners have developed techniques for overcoming such biases, and various industries are beginning to apply them. Some energy utilities are trying to eliminate bias by redesigning the processes they follow in making major investment decisions, for example. Banks are also likely to deploy techniques to remove bias from decision making, including analytical measures that provide decision makers with more fact-based inputs, debate techniques that help remove biases from conversations and decisions, and organizational measures that embed new ways of decision making.

The risk function could take the lead in de-biasing banks. It could even become a center of excellence that rolls out de-biasing processes and tools to other parts of the organization.

Trend 6: The pressure for cost savings will continue

The banking system has suffered from slow but constant margin decline in most geographies and product categories. The downward pressure on margins will likely continue, not least because of the emergence of low-cost business models used by digital attackers. As a result, the operating costs of banks will probably need to be substantially lower than they are today. After exhausting traditional cost-cutting approaches such as zero-based budgeting and outsourcing, banks will find that the most effective remaining measures left are simplification, standardization, and digitization. The risk function must play its part in reducing costs in these ways, which will also afford opportunities to reduce risks. A strong automated control framework, for example, can reduce human intervention, tying risks to specific process break points. As the pressure to reduce costs will persist, the risk function will need to find further cost-savings opportunities in digitization and automation while delivering much more for much less.

Preparing for change

The six trends suggest a vision for a high-performing risk function come 2025. It will need to be a core part of banks' strategic planning, collaborate closely

with businesses, and act as a center of excellence in analytics and de-biased decision making. Its ability to manage multiple risk types while complying with existing regulation and preparing for new rules will make it more valuable still, while its role in fulfilling customer expectations will probably render it a key contributor to the bottom line. For most banks, their risk function is some way off from being able to play that role. The optimal function would have the following attributes and capabilities:

- full automation of decisions and processes with minimal manual interventions
- increased reliance on advanced analytical models to de-bias decisions
- close collaboration with businesses and other functions to provide a better customer experience, de-biased decisions, and enhanced regulatory preparedness
- strong advocacy of corporate values and principles, supported by a robust risk culture that is clearly defined, communicated, and reinforced throughout the bank.
- a talent pool with superior advanced-analytics capabilities

To put all this in place, risk functions will need to transform their operating models. How can they begin? They cannot prepare for every eventuality, but initiatives can be implemented that will bring short-term business gains while helping build the essential components of a high-performing risk function over the next decade. Here are some examples of such initiatives that can be launched immediately:

- *Digitize core processes.* Simplification, standardization, and automation are key to reducing nonfinancial risk and operating expenses. To that end, the risk function can help speed the digitization of core risk processes, such as credit applications and underwriting, by approaching businesses with suggestions rather than waiting for the businesses to come to them. Increased efficiency, a superior customer experience, and improved sales will likely be additional benefits.
- *Experiment with advanced analytics and machine learning.* In the same vein, risk functions should experiment more with analytics, and particularly machine learning, to enhance the accuracy of their predictive models. Risk functions can be expected to use these models for a number of purposes, including financial-crime detection, credit underwriting, early-warning systems, and collections in the retail and small-and-medium-size-enterprise segments.
- *Enhance risk reporting.* Ever-broader regulation and the need to adjust to market developments require rapid, fact-based decision making, which means better risk reporting. While regulatory requirements have already done much to improve the quality of the data used in risk reports and their timeliness, less attention has been given to the format of reports or how they could be put to better use for making decisions. Replacing paper-based reports with interactive tablet solutions that offer information in real time and enable users to do root-cause analyses would enable banks to make better decisions faster and to identify potential risks more quickly as well.
- *Collaborate for balance-sheet optimization.* Given regulatory constraints, balance-sheet composition is arguably more important than ever in supporting profitability. The risk function can help optimize the asset and liability composition of the balance sheet by working with finance and strategy functions to consider various economic scenarios, regulation, and

strategic choices. How prepared would the bank be, for example, if the loan portfolio were contracted or expanded? Such analyses, optimized with analytical tools, can help banks find ways to improve returns on equity by 50 to 400 basis points, while still fulfilling all regulatory requirements.

- *Refresh the talent pool.* High-performing risk functions commonly depend on a high-performing IT and data infrastructure—a central "data lake" with harmonized definitions and clear data governance, for example. Building the right mix of talent is equally important. Data scientists with advanced mathematical and statistical knowledge are needed to collaborate across the bank in the conversion of data insights into business actions. Risk managers will become trusted counselors to business areas, while traditional operational areas will require fewer staff. Attracting talented employees will itself be a challenge, as potential candidates would tend to prefer technology firms unless banks strengthen their value propositions.

- *Build a strong risk-management culture.* The detection, assessment, and mitigation of risk must become part of the daily job of all bank employees and not only those in risk functions. With automation and more sophisticated analytical and technical capabilities, human intervention is needed to ensure appropriate and ethical application.

The risk function will have a dramatically different role by 2025. To get there, needed changes will take several years, so time is already short. The actions recommended here can equip the risk function with the capabilities it needs to cope with new demands and help the bank to excel among its competitors. ■

[1] For a more detailed discussion, see *The fight for the customer: McKinsey global banking annual review 2015*, September 2015, McKinsey.com.

[2] Allan E. Alter and Jeanne G. Harris, "How to accelerate IT to the speed of business," August 27, 2012, *Wall Street Journal*, wsj.com, and Clint Boulton, "How Allstate used crowdsourcing to tune up its car insurance business," March 27, 2012, *Wall Street Journal*, wsj.com.

Download the full report on which this article is based, *The future of bank risk management*, on McKinsey.com.

Philipp Härle is a senior partner in McKinsey's London office, **Andras Havas** is an associate principal in the Budapest office, and **Hamid Samandari** is a senior partner in the New York office.

The authors wish to thank Andreas Kremer and Daniel Rona for their contributions to this article.

Nonfinancial risk: A growing challenge for the bank

With credit and market risks now under better control, the focus is shifting to nonfinancial risks. Managing these well will require big shifts in banks' practices.

Piotr Kaminski, Daniel Mikkelsen, Thomas Poppensieker, and Anke Raufuß

Banks are accustomed to taking on financial risk and generating profit from it. It is the premise of their business models. But nonfinancial risk (NFR), whether related to compliance failures, misconduct, technology, or operational challenges, has only a downside. And the downside is large.

Foremost are the financial consequences. Between 2008 and 2012, the top ten banks globally lost close to $200 billion through litigation, compensation claims, and operational mishaps.[1] At least 17 incidents racked up losses of more than $1 billion each; another 65 incidents each resulted in losses above $100 million.

Yet the direct financial consequences of NFR are not the only concern. The reputational damage wrought can hit a bank hard at a time when customers, shareholders, and public stakeholders are questioning banks' business models. And there are also the personal consequences for senior managers, whom regulators increasingly hold accountable for misconduct or failure to comply with laws and regulations.[2] All of this, and the prospect of still tighter regulation, puts considerable pressure on banks to manage NFR better.[3]

Many have already invested heavily to do so, boosting head counts, creating new governance structures, and making operational improvements to control risks related to compliance, fraud, and IT. Yet the mitigation of NFR remains elusive. Much time is spent firefighting and remediating audit findings, yet too often there is no warning of when or where the next risk might materialize.

An important factor underlying this is a fuzzy definition of the responsibilities between the first line of defense, in the businesses, and the second-line control functions. In addition, control functions are siloed, each having its own risk-identification processes, reporting structures, and IT systems.

The result is duplicated work as well as costs. Banks feel they are drowning in parallel efforts aimed at identifying, assessing, and remediating risks, with the same individuals being approached over and over again, and diluting scarce resources and attention from running the business. Inevitably, the chief risk officer and his or her operational-risk unit struggle to provide the board and regulators with a thorough view of risks faced and controls required.[4]

Against this backdrop, many institutions seek a more integrated NFR-management approach in order to reduce the risk of further failures, meet stakeholders' requirements and expectations, and limit costs. This article describes the three key components of such an integrated approach: an enhanced governance framework, a set of enablers, and changes in the front office's approach and mind-set. It is based on our work with many financial institutions globally and an informal survey of 15 global and regional banks. Some of the structures and ideas we outline here are familiar to banks from their work on financial risk; many are newly conceived for the management of nonfinancial risk. Taken together, a full implementation of these concepts represents a paradigm shift in the NFR-management practices of many banks today.

An enhanced NFR-governance framework

In line with regulatory expectations, banks are building a governance model with three lines of defense. The first line owns and manages risks, the second line sets control standards and monitors adherence to them, and the third line—audit—checks on the adequacy of the first two.

Whereas all institutions regard the business divisions as the first line of defense, some overlook the role of central-infrastructure areas, such as IT and operations. These central areas do not take on financial risks from the balance sheet, but they are where the risk of most operational failure resides. Hence, many banks have extended the definition of the first line to include them.

In addition, they have broadened their definition of the second line beyond the risk and compliance functions to include areas such as legal, HR, finance, and tax, recognizing their role in managing the institution's control framework in their respective areas of risk expertise. Take legal. Like credit risk, it is often directly involved in business transactions, advising on and approving legal structures. HR, meanwhile, often sets and monitors policies on hiring, promotions, and compensation.

How a bank chooses to delineate first- and second-line activities in these areas might vary—there is no one-size-fits-all approach—but it is essential that the bank defines a consistent set of principles that reflect its governance structure, operational complexity, and specific regulatory requirements. These principles need to be permanent enough to guide future adjustments to the organization and operating model. They should clarify the organizational separation of the first and second lines to ensure independent control by second-line areas, while permitting them to perform activities as adviser or servicer. This is culturally important, so that second-line areas are seen as vital to the bank's business model.

The principles also need to emphasize the importance of first-line areas taking responsibility for NFR management, rather than focusing entirely on revenue or cost management. To be sure, given the complexity of managing controls consistently across the bank while meeting regulatory standards,

the first line may need additional expertise. For example, dedicated control units can help senior management identify and design improvements. Balanced scorecards, which measure control effectiveness and review thresholds and penalties for breaching them, can also help. Ultimately, the principles must promote a change in the organization's thinking so that risk management and controls are at the front of senior management and employees' minds.

Once they are agreed, the risk-governance principles need to be shared across the organization and formalized as part of the risk-policy framework, while the chief risk officer ensures their consistent application.

The role of the board

Despite recent improvements, many bank boards do not routinely consider NFR management, engaging only in some firefighting when risk controls fail. They can increase their engagement in various ways. Quarterly board meetings or a board committee dedicated to risk control are options. The meetings will need to provide auditable proof of appropriate risk-taking and risk-management decisions in line with the board's regulatory and legal accountability. Their quality will depend on input from both first and second lines and, crucially, on action-oriented reports on nonfinancial risk that align to a clear definition of risk appetite.

These meetings and reports are required so that boards can build a forward-looking perspective of the bank's top risks (and challenge the bank's risk profile), to assess the adequacy of the overall control system to keep the bank within its agreed risk-tolerance boundaries, and to ensure that any control gaps are addressed.

To these ends, the reports should consolidate risks by business and type of risk, and aggregate the following information:

1. *A set of quantitative risk indicators* that can be monitored to ensure the bank's tolerance of risk is not breached. These might include the history of operational losses as the basis for capital quantification, as discussed later, but can be more business specific, ranging from employee turnover (if the ability to recruit and retain is regarded as a top risk) to the number of customer complaints (if compliance is regarded as a priority risk).

2. *A record of major incidents and near misses,* and their impact in terms of financial losses or capital implications. The report should analyze the causes of such incidents, state what lessons have been learned, and indicate where similar incidents might occur elsewhere in the organization. This process can be augmented by scenario analysis.

3. *The results of risk and control assessments and internal and external audits,* highlighting control effectiveness and critical control themes.

4. *The status of efforts to reduce risks,* be they better controls or business adjustments—such as exiting certain businesses or improving processes—or an indication of new controls that might be needed as a result of regulatory change. Timelines for implementation should be clear.

Risk-management enablers

Banks have a standard set of tools and processes in place to manage NFR, but they are not always up to the job of managing risk effectively. Good NFR management depends on four elements: an integrated risk taxonomy, a control framework focused on prevention, an integrated risk and control assessment that considers emerging risks, and a quantitative assessment of risk.

An integrated risk taxonomy

If NFR management is to be integrated, all parties must speak the same language. Yet it

is common for second-line functions to use different taxonomies with overlapping types of risk and different definitions of those risks. This creates inconsistencies when applied in different risk assessments and reports or used to assign responsibilities. The number of taxonomies within an institution can easily exceed a dozen and may contain several hundred risk definitions. Consolidation into a single taxonomy can reduce the number of risk types to around 100, which in larger institutions can then be assigned to about a dozen second-line functions.

A control framework focused on prevention

It is important to be deal with risk efficiently when it arises. More important still is to prevent it materializing in the first place. There are two main ways banks can improve their control frameworks to achieve this. First, wherever possible, they should move controls upstream. Rather than relying heavily on reconciling data downstream between finance and risk, for example, they should ensure error-free data capture in their front-office systems from the outset. And rather than having the back office sample-test trades, front-office systems should automatically check trader mandates to prevent a trade being generated if a product or asset class is not approved for a specific trader or desk.

Second, banks should map risks along entire value chains and processes in order to understand where they might lie and their interdependencies. For example, the front office needs to be aware of all risks that can result from trading complex products because of the manual work-arounds that may be necessary to process them in downstream systems.

This end-to-end business view should also enable banks to review their business complexity in the light of control requirements. Controls might be unnecessary if underlying processes and systems or product complexities are addressed in ways that improve the robustness of the business model—which would also reduce the cost of control.

An integrated and forward-looking risk and control assessment

The evidence of audit findings and risk incidents calls into question the comprehensiveness and effectiveness of internal control frameworks. A rigorous assessment of the adequacy of controls will examine the following elements:

1. *A clear breakdown of the organization and its activities into assessment units.* These units should reflect the management structure and provide an end-to-end view of value chains within the bank's operating model.

2. *Common components.* These should include risk and control taxonomies, definitions of risk materiality, and a common aggregation logic. These should be defined for each risk type by the responsible second line.

3. *A common set of control attributes.* These serve as evidence for the design and implementation effectiveness of controls and can include characteristics such as the frequency of controls, the level of automation, and whether they aim to prevent or detect risk events.

4. *A clear governance structure across first and second lines.* Responsibility for identifying, assessing, validating, and reporting on risks and controls should be assigned clearly.

5. *An integrated management information system for first and second lines.* This houses assessments and provides a consistent reporting base by division and risk type.

Assessments also need to consider emerging risks. Traditional risk assessment (especially of

operational risk) often looks at avoiding risks that have led to losses in the past. But it is a reasonably safe bet that many of the risks that will trip up banks in the future are not yet on their radar. Some incidents, such as benchmark manipulation, were not identified because the assessments carried out at the time did not consider these activities specifically. To identify similar risks, systematic business reviews—not just once-a-year, group-wide assessments—are necessary. Leading banks monitor developments in other companies and even other industries for clues as to where new risks might arise, while deploying quarterly senior-management think tanks and mechanisms that encourage employees to flag risks.

These frameworks can help banks move away from the current fragmentation that sees different reports for operational risk, legal risk, conduct risk, and so on. Too often, top management is presented with hefty documents full of risk data from the various functions and a sea of red-amber-green assessments denoting the level of risk in what might be 100 different risk categories, in 50 business lines, and across 2,000 processes. This makes it hard to prioritize. Is a red flag for market manipulation in foreign-exchange trading more important than one for potential money laundering in wealth management, for example? It is also difficult for senior management to recognize patterns across units or types of risk, or to conduct root-cause analysis.

Transparent, aggregated reporting and active management involvement remain key challenges. Regulators tend to spot inconsistencies when reporting is fragmented; more important, they question whether senior management has an aligned view of its major risks and has lined up the appropriate remediation efforts and investments.

A quantification of nonfinancial risk

What gets measured gets managed. Hence, high-quality quantification of NFR is a great enabler of better risk management—at lower cost.

Unlike credit or market risk, where exposure is relatively easy to quantify at the level of each transaction and on aggregate, measuring NFR is hard, and few banks have tackled it sufficiently. Those red-amber-green assessments that banks use are often too imprecise for management purposes, even when combined with complex internal models for calculating capital requirements.

Several approaches to improving the quantification of NFR are gaining ground. A foundational element is to identify quantifiable risk indicators, such as error rates, linked to the top risks a bank faces. If selected appropriately, these indicators capture the true drivers of NFR exposure and the quality of controls, in turn providing a more robust foundation for risk assessments, scenario analysis, risk-appetite definition, and capital calculations.

Accurate capital quantification is also important, especially given the growing levels of risk-weighted assets banks are obliged to hold to cover operational risk. However, the advanced internal models

many banks currently use to calculate regulatory capital requirements have a mixed record. While arguably better than approaches based on income and balance-sheet metrics, they are complex and volatile, and at times unable to capture risks (or their drivers) at a sufficient level of detail. There are ways to ameliorate these issues by, for example, modeling at lower confidence intervals and tying the approach to quantifiable risk indicators. However, institutions need to consider the costs and benefits of making such improvements, not just today but also in light of regulatory developments (such as the Basel Committee's proposal to abolish the use of advanced internal models for calculation of Pillar 1 capital requirements for operational risk).

Stress-testing models are growing in importance and can provide valuable additional perspectives, especially as they take into account macroeconomic conditions, and can incorporate forward-looking scenario analysis.

Finally, advanced analytics, such as machine learning, combined with the analysis of a broader range of data than traditional loss databases (including country-specific legal-loss and fraud statistics, as well as voice, chat, and social-media data) hold great promise for better NFR management (and potentially capital calculation). Leading banks are using these methods to catch unauthorized behavior on trading floors and in branches, reduce employee turnover, improve hiring decisions, reduce fraud rates, and reduce both "false negatives" and "false positives" in their money-laundering screening processes. That means better detection of suspicious transactions with far fewer resources.

NFR in the business

Even as banks change their approach to risk management to account for NFR, so they must also make a couple of changes in the business. One is a more structured and strategic approach to the remediation of risk. The other entails cultural change.

Remediation

Almost every bank has been asked by regulators to fix problems and close gaps in their approach to NFR. In many cases, these remediation efforts are so numerous and so extensive that they take on a life of their own and seem to occupy nearly as much management attention as the core business. To avoid more remediations, banks should take three steps. For a start, they must actively engage the businesses, to identify areas where business complexity or footprint leads to unnecessarily high risks that should be addressed at the source, rather than adding costly controls.

Second, control remediation efforts have many interdependencies and often implicate several change projects. Banks need effective governance structures led by senior business managers to provide direction to remediation efforts and align them with the second line. Finally, banks should also strive for a good balance between cost reduction and control enhancements.

All of this requires a lot more participation by business leaders than in the past. These leaders may need additional expertise from control groups in the first line, to work with the second line to establish control environments, translate these into the business context, assess and monitor risk in the front office, and define and prioritize control enhancements.

The chief risk officer too has a role to play, in develeloping a groupwide understanding of the remediation efforts and establishing credibility (to senior managers, shareholders, analysts, and regulators) on the health of the control system and the adequacy of the risk profile.

Culture

However strong the risk framework might be, NFR management will fall short unless it is supported by a culture that acknowledges its importance, as not all risks can be controlled. Recognizing this, regulators pay specific attention to risk culture.[5]

Company values and norms therefore have to be communicated, and backed up by measures such as awareness training, incentive systems, and sanctions. Performance assessments also need to take it into account.

Senior-management involvement and role modeling will be especially important. Experience shows that in organizations where senior managers take the lead in NFR management, a strong risk culture emerges. If it is delegated down the ranks and senior managers focus instead on revenue generation or cost control, the message received is that what matters most is short-term performance.

The second line has a role to play in cultural change. Senior employees in compliance and operational risk often come from a quantitative, legal, or audit background, and can be seen by business managers as a hindrance rather than as adding value. This perception can be changed if they improve their understanding of the business by, say, spending more time on the "shop floor." Rotation of people with a business background into second-line functions is another way to bring about cultural change. Some banks require senior managers to rotate in this way before being promoted further.

■ ■ ■

The management of nonfinancial risk is complex and evolving, and banks around the globe are at different starting points. The size and complexity of an organization will influence its approach. Some might begin by building capabilities: training senior managers on the front line, for example. Others might overhaul those processes where they detect the highest risks. Or they might decide to embark on a major organizational realignment. Regulatory requirements will no doubt influence the approach as well as the speed of implementation. But whatever the approach, the prize of an integrated NFR-management framework is not only regulatory compliance but also significant business benefits in the form of lower risk and lower costs, as well as the protection of senior management with respect to their personal liabilities. A prize indeed. ■

---

[1] The Conduct Costs Project, CCP Research Foundation, ccpresearchfoundation.com.

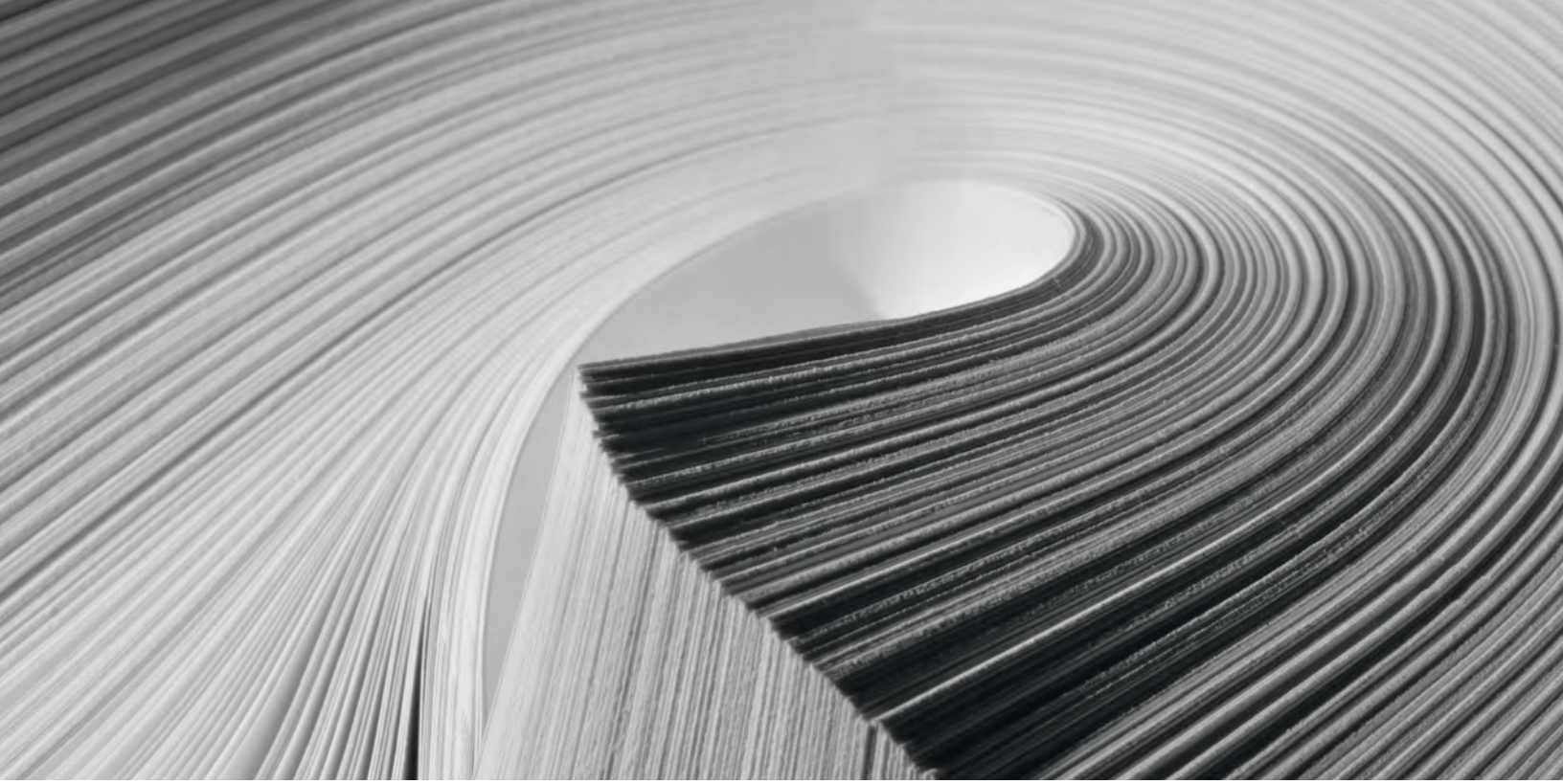
[2] See, for example, the Bank of England Prudential Regulation Authority's Senior Managers Regime, bankofengland.co.uk.

[3] As an example of possible tighter regulation, the Basel Committee on Banking Supervision proposes to remove the advanced measurement approach and replace it with a standardized measurement approach. By our estimate, the impact would be to increase European banks' capital requirements by 70 to 80 percent, while US banks would see a much smaller increase because, on average, they already hold more capital for operational risk.

[4] See, for example, *Corporate governance principles for banks*, Basel Committee on Banking Supervision, July 2015, bis.org; *OCC guidelines establishing heightened standards for certain large insured national banks, insured federal savings associations, and insured federal branches; integration of regulations*, US Office of the Comptroller of the Currency, September 2014, occ.treas.gov; and *EBA guidelines on internal governance (GL 44)*, European Banking Authority, September 2011, eba.europa.eu.

[5] See Eric Lamarre, Cindy Levy, and James Twining, "Taking control of organizational risk culture," February 2010, McKinsey.com.

Piotr Kaminski is a senior partner in McKinsey's New York office; **Daniel Mikkelsen** is a senior partner in the London office, where **Anke Raufuß** is a partner; **Thomas Poppensieker** is a senior partner in the Munich office.



Compliance in 2016:
More than just following rules

The traditional approach is losing effectiveness. Banks must turn the page and build a new model.

Piotr Kaminski and Kate Robu

The tougher compliance environment has not only multiplied the various regulations that financial institutions must follow but has also made it necessary for banks to think about compliance in an entirely different way. Those that throw out the old playbook and adapt to this new reality may enjoy a distinct competitive advantage.

Since 2009, regulatory costs have increased dramatically relative to banks' earnings and credit losses. More important, the scope of regulators' focus continues to expand, with new issues emerging and getting more attention. They include conduct risk, the quality of banks' corporate and risk culture, the next generation of anti-money-laundering measures, and third-party risk management. Banks, as they must, have continued to respond to these immediate pressures.

But the industry also needs to implement more structural changes in its compliance processes to make its risk and internal-control frameworks more effective and sustainable over time.

The traditional model for bank compliance was designed in a different era for a different purpose. An institution's compliance professionals would operate largely in an advisory capacity, having less to do with identifying and managing risks. Rather, they would lend their insight to higher-level executives, resulting in inconsistent influence on actual business practices.

Under this model, the compliance team has a limited understanding of business operations and underlying risk exposures. As a result, many banks still operating this way struggle with fundamental

control issues in the first line of defense, such as compliance literacy, accountability, performance incentives, and risk culture. Compliance activities tend to be isolated, lacking a clear link to the broader risk-management framework, governance, and processes. More often than not, the net result is a dramatic increase in compliance and control costs, with either limited or unproven impact on a bank's lingering risks.

To turn the page and enable a more sustainable compliance model, banks should consider these four principles.

Own the risk-control framework

In most cases, banks need to transform the role of the compliance department from serving in an advisory function to having direct influence on risk management and monitoring. In practice, that means becoming an active co-owner of risks and providing independent oversight of the control framework. Given this evolution, compliance specialists now must focus on these four responsibilities: having an independent and objective perspective on the quantum of residual compliance risk; translating laws, rules, and regulations into specific operational requirements; requesting and approving remediation activities; and shaping the bank's overall risk culture and literacy.

These expanded responsibilities require an unprecedented level of insight into business practices, necessitating new compliance practices such as incorporating process walk-throughs into risk assessments, monitoring significant operational changes, and developing residual-risk metrics and markers.

Integrating a common compliance vision into an institution's separate business units is also increasingly important. Institutions should stop thinking about different compliance risks as being embedded just within individual business units. That silo model should shift to one where business-unit coverage is combined with horizontal expertise around key compliance areas.

Focus on what's getting through the cracks

A common compliance practice is to mandate business-led identification of high-risk processes, as well as all risks and all controls that pertain to them. But this approach falls short of achieving transparency into all material-risk exposures. It often becomes merely a mechanical exercise, resulting in lengthy, qualitative, and indiscriminate lists of risks and controls instead of identifying material-risk exposures and their root causes. Essentially, this model means a bank's understanding of the residual risks, which might be getting through the cracks, is insufficient.

The new compliance approach needs to focus instead on residual-risk exposures in order to ensure that no material risk is left unattended and then enable effective corresponding oversight and remediation. It should tie regulatory requirements directly to specific process break points by defining which risks apply to a given business process, identifying exactly where they could occur and why, and defining objective key risk indicators in the areas where a process creates material residual-risk exposure.

Tie compliance to operational-risk concerns

A modern compliance framework must be integrated with the bank's operational-risk view of the world.

Integrating the management of these risks offers tangible benefits. It ensures a comprehensive coverage of risks, lessens the burden on the business and the control functions, and facilitates a more efficient allocation of enterprise resources and management attention.

Banks can start this journey by developing an integrated inventory of operational and compliance risks; standardizing risk, process, product, and

control taxonomies; coordinating risk assessment, remediation, reporting methodologies, and calendars; and clarifying roles and responsibilities among control functions for each material-risk type to ensure there are no gaps or overlaps.

Some banks are also making changes in the organizational structure and placement of the compliance function. A few global banks have moved compliance under the supervision of the risk department, which reinforces the view of compliance as a control function rather than an advisory function and facilitates an integrated view across all risk types.

Monitor and measure progress from the top down

The three previous principles help in executing a multifaceted compliance transformation. But banks can maximize the impact of a new compliance approach by rigorously monitoring how progress is meeting desired outcomes. A clear tone from the top and active board oversight in measuring the success of a more structural compliance system are important. An institution should monitor progress in raising the stature of compliance, creating an integrated view of all risks, achieving a strong risk culture, driving risk ownership, employing a risk-based program to assess compliance risks, using quantitative metrics and qualitative markers to measure compliance risk, and ensuring that the first line of defense is taking action and owning compliance and control issues. ■

This article appeared in *American Banker* on January 27, 2016, and is reprinted here by permission.

Piotr Kaminski is a senior partner in McKinsey's New York office, and **Kate Robu** is a partner in the Chicago office.

The authors wish to thank Andreas Kremer and Daniel Rona for their contributions to this article.

The evolving role of credit portfolio management

Banks can no longer manage loan books in isolation. A new survey reveals how portfolio managers are dealing with growing complexity.

Luis Nario, Tamara Pfister, Thomas Poppensieker, and Uwe Stegemann

Credit portfolio management (CPM) is a key function for banks (and other financial institutions, including insurers and institutional investors) with large, multifaceted portfolios of credit, often including illiquid loans. Historically, its role has been to understand the institution's aggregate credit risk, improve returns on those risks—sometimes by trading loans in the secondary market, and hedging—and identifying and managing concentrations of risk. In contrast to traditional origination and credit risk-management functions that look only at individual deals or borrowers, CPM looks across the entire credit book.

The financial crisis of 2007 changed the way most functions at these institutions operate, and CPM is no exception. The historical role of CPM remains. However, new regulatory requirements, especially with respect to capital and liquidity, increasing cost and margin pressure, and changed market conditions have pushed CPM into a broader role with the need to align closely with other areas, such as finance, treasury, risk data and methodology, and business-origination functions.

To understand exactly how the role of CPM is evolving, McKinsey, in collaboration with the International Association of Credit Portfolio Managers (IACPM),[1] conducted a survey of 41 financial institutions around the world (see sidebar, "About the survey"). We asked what changes were afoot, what CPM's mandate should be, how it should be organized to deliver on that mandate, and what tools and analytics were required. We discovered that there is broad agreement on the need for change—and change is under way in many institutions. Just as there has

never been a unique template for the CPM function, there is no consensus on how it will evolve. Much will depend on the institution and its business model. The results point, though, to certain trends. And they highlight the choices that senior managers in banking, asset management, and insurance will have to make to adapt and shape their CPM functions for high performance.

Why CPM's role is evolving

While several factors came to light, institutions identified three main reasons for the changes in CPM's role.

Capital and liquidity constraints

Some 85 percent of institutions surveyed said that regulations relating to the levels of capital and liquidity that banks must hold—and the prospect of even tighter regulation ahead—were the main reason. Institutions need to restructure their balance sheets to achieve required target ratios, optimize the use of capital, and help drive profitability. As the largest component of the balance sheet is typically the credit book, they are looking to draw on CPM's unique portfolio-management expertise, and to encourage CPM to influence loan origination as well as asset sales.

McKinsey analysis shows that many of the world's top 150 banks by assets, especially in Europe, hold only a little more capital than the "fully loaded" minimum requirements of Basel III. In some cases, depending on the nature of their business, banks may face a significant capital shortfall under the provisions of the so-called Basel IV rules, driven by regulations currently under consultation, such as a changed credit risk standardized approach, new internal-ratings-based approaches, and potential capital floors. Another complication for CPM is the multiplication of different and sometimes contradictory requirements (such as the rules on risk-based capital minimums, which are at odds with the leverage-ratio rules). The thicket of rules requires institutions to keep an eye on many constraints simultaneously, and renders a single measure of return on capital misleading.

This is a significant change. Until recently, CPM teams could manage the loan portfolio largely independently from the rest of the balance sheet. Funding and leverage were not an issue for CPM. The team was free to manage for return on equity. Now, with all the multiple requirements in play (including rules on capital, funding, liquidity, and leverage), credit, the largest asset class on most balance sheets, is front and center in the new approach to integrated balance-sheet management.

Increasing cost and margin pressure

Weakening margins add to the pressure exerted by the regulatory demands and make optimization of scarce resources particularly urgent. Some 59 percent of surveyed institutions named the resulting cost and margin pressure as a motive for

About the survey

- Participants included 39 banks and 2 insurance firms.
- North America accounted for 41 percent of the sample, Europe for 41 percent, Asia–Pacific for 13 percent, and South America for 5 percent.
- More than half of the 41 institutions have a total balance sheet greater than $500 billion, while almost a fifth have balance sheets of less than $100 billion. The remaining 30 percent are in between.
- Sixty-five percent of institutions use the internal-ratings-based (IRB) advanced approach, 10 percent the IRB-foundation approach, and 5 percent the standardized approach. Twenty percent of respondents are not subject to Basel requirements.

CPM's evolution. The issue is most significant in Europe, where 71 percent of participants named cost pressure as a factor. From 2010 to 2015 the cost-income ratio of the 150 largest institutions in Europe increased from 59.1 percent to 65.6 percent, while the income-asset ratio was essentially unchanged.

Changing market conditions

Postcrisis market conditions are a third dimension in the evolution of CPM, though less important than rising capital needs and cost pressures: only about 40 percent of surveyed institutions felt that this is a key driver for change. Significantly reduced opportunities for hedging and secondary trading, low risk appetite for going long credit in secondary markets, and lack of acceptance of going short credit exposure generally have led to a shift of focus toward portfolio management at the point of origination.

For example, activity in securitization markets and single-name credit-default swaps (CDS), CPM's main hedging tool, have declined significantly because of higher costs and stricter rules for CDS. According to the Bank for International Settlements, single-name CDS outstanding had a global notional value of $18.1 trillion in the second half of 2010. By the second half of 2015, this had more than halved to $7.2 trillion.[2] Multiname CDS, a useful tool for managing portfolios and correlations, have also been hard hit by changing bank-capital rules. Here too, volume more than halved over the same time period, from $11.8 trillion to $5.1 trillion. To get rid of unwanted exposures, CPM units often look to bundle similar assets. But securitizations in Europe declined by more than 50 percent since 2010 and are still below 2007 levels.[3] In the United States, securitization volumes have rebounded slightly, starting in 2010.

In this context, CPM has had to rethink its main job, of mitigating risk within the portfolio and maximizing risk returns.

How the role of CPM is evolving

Together, these three factors are altering CPM's mandate, the tools it needs to carry out that mandate, the way in which it works with the rest of the organization, and its data requirements. Most banks and other institutions are good at originating, structuring, and pricing risk, but not as good at holding volume on their balance sheet. That has to change—even as banks wrestle with an urgent challenge to substitute interest income with fee income. CPM has to revamp its offering for banks' changed circumstances.

A broader role in balance-sheet management

Once largely focused on the loan book, in many institutions CPM is now managing the entire range of credit exposures and their effect on the balance sheet. With that, CPM functions are also conducting new activities. For example, 54 percent of respondents said they already observed a change in the scope of the function and the tasks it was conducting, with an increasing focus on loan origination, expanded analytics (for example, on deposits and client profitability), use of additional metrics (such as the leverage ratio), more explicit alignment with risk appetite, and additional legal entity reporting.

There is, however, no single template for that extended role. In Europe and Asia–Pacific, most institutions (up to 80 percent) expect CPM to assume an active, first-line role in managing the portfolio, taking responsibility for reducing credit risk and optimizing the balance-sheet structure to secure the highest return on equity or return per risk within the constraints of regulation. This might include, for example, a closer alignment of the credit portfolio with the particular funding strategy (asset-backed funding, securitization, syndication, and so on).

In North America, an advisory, second-line role is more common, in which CPM ensures compliance with risk limits and risk-appetite constraints, assesses market opportunities and capital requirements, offers a perspective on stress testing and its strategic implications for the lending portfolio, and recommends actions to business leaders. An essential component of CPM's contribution is a superior market perspective and the capability to identify business opportunities. Seventy-six percent of North American respondents foresee the role in this way.

The design choice appears to be driven by historical precedents, market context, management priorities and regulatory emphasis; the size of the institution is also a factor. In the United States, for example, we think that the Comprehensive Capital Analysis and Review might push CPM into an advisory role because of the expertise required for stress testing. In Europe, where liquidity is tighter, more active portfolio management might be required. In addition, the survey shows that smaller institutions tend to favor a second-line CPM function, while larger ones often choose a more active role for the function, with direct market access.

But whatever the design choice, an essential component of the evolving function—if it is to fulfill its value potential—is the aggregation of risk and funding information from across the organization in order to make strategic decisions or proffer strategic advice while providing oversight and control.

An enhanced management framework and tool set

To carry out its new mandate and earn the right to participate in strategic decisions—an important component of the potential value CPM can contribute to an institution today—will require superior analytics and a new management framework. Survey respondents identified tools for measuring regulatory capital and capital allocation (that is, discipline at origination) as the most important for the CPM function, and growing in importance; 88 percent plan to use regulatory capital-allocation mechanisms. Sophisticated tools and analytics will allow them to earn credibility, participate in the primary market, and be a strategic partner to the business.

In the secondary market, survey participants see wholesale loan purchases and sales as the most important CPM tool. Their use is growing. Some 60 percent already use them, and 71 percent expect to do so in the near future. In contrast, tools such as index options and single-name CDS hedges are losing influence. In addition, the survey showed a likely shift in the way CPM makes hedging and sale decisions. Only 5 percent of respondents said CPM currently has the capabilities to consider a holistic

To carry out CPM's new mandate and earn the right to participate in strategic decisions will require superior analytics and a new management framework.

view of the portfolio, including stress outlook and capital and liquidity usage. But 39 percent said they aim to develop these capabilities in the future. Exhibit 1 shows how other considerations are also changing.

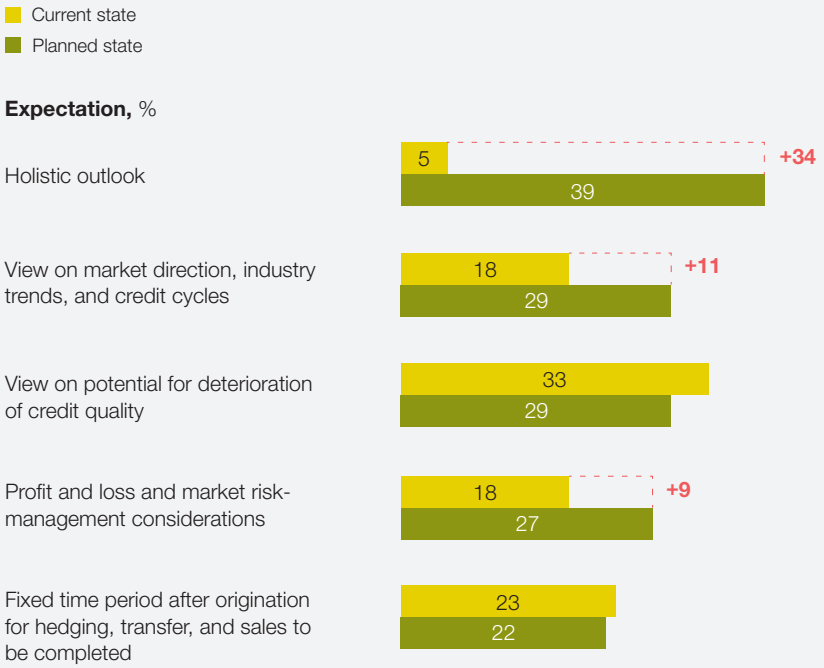
To steer business decisions, CPM will also need to use a granular and rigorous limit framework and evolving optimization tools. The new limit system needs to be in line with overall targets and limits for the balance sheet, reflecting the multitude of key performance indicators the institution has to optimize for. Before the crisis, CPM units often used transfer pricing to create effective internal markets. But this tool is losing its importance. With a host of new regulatory constraints to consider, transfer pricing would need to include so many components that it becomes increasingly misleading and opaque, and hence loses its power of influence.

Greater collaboration with the rest of the organization

CPM's new work at the point of origination, and its multifaceted challenge with capital constraints, liquidity ratios, and other regulatory demands, means the group has to work more closely with the range of functions governing the balance sheet. Eighty-three percent of executives describe an increased need for coordination between CPM and the rest of the organization during the past few years, particularly with finance and risk, and more than a quarter of respondents said they saw the need for significant change in the current interaction model.

Geography made almost no difference to respondents' views on this issue. Wherever they were located, the vast majority felt CPM should be engrained in the organization if it is to fulfill its new mandate. "Collaboration across the

Exhibit 1 **Expectations of credit portfolio management are changing.**



What credit portfolio management leaders said:

"We should move from 'do the deal' to influence and shape the balance sheet, define the strategy, and bring it to business."

"We need to understand the macro perspective better, and give a robust outlook in order to mitigate on the macro level and through the cycle."

"Tools are not applied mechanically anymore but with a more holistic view."

Source: International Association of Credit Portfolio Managers/McKinsey 2015 survey

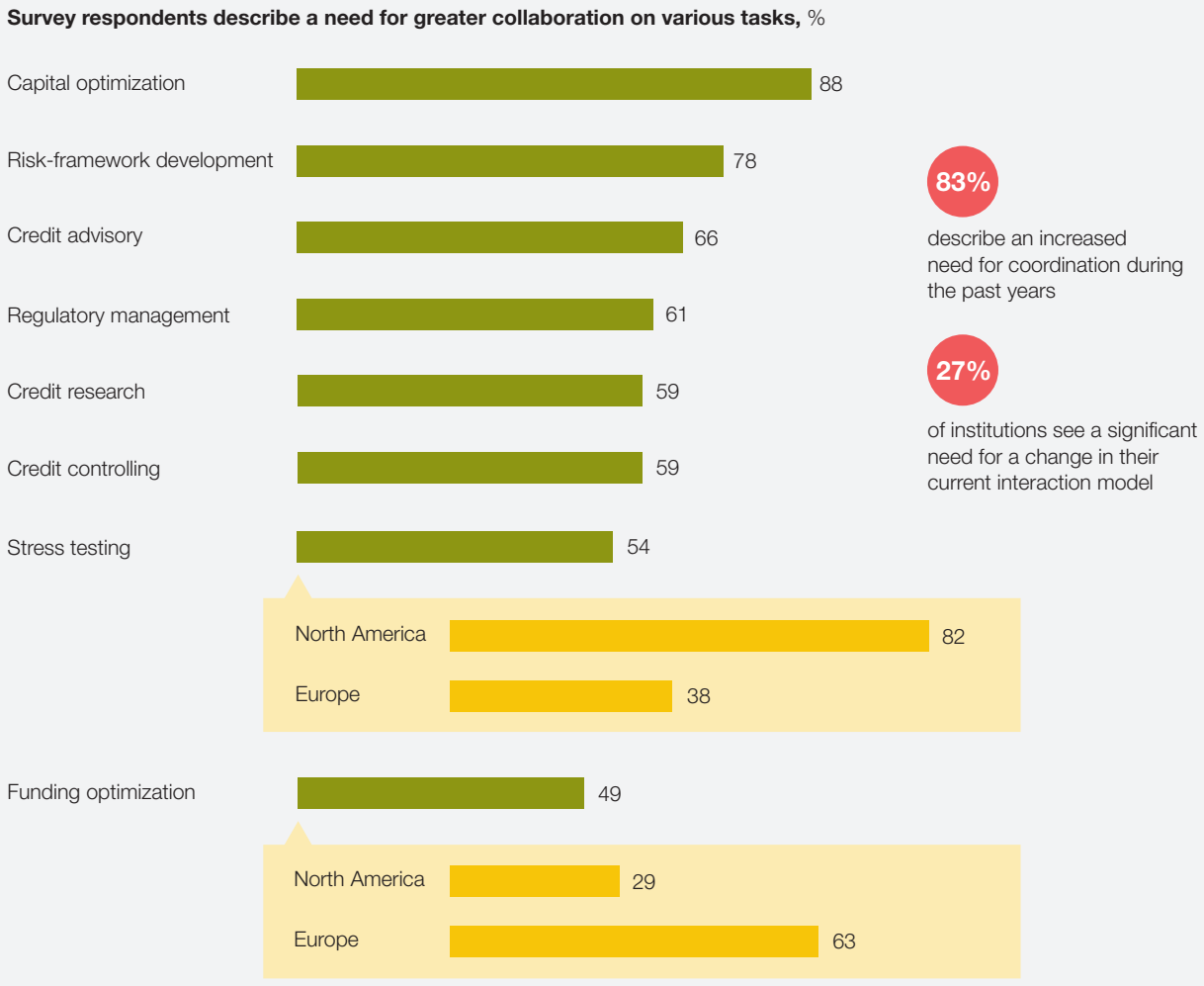
organization—covering risk and finance—is key to developing a capital-efficient business," was the view expressed by one respondent.

Exhibit 2 shows respondents' views on where CPM needs to be more closely involved. Capital optimization (88 percent) and the development of risk frameworks top the list.

Changing data needs

However the future role of CPM shapes up, it will need excellent data to fulfill its tasks and comply with regulations. Highly detailed finance and risk information is essential to risk-return models, and high-quality market information will be necessary to gain superior industry insights. Yet despite all the investment in data management and digitization,

Exhibit 2 **Credit portfolio management is moving from independence to collaboration.**



Source: International Association of Credit Portfolio Managers/McKinsey 2015 survey

largely in response to regulations such as Basel Committee of Banking Supervision (BCBS) 239, as well as digitization, results are lackluster. Sixty-six percent of respondents saw poor data as the single most important constraint preventing the function from performing its new mandate well (Exhibit 3). The transformation of data systems and data governance currently under way at many banks could provide the ideal opportunity for CPM to influence future investments and systems development. With its unique position at the center and in between many related functions, CPM can be in the optimal spot to define business requirements, with an overarching perspective on business, finance, and risk data and system needs.

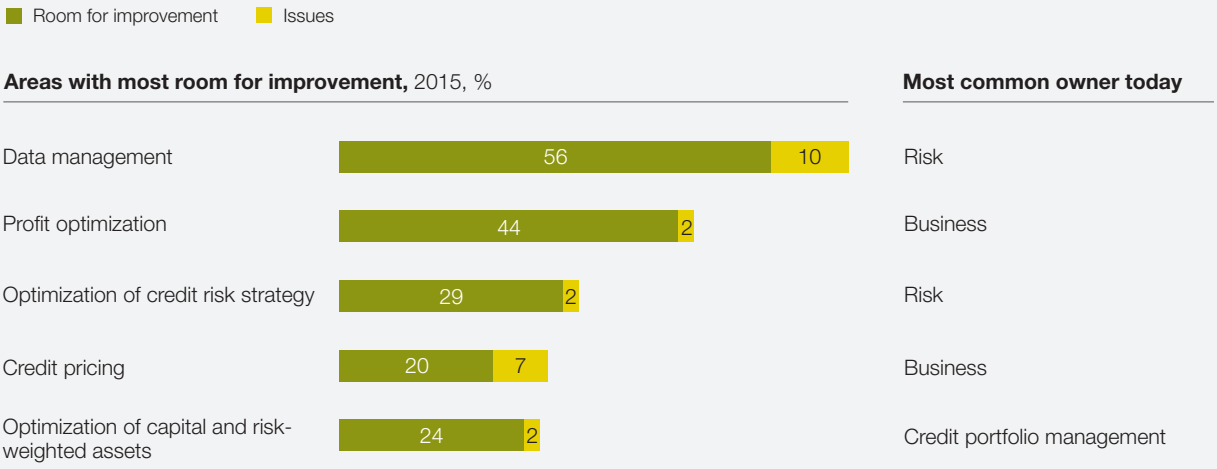
What senior leaders should consider

The need for CPM to play a different and wider role is clear. CPM's focus on portfolio dynamics puts it in a particularly advantageous position to steer balance-sheet construction, as compared with finance functions focused on measurement, credit risk functions focused on individual assessment and limits, and originators focused on individual deals and clients. Such a role is needed without delay, given the balance-sheet constraints that institutions already face, and the prospects of further tightening. Institutions should take five actions that will serve as building blocks for CPM to assume its elevated role.

Define the new mandate

How the new role of the CPM function takes shape will vary by institution, ranging from advisory to active portfolio management. For example, an investment bank that uses corporate credit lines as a loss leader to build relationships is likely to have a very different CPM function from a regional bank that generates core profits from its middle-market and small-and-medium-size-enterprise portfolios. The former will need a global overview and advice on risk positions and improving cross-selling, while the latter might benefit more from active portfolio management at a sector level.

Exhibit 3 **The biggest hurdle for credit portfolio management is data management.**



Source: International Association of Credit Portfolio Managers/McKinsey 2015 survey

Institutions with active trading operations should also consider the scope of responsibility for the function across loan books, securities portfolios subject to default risk, and trading counterparty risk. A comprehensive approach may be needed but presents additional complications. A thorough cost-benefit analysis and careful implementation of expanded scope is critical.

Whichever role is chosen, the change needs to proceed quickly and with a clear mandate that defines how the function will add value to the institution. This will help focus efforts to drive the change, which in many cases is already under way. Senior managers must ask whether this change is taking place in a way that suits the institution. And if CPM is not taking on an expanded role, who will be responsible for integrating balance-sheet optimization, stress testing, and ongoing management of the credit books?

Rethink the organizational setup

The new CPM mandate may entail some changes in organizational structure. Large institutions often want CPM to have direct market access, which would place it on the first line and hence anchored in the business. For some banks, that will mean moving the group out of the second line. Many respondents cited business proximity and alignment as important design principles for the CPM function.

In some cases, however, where the function is split into separate teams within each business unit, it may lose a centralized overview, making it harder to interact consistently with risk and finance. That's a problem: as an example, when profit optimization was carried out centrally, only 35 percent of survey respondents said significant improvement was required. In decentralized instances, the figure was 75 percent. An option to address this challenge might be to establish a thin central "layer" that combines the information from decentralized teams.

On the other hand, a setup as part of the second line of defense bears the risk of less credibility with the business side. A second-line CPM might also be seen as a team that only wants to "hit the brakes" instead of a function supporting the business. One survey participant suggested that job rotation between CPM, finance, and risk works well to address this challenge.

Another option might be to split the CPM function in two—a decentralized first-line team and a centralized second-line team, typically anchored in the risk function. In our experience, CPM functions at European banks tend to be anchored in finance or treasury, especially when newly established. This simplifies their mandate to optimize risk returns on the balance sheet as they naturally consider funding and liquidity needs. Exhibit 4 shows the current distribution of the various options.

In addition, each institution should consider whether its CPM function has the right proximity to senior stakeholders. Even though most institutions recognize the growing importance of CPM and the strategic role it will have to play in steering the balance sheet, it still sits at the third or fourth level of management in two-thirds of the institutions in our survey. And if it is to take a more strategic role in managing the balance sheet, a closer interaction with the board can help to address strategic topics effectively.

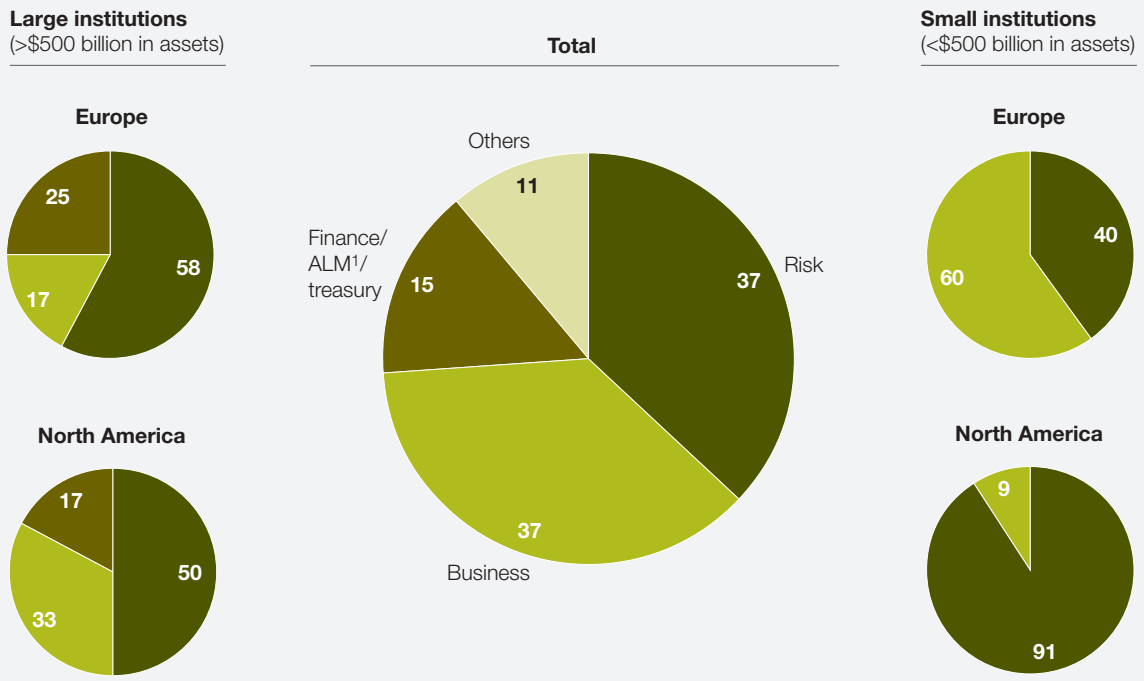
Redefine the functional position and promote greater integration

To be successful, CPM will need to work closely with the businesses and the risk and finance functions. As a starting point, senior managers should ask themselves whether roles and responsibilities are clear, and they should also factor in cultural considerations. What is CPM's functional fit with risk, finance, treasury, and the business?

Exhibit 4

Credit portfolio management is usually placed with the risk function in North America and with the business function in Europe.

Organizational group that includes credit-portfolio-management team, 2015, %



[1] Asset-liability management.

Source: International Association of Credit Portfolio Managers/McKinsey 2015 survey

There are then various measures, including job rotation, that can promote better integration. Institutions can give businesses and CPM joint responsibilities, such as ownership of models for pricing or industry analysis. They can make CPM the advocate of business in its dealings with finance and risk. And they can align incentives. Clearly, interaction is naturally supported if CPM has a representative within each business unit.

Build the analytic capabilities needed to restructure the credit book

Whatever the function's mandate and the way it is organized, it will need outstanding analytic capabilities. External factors such as market liquidity, the cost of funding, and regulatory scrutiny will require continual adjustments to the institution's credit book. CPM will need to understand these balance-sheet constraints, how they might change, and their interdependencies. Only with a trusted tool kit that provides the business superior insights from a portfolio perspective, which they cannot gain without CPM's support, will the CPM function be able to earn the right to be part of strategic discussions and business decisions.

Increasingly, CPM teams will need analytics to meet needs such as advanced pricing, an improved combination of risk and finance data (for better capital optimization), a more detailed and solid link

from the risk strategy and appetite to origination, and macro and industry insights (to aid mitigation at the macro level and through the business cycle).

Ensure adequate data, system governance, and infrastructure

Fundamental to successful CPM is the availability, analysis, and interpretation of information. Sixty-six percent of institutions named data constraints as the main hurdle for filling their expanded mandate. Senior managers must ask themselves whether the quality and availability of data is sufficient to enable CPM to form insights of value to the business. Current initiatives, like those begun in response to BCBS 239, can be an opportunity to ensure a clear data and system governance. To steer the business, CPM will need sufficient detail for portfolio analysis. To optimize the portfolio within current and future constraints, risk and finance data needs to be integrated. CPM functions have an opportunity to step in and take a vital role in the definition of business requirements, combining the perspectives of business, risk, and finance together with those of the IT department.

The survey reveals broad agreement on the need to evolve the role of CPM, and to do so promptly to respond to the current industry environment. That said, the role is evolving in different ways, depending on geography, business mix, and institutional idiosyncrasies. Senior managers cannot rely on a single template. The survey sheds light on the different choices being made about the function's mandate, the way it is organized, and the tools it is using, as well as what is driving those choices. We hope it will help others make their own choices wisely—and without delay.

[1] The IACPM (iacpm.org) is an industry association established to further the practice of credit exposure management by providing an active forum for its member institutions to exchange ideas on topics of common interest. Currently, 95 financial institutions in 19 countries are members.

[2] *Semiannual OTC derivatives statistics*, Bank for International Settlements, May 4, 2016, bis.org.

[3] *Securitisation data report, fourth quarter 2015*, a joint report from the Association for Financial Markets in Europe (AFME) and the Security Industry and Financial Markets Association (SIFMA), March 17, 2016, sifma.org.

Luis Nario is a partner in McKinsey's New York office; **Tamara Pfister** is an associate principal in the Munich office, where **Thomas Poppensieker** is a senior partner; **Uwe Stegemann** is a senior partner in the Cologne office.

The authors wish to thank Florian Fuchs for his contributions to this article.

‘The ghost in the machine’: Managing technology risk

Technological risks are becoming more prominent—and more dangerous. Six principles can guide banks as they manage them.

Oliver Bevan, Saptarshi Ganguly, Piotr Kaminski, and Chris Rezek

Technology is synonymous with the modern bank. From the algorithms used in proprietary trading strategies to the mobile applications customers use to deposit checks and pay bills, it supports and enhances every move banks and their customers make.

While banks have greatly benefited from the software and systems that power their work, they have also become more susceptible to the concomitant risks. Many banks now find that these technologies are involved in more than half of their critical operational risks, which typically include the disruption of critical processes outsourced to vendors, breaches of sensitive customer or employee data, and coordinated denial-of-service attacks. Cybersecurity alone can account for 10 percent of total information-technology spending, which is now growing at three times the rate of the budget of the technology being secured.

Exposure to these IT risks has grown in lockstep with the rapid increase in digital services provided directly to customers.[1] For example, mobile transactions have expanded exponentially, presenting malicious external actors with billions of new entry points into bank systems. The complexity and growing vulnerability of the underlying IT systems are of equal concern. Big banks must manage hundreds or even thousands of applications. Many are outdated, having failed to keep pace with the radically changed processes they are supposed to support. Even banks that have successfully upgraded their infrastructure face upgrade-related risks—from project and data management to security problems that persist after the migration is complete.

When technology risks materialize, the financial, regulatory, and reputational implications can be severe. If banks lose customer data in a high-profile incident, they face legal liabilities and fleeing customers. Investors sell shares in the wake of cyber-attacks, around 10 percent of which result in a more than 5 percent dip in the stock prices of the companies affected.[2] Regulators penalize firms for noncompliance—from data breach–related fines to mandated remediation activities. Basel II could not be clearer on the topic: one of its seven level-one operational-risk categories is "business disruption and systems failure."

To manage these risks, many banks simply deploy their considerable IT expertise on patching holes, maintaining systems, and meeting regulations. Some have set up specialized teams to cope with particularly acute problems, such as cybersecurity. But these half-measures are unlikely to afford sufficient protection. An IT-oriented approach, furthermore, may be unable to account for wider business implications and operational interdependencies. Institutions focused on compliance could ignore vulnerabilities outside the purview of the regulator and overlook applications critical to the business, with implications for business risk down the road.

Muddling through is no longer an option. The adequate mitigation of technology risk requires a coordinated effort that goes beyond IT-centered remedies. Leading banks are creating specialized teams within the enterprise-risk-management group to manage technology risk, in all its manifestations, across the organization. In this article, we will outline the six principles that these teams use to stay well connected and integrated with the rest of the bank, to develop the skills needed for these complex jobs, and to drive transformation and remediation activities. We conclude with some suggestions for getting these teams off to a good start.

Six principles

These principles are not a step-by-step manual but rather guidance for creating best-practice technology-risk management. By adhering to them, bank leaders will be able to remain in control of the rising levels of risk associated with the digital age.

Adopt a business-first approach

Companies can develop a complete picture of their information needs, uses, and risks only through a dialogue between IT and the business to identify the most critical business processes and information assets. The strongest controls can then be applied to the most valuable IT systems and data, the bank's "crown jewels." Proprietary trading algorithms stored on laptops, credit transaction data shared with third parties, and employee-health information—all may qualify. The IT-risk group should drive the assessment program, but the businesses need to be engaged with it and assume responsibility for the resulting prioritization, as they are the true risk owners. Only in this way will banks make the most effective investments in security. For example, an IT-led prioritization typically focuses too much on securing "big iron" applications while underemphasizing risks from unstructured data flowing through email and stored in collaboration platforms. For the crown jewels, remediation investments might include multifactor authentication, data-loss-prevention tools, and enhanced monitoring and analytics.

Thinking "business first" is especially important in information security. Data leaks, fraudulent transactions, blackmail, and "hacktivism" all pose dangers. Banks should consider their defenses in light of a threat's potential adverse impact on the business, rather than defaulting to blanket security standards that ratchet up after each negative headline. Nevertheless, security and the customer experience need not be approached as a trade-off. Leading banks are finding ways to give their clients

improved digital solutions that are simultaneously more secure and easier to use.

Coordinate across the subdisciplines of IT-risk management

Most banks have established groups to manage some or all of the various realms in which technology risk can pop up. These typically include cybersecurity and disaster recovery—as well as, increasingly, vendor and third-party management; project and change management; architecture, development, and testing; data quality and governance; and IT compliance (exhibit). While such groups are interdependent in many ways, particularly when a new product or service is under development, they often are not formally connected.

Best-practice banks coordinate the work of the subdisciplines to capture significant risk-mitigation synergies. For example, housing crown-jewel data on servers other than those used for the main operational IT systems has implications for security, disaster recovery, and data management. Analyzing these three risks separately could lead to inadvertent gaps in risk management or to redundant overprotection. Coordinating the subdisciplines also avoids duplication of effort, such as a product manager completing a half-dozen overlapping risk reviews before product launch.

Exhibit

Effective IT-risk management covers relevant subdisciplines.

IT-risk subdisciplines	Key risks for banks
Information and cybersecurity	Leakage of confidential customer and internal data, fraudulent transactions, blackmail, “hacktivism”
Resilience and disaster recovery	Recurring or prolonged interruptions of IT services supporting processes that are critical for customers or bank
Vendor and third-party management	Vendors or third parties not delivering reliable and secure service
Project and change management	IT projects not delivering on schedule and within budget, or not at adequate quality
Architecture, development, and testing	Systems not being designed to deliver long-term affordable, reliable, and maintainable service to enterprise
Data quality and governance	Legal/regulatory or transaction-settlement issues as a result of inaccurate, inconsistent, or missing data
IT compliance	Noncompliance of IT systems and process with regulations

Close the gaps in the three lines of defense

Banks have not always consistently applied the principles underlying the three lines of defense—the risk-management approach adopted by almost all financial institutions of any size—to technology risk. The three lines of defense is a more complicated approach for technology risks than for market or credit risk, for two main reasons. To begin with, the first line includes both the business and the IT function that enables it. Second, there are often "line one and a half" functions. In cybersecurity, for example, the chief information security officer (CISO) is responsible for setting policies and risk tolerances, as well as for managing operations to meet those expectations—both second-line activities. Yet the role usually resides in the first line, as part of the organization of the chief information officer (CIO). This blurring of the lines can create potentially problematic situations in which the group is "checking its own homework." Similar boundary confusion can arise in certain subdisciplines, like disaster recovery, where both the first and second lines need real technology expertise.

Banks should carefully clarify the roles and responsibilities in managing technology risk for each line of defense. Increasingly, organizations are asking the IT-risk group to take on the policy, oversight, and assessment roles, while security operations remain within the CIO's scope.

Careful distinctions like these are needed, for example, when institutions launch a new mobile-banking application. While the business sets out its commercial requirements, the IT group will work collaboratively to define the architectural and technical requirements. The second-line IT-risk function should be engaged from the start of such a project to identify risk exposures (such as the possibility of increased fraud or customer-identify theft) and provide an independent view on mitigation actions and feedback from testing results. Risks identified can be mitigated by the CISO and his or her team, through compensatory controls or design changes before the app is launched. This avoids the delays, cost overruns, and organizational tensions that arise from discovering exposures during a security review conducted too close to launch.

Integrate with enterprise risk management

In many banks, technology-risk management is disconnected from enterprise risk management (ERM) and even from the operational-risk team. That inhibits the bank's ability to prioritize the risks that are of critical importance and deploy the resources to remediate them. A contributing factor is often the absence of a common risk-management technology platform shared by both the IT-risk team and the ERM or operational-risk group. Without such a platform, banks struggle to aggregate risk information consistently, and managers are not equipped with the data they need to make decisions.

For example, as banks manage operational risks, they frequently balance the benefits of automation (to reduce opportunities for human error) against operational process controls (to improve behavior). Each option has advantages but also challenges—automation can introduce technology risk while operational controls can make systems unwieldy. Without a unified view of the risks involved, banks must often rely on advocates of particular initiatives when making risk-management decisions, rather than a holistic view of the available approaches and their merits. The bias can thus be to optimize within a risk category rather than to promote the good of the enterprise.

When the IT-risk group is integrated with ERM, on the other hand, real benefits can result—particularly if the technology-risk team comes under the same umbrella as other operational-risk-management teams. Decisions can be made at the level appropriate to the needs of the business and the potential severity of the risk. The business

To prevent the interruption of critical services, IT-risk managers should articulate a risk appetite that reflects the business impact of disruptions.

can make decisions about low-level exposures directly, while the tech- or op-risk group addresses the more significant risks and corporate ERM and senior management address the most significant ones.

Typical decisions with significant but underappreciated risk implications include those affecting a bank's long-term architectural road map and risk-appetite decisions about testing requirements for major IT changes. When it comes to mobile apps, for example, some banks will choose to be early adopters, given the anticipated customer value, while others wait for best practices to develop. Both courses might be sensible, but only senior management should decide between them.

Two domains where ERM integration can yield great benefits are resilience and disaster recovery, and vendor and third-party management. To prevent the interruption of critical services, IT-risk managers should articulate a risk appetite that reflects the business impact of disruptions. Most banks will find that for a small percentage of their business processes, near-perfect IT resilience is essential. These are customer-initiated, time-critical processes (such as ATM withdrawals, brokerage transactions, and point-of-service purchases) with no real-time alternative. Risk investments in resilience and disaster recovery must focus on these specific processes and the relatively small number of systems that support them. For other processes, IT-risk managers should work with the IT function to define the needs for supporting processes where the appetite for risk is relatively high and banks should be able to make savings by reducing the level of support required.

IT-risk managers should also partner with the business and IT to establish standards for security, continuity, and disaster recovery for a bank's external service providers. Given the sheer number of vendors that banks use, standards and audits must be applied in a risk-prioritized way. Banks should also consider involving their closest vendors and partners more significantly with internal ERM processes (to improve risk identification, assessment, and control) and also with incident response. Banks that use "war games" to test their crisis-response plans often find that the roles and responsibilities of third parties are outdated or poorly defined in service-level agreements, potentially leading to problems during a live breach.

Change the performance incentives for IT managers

Banks encourage IT managers to deliver projects on time and on budget and to maintain near-perfect levels of system availability. These objectives are obviously important, but overemphasizing them can mean that project managers do not do enough to minimize business-risk exposure. The prevailing culture encourages short-term delivery while underemphasizing long-tail but significant risks. For example, situations arise in which back-end systems are technically operational but the actual customer-facing business process is unavailable as a result of a lost database connection, for example,

or a lost connection with a client and a delay while the backup system kicks in. Infrequent but high-impact outages are almost never mentioned in performance-management systems, which instead feature operational data.

To monitor risk, best-practice banks add forward-looking metrics, such as the time it takes to detect and mitigate cyberincidents, the volume of unknown devices connected to the internal network, vendors out of compliance with security requirements, and employees failing phishing tests. Leading banks also track the number of incidents and the actual recovery times for highly critical service chains, including systems supporting mobile banking, ATM services, and electronic trading. Such a performance-management system should work hand in hand with a value-assurance framework, which establishes, for each major IT project, the criteria for aligning stakeholders and the software-development life cycle. Research has shown that a failure to manage these elements is the most common cause of budget and schedule overruns.[3] Aligning business and IT managers with appropriate risk-management mindsets and behavior is critical.

Invest in specialized talent

Technology-risk management requires critical thinking and hands-on experience in technology, business, and risk. Individuals with all of these skills are hard to find and command high salaries—but they are indispensable. Only someone skilled in all of these areas can both effectively challenge IT teams and act as a thought partner to guide strategic decisions.

The good news for banks is that they can develop this kind of talent through part-time staffing models, training, and rotational programs. Some banks have succeeded by recruiting experienced IT specialists willing to learn risk-management skills and giving them appropriate training and a ladder for advancement. Banks can thus build a core group of IT-risk professionals with a strong knowledge of functions, technology subdisciplines, and operational-risk practices. These are essential skills for the core work of the group—exercising proper oversight from the second line of defense. They will also help the technology-risk team with other parts of the job. IT-risk managers should define architectural standards, sit on architectural-review committees, establish a consistent software-development life cycle across the enterprise, and monitor test results. They should ensure not only that individual IT changes are delivered efficiently but also that the IT environment is sustainable in the long run.

Independent yet connected

The IT-risk group must be aware of what is happening in all parts of the organization. As a bulwark of the second line of defense, it must have strong insights into the first line (both the businesses and the IT units that support them), have a strong connection to the central IT team, forge connections among the various subdisciplinary teams, and integrate its work with the core risk-management team driving ERM.

To accomplish this delicate two-step of independence and partnership, banks can consider two actions. First, they can establish a single unified mission for the IT-risk group, which should enable the core business and be a partner to other functions to improve the overall effectiveness of technology-risk management. The function's activities in managing technology risks should focus on this vision, shared by the board and top management. The function's mission is then to understand the specific risks facing the bank given its core operational processes and organizational structure, to identify the major challenges in remediating or managing these risks, and to allocate responsibility for the specific actions needed.

Second, banks should create effective interaction and communication models that reduce ambiguity and promote collaboration. Clear committee structures, the frequency of meetings, and reporting lines will both help avoid duplication and ensure that key functions are not left undone. In identifying and prioritizing risk, organizations can usually build on existing risk evaluations and analyses and add mechanisms to ensure collaboration.

The expectations of customers, shareholders, and regulators for the resilience of banks will continue to escalate. Recent events have exposed the ghost in the machine—how the failure of technology can cause lasting damage to an institution's brand and reputation. Successful banks will establish an IT-risk group as a second line of defense that engages with the business and IT function while providing effective oversight and challenge. The group will also be staffed with experts in technology and risk management. With the right practices and capabilities, banks can effectively manage technology risk for the digital age.

[1] Michael Bloch, Sven Blumberg, and Jürgen Laartz, "Delivering large-scale IT projects on time, on budget, and on value," October 2012, McKinsey.com.
[2] Alison Smith, "Share prices are rarely hit hard by cyberattacks," *Financial Times*, October 31, 2013, ft.com.
[3] Bloch et al., "Delivering large-scale IT projects."

Oliver Bevan is a consultant in McKinsey's Chicago office; **Saptarshi Ganguly** is a partner in the Boston office, where **Chris Rezek** is a senior expert; **Piotr Kaminski** is a senior partner in the New York office.

The authors wish to thank Salim Hasham and Wolf Richter for their contributions to this article.

Transforming enterprise risk management for value in the insurance industry

Leading insurers are retooling the role of their risk function from incident response and compliance to an essential partner in advancing the business strategy.

Christian Bongiovanni, Luca Pancaldi, Uwe Stegemann, and Giambattista Taglioni

The value of enterprise risk management (ERM) in the insurance industry was given a decisive demonstration in the financial crisis. McKinsey research showed that the better their ERM systems, the better insurers performed financially in 2008 and 2009.[1] In the aftermath, much industry attention focused on creating or improving ERM systems, and the focus has been sustained under pressure from regulators, rating agencies, and investors. The starting point for the industry's ERM efforts has been, perhaps naturally, a reactive stance, with systems designed to respond to incidents and ensure compliance with existing and forthcoming regulations. Yet a few insurers have been able to develop ERM frameworks that support strategic decisions and create real business value. Over time, they have reduced the volatility of their returns and improved capital performance—results of having enabled a more penetrating view of proposed risk taking across the enterprise and embedding the ERM function as an active partner in business decision making.

What are the elements of an effective ERM framework? How can insurers move from playing defense to using ERM systematically to advance business objectives? In a recent survey we conducted, leaders of a range of insurance companies revealed that they were thinking about such questions in a focused way.[2] While expressing confidence in the strength

of their companies' risk capabilities, respondents identified key areas for improvement in risk transparency and insight (Exhibit 1). Smaller companies also indicated gaps in risk culture and performance transformation. Most of the surveyed chief financial and risk officers indicated that they are enhancing ERM amid a perceived climate of heightened risk—one defined by a more uncertain macroeconomic environment, persisting low interest rates, financial-market volatility, and rising geopolitical instability.

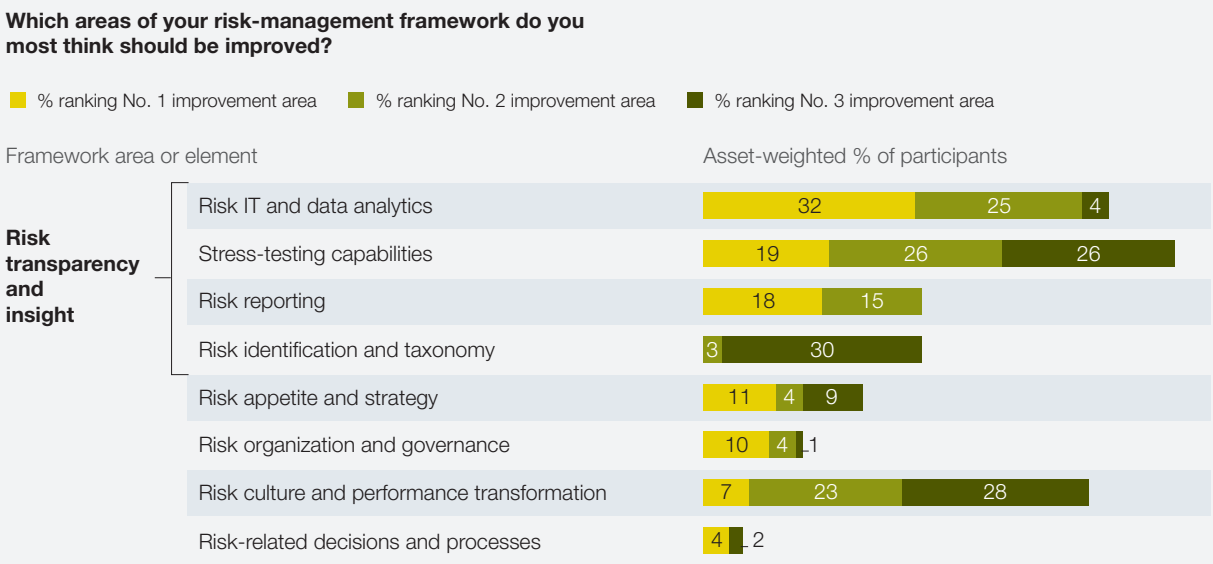
Attaining ERM excellence: A journey to value creation

In thinking about the experience of leading institutions with enterprise risk management, McKinsey developed a framework to help capture best practices (see sidebar, "Where do you stand? The ERM framework"). The framework integrates the elements of risk management in a reinforcing cycle that supports the business strategy (Exhibit 2).

A best-practice risk function fosters a highly integrated, enterprise-wide risk culture across the organization, managing the risk profile to serve the business strategy. The path to ERM excellence involves a transformative journey, and most insurers are at its beginning stages (Exhibit 3). For the majority of companies, the risk focus is on compliance, a necessary starting point. They monitor risk, gauge risk levels against new regulations, and react appropriately to risk incidents. The ERM function at this stage is mainly backward looking, developing controls and aligning existing risks with current and forthcoming regulation. The risk function first establishes and then operates within risk-review guidelines and may have (and at times may exercise) formal veto power over business decisions.

Systematic ERM really only begins after compliance-focused capabilities have been adequately developed, including the setting of risk limits and policies

Exhibit 1 **Respondents identified risk transparency and insight as improvement targets for enterprise risk management.**



Source: 2015 McKinsey survey of 27 insurers, representing ~$3 trillion in assets, on enterprise risk management

Exhibit 2 **The enterprise-risk-management framework illustrates an integral cycle of best risk practices.**

Source: McKinsey analysis

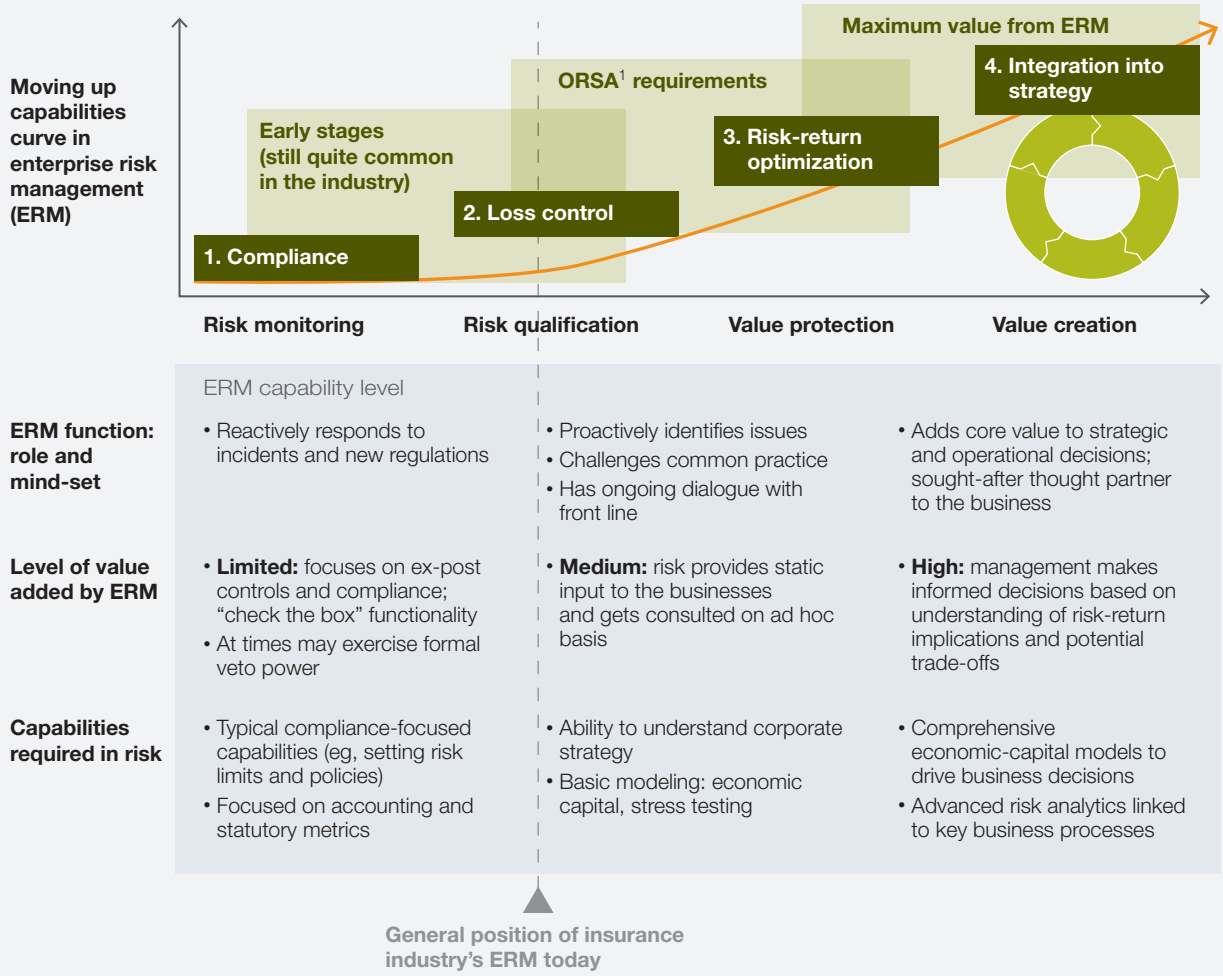
and the adoption of accounting and statutory metrics. Most insurers are at this stage of development. They use their own risk and solvency assessment (ORSA), in line with US and EU regulations. This provides insurers with an internal process for assessing the effectiveness of risk-management capabilities and solvency under normal and stressed conditions. ORSA helps insurers evaluate all material risks that could affect their ability to meet policyholder obligations, including market risks, credit and underwriting risks, liquidity risks, and operational risks.

At this stage, the ERM approach pushes the risk-management function to incorporate loss control and risk-return optimization into its role. In ongoing dialogue with other functions (such as finance) and the business, risk managers proactively identify potential issues and, where helpful, challenge common practices. The function develops an understanding of corporate strategy and the ability to model economic capital (risk capital) and conduct stress testing. The function then converts the models into strategic input for top management.

In the ultimate stage of the journey, the risk function creates value by integrating ERM with corporate strategy. The function becomes a sought-after thought partner, enabling business management to weigh risk-return implications and potential risk trade-offs in strategic and operational decisions. To become a strategic thought partner, the ERM

Exhibit 3

The insurance industry as a whole is still at the beginning of a journey to excellence in enterprise risk management.



[1] Own risk and solvency assessment.

Source: 2015 McKinsey survey of 27 insurers, representing ~$3 trillion in assets, on enterprise risk management

function must be able to create the comprehensive economic-capital models needed to drive business decisions and to link advanced risk analytics to key business processes.

Improving ERM: Where insurers say they are focusing

As Exhibit 1 displayed, our survey respondents mostly cited capabilities within risk transparency and insight as the objects of their planned ERM-improvement efforts.

Risk transparency and insight

Within this ERM area, respondents noted their intentions to improve stress testing, risk reporting, and—especially—data and analytics. One-quarter of respondents cited data governance and quality and another quarter cited automation and speed of data gathering as their initial improvement priorities. In the survey and follow-up discussions, respondents shared their perceptions that the industry needs generally to invest more in analytics, recognizing the transformative power of big

Where do you stand? The ERM framework

On the journey toward its integration into business strategy, the epitome of excellence in enterprise risk management (ERM), the risk function strengthens the interlinked areas of the framework. It is always good to know where you are going well before you get there. Optimally, the broad areas of ERM and their constituent elements are mutually reinforcing.

Risk transparency and insight

- *Risk identification and taxonomy.* A common vocabulary for different risks enables an enterprise-wide view of the risk profile, so that it can be shaped according to the business strategy. Risks are thereby defined and prioritized based on probability, impact, and preparedness.
- *Risk reporting.* Regulatory and company-specific reporting principles are selected for timeliness, clarity, comprehensiveness, and accuracy; the underlying data architecture and IT must support risk-data aggregation. Strong governance is essential.
- *Risk IT and data analytics.* With technical and business-leading analytics talent, new sources and types of data are captured to extract differentiating insights; machine learning is applied to improve existing models and enable the underwriting of new risks.
- *Stress testing.* Models are based on consistent scenarios and translation of economic drivers into key insurance risks. The approach is to assess risks in line with the business strategy, taking account of balance-sheet and capital implications.

Risk appetite and strategy

- *Risk appetite.* The risk appetite is defined by the business strategy. An understanding of whether you are the natural owner of given risks is developed on this basis; how much risk to take to pursue company goals is then cascaded down to the businesses.
- *Risk strategy.* The strategy comprises actions to transform the risk profile, selected based on priorities and including trade-offs with corresponding costs.

Risk decisions and processes

- *Decisions.* Risk is embedded in strategic and business decision making rather than used in a purely compliance-driven approach.
- *Processes and operations.* Core business processes and operations are designed and executed on a risk-informed basis.

Risk organization and governance

- *Risk archetypes.* The risk function's mandate for enterprise risk management is clearly defined.
- *Risk organization.* Risk structures are designed across the entire organization with the support of top management.
- *Risk-function profile.* Responsibilities are clearly allocated between the risk-taking and controlling units.

Risk culture and performance transformation

- *Risk culture.* Diagnostic inquiries can be made periodically to ensure that the risk culture is sound across the entire organization.
- *Risk norms.* New risk norms should be embedded through corporate processes and governance.
- *Risk skill building.* A program should be in place to enhance risk skills for key roles as needed.

data. Fast, automated access to accurate data is only a prerequisite for the strategic use of advanced analytics. The broad challenge is to generate value from the data. Advanced analytics enables better decision making in pursuit of strategic objectives and increased performance transparency to improve bottom-line financial results.

Most respondents indicated that they perform stress testing and consider results in decision making, but about half revealed that not all risks are taken into account in the process. In interviews and follow-up discussions, survey participants expressed their intention to improve stress testing by properly accounting for all risks in their stress tests and by deriving more useful insights from the results. Nearly half of respondents revealed that their risk-reporting process was only partly structured and had no predefined escalation mechanisms in place.

Risk culture

When asked about the level of accountability for risk-related matters in their organization, 38 percent of respondents declared that risks in daily business are not always considered with the support of both qualitative judgment and quantitative tools. This implies that a plurality of the industry is not achieving available levels of risk transparency that could improve business decisions.

With respect to frontline functions, participants indicated that risk is most engrained in people's minds in the following areas: investment management (the first choice for 56 percent of participants) and corporate and commercial nonlife (22 percent). Room to improve frontline risk culture seems to exist in retail life and nonlife businesses.

Discussions and interviews with insurance leaders highlighted that some players are making significant investments in risk-culture programs, in particular launching dedicated actions to increase risk culture in retail businesses where third parties (that is, brokers and independent financial advisers) are often the main distribution channel.

Approaching ERM transformation

ERM transformations can be focused on selected priority areas or the overall ERM program. Experience has shown that successful transformations have key traits in common. Direct board and top-management sponsorship and participation is the first requirement. Second, a chief risk officer (CRO) should be elevated from the usual technical-advisory status to play a true leading role. As leader, the CRO should drive the initiatives and set the direction of the effort. In planning the transformation, the CRO-led team must take

Fast, automated access to accurate data is only a prerequisite for the strategic use of advanced analytics. The broad challenge is to generate value from the data.

an integrated perspective, above all ensuring consistency across all core ERM elements. This is even more important than achieving excellence in any one area. The CRO should communicate the core messages of the transformation and ensure that they are cascaded to all levels of the organization. The CRO-led effort must also influence risk management throughout the organization, using such leverage as material incentives and role modeling optimal behavior.

A targeted intervention

In a targeted ERM intervention, particular elements—such as risk-appetite definitions, stress testing, or reporting, for example—are addressed as priority challenges. Such interventions are efficient when the overall ERM framework has been thoroughly evaluated and determined to be robust. They can also be helpful in addressing particular external constraints, such as regulatory findings or new rules (and rulings). Success depends on a well-defined starting point and clearly articulated set of priorities.

The targeted transformation begins with a diagnostic evaluation of the ERM framework. This will scan each segment and identify and prioritize improvement initiatives. The development of advanced capabilities can be an ideal choice for a targeted intervention. Machine learning, for example, allows companies truer visibility into their customers' risk profiles. It improves existing models and helps companies avoid unseen risks while potentially allowing them to underwrite completely new risks. The future profitability of the sector depends on such differentiating insights from new sources and types of data. To obtain these insights, leading companies are investing in innovative capabilities such as advanced analytics and machine learning.

An overall ERM transformation

An overall transformation program will cut across all or most of the ERM framework's segments and their constituent elements, and it could take up to two years to complete. Insurers undertake such transformations when a diagnostic evaluation reveals that the ERM framework requires general improvement; when the company is undergoing a strategic change of course, such as a modified risk appetite or a significant change in the business mix; or when the improvement areas indicated in the diagnostic require interventions that cut across the entire organization or involve cross-functional elements in the framework.

An overall ERM transformation is shaped in three steps. First, an independent diagnosis of the current ERM status is undertaken, based on best-practice knowledge and insights, with peer-performance benchmarking. The results are discussed with top management and the board, in order to define the target ERM state and prioritize the needed array of initiatives. Finally, an integrated action program is built, with clearly defined milestones and deadlines, incorporating early experiences and making needed improvements and adjustments as the transformation progresses.

Exhibit 4 presents a brief outline of the results of an actual diagnostic evaluation of a large insurer's ERM framework and proposed transformation program.

The evaluation is the beginning of the journey to build a new ERM foundation and to formalize risk strategy and processes. In each part of the framework, actions are identified and implemented to focus the transformation effort on a defined target ERM state. Actions are rolled out strategically, according to prioritized needs. In the example diagnostic, priority actions for transparency and insight would include a review of reporting

Exhibit 4

An ERM diagnostic and benchmarking revealed improvement areas for one European insurer.

Risk culture and performance transformation
- No challenge made on risks; weak communication
- No ownership of risk culture

Risk transparency and insight
- **Models:** major audit findings for several rating models; no capability to fulfill required stress tests
- **Reporting:** inconsistent metrics; no forward-looking information
- **IT infrastructure:** no "single source of truth"; many manual work-arounds

Risk appetite and strategy
- Risk-appetite framework not cascaded through organization
- Only simple metrics defined; no linkage of strategic risk-appetite metrics; no specific metrics for operational risk or risk type

Risk decisions and processes
- Risk-related processes ineffective and inefficient
- Risk acts as a "checker," not an "adviser"
- Compliance function not clearly defined

Risk organization and governance
- No budget for risk transformation program
- No metrics on risk capabilities
- Complex organization
- Weak mandate for chief risk officer and risk function
- Unclear roles and responsibilities
- Many risk positions vacant

Note: Each dot represents an element within the framework category; color represents the diagnostic evaluation of the element's state of readiness; the bulleted notes characterize development needs.

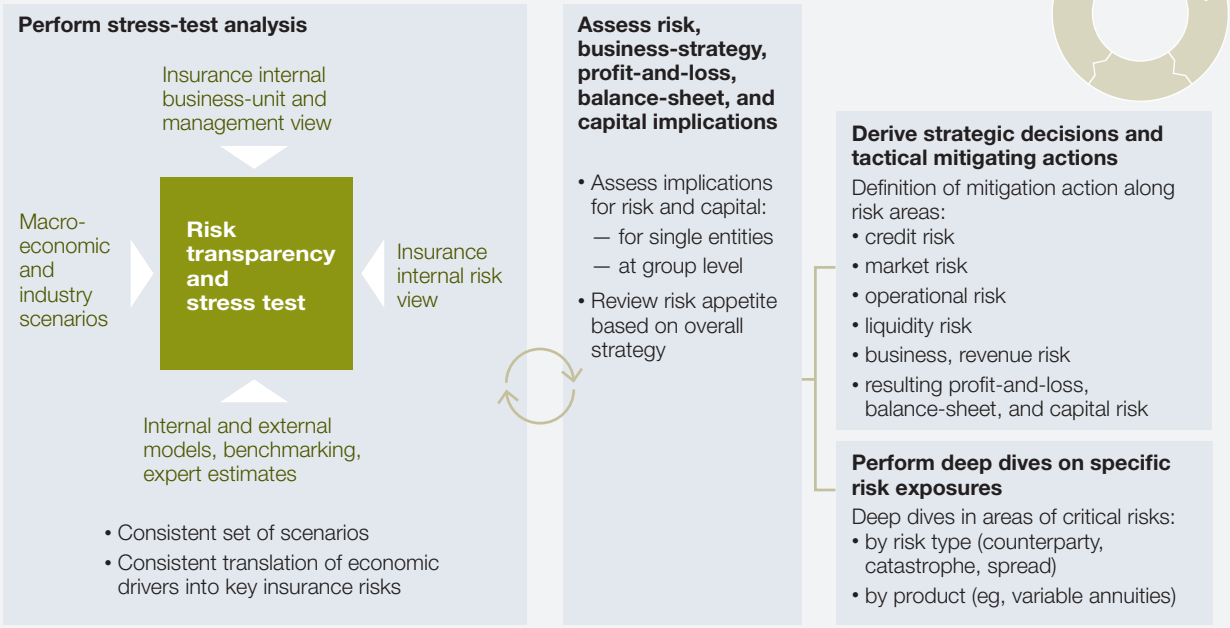
Source: McKinsey analysis

and stress testing and the development and implementation of new governance and models. The approach to stress testing would be shaped by the insurer's specific situation and needs. It would involve deep analysis on a consistent set of scenarios, a comprehensive assessment of implications, identification of tailored strategic actions and mitigating decisions, and deep dives on specific risk exposures (Exhibit 5).

As the transformation proceeds within each area of the ERM framework, and as gaps with the target end state are closed and connections across the risk function are strengthened, priorities can be reassessed and realigned in light of new insights and accomplishments.

With a broad consensus among insurers that the environment has become riskier and the regulatory atmosphere more complex, greater and more systematic attention is being afforded to the state of enterprise risk management. As improvement areas in the ERM framework are identified, leading insurers are taking this opportunity to move

Exhibit 5 **Stress-testing capabilities are reviewed and redesigned in a transformation according to the insurer's situation and needs.**



Source: McKinsey analysis

beyond plugging the gaps. Commanding new capabilities and techniques, they are defining a target state for ERM and cultivating an organization-wide risk culture that could become sources of real competitive value. ■

Christian Bongiovanni and **Luca Pancaldi** are partners in McKinsey's Milan office, **Uwe Stegemann** is a senior partner in the Cologne office, and **Giambattista Taglioni** is a senior partner in the New York office.

The authors wish to thank Daniel Kaposztas for his contributions to this article.

[1] *From compliance to value creation: The journey to effective enterprise risk management for insurers*, February 2014, McKinsey.com.

[2] Twenty-seven insurers representing approximately $3 trillion in assets were asked about systemic risk in the sector, the adequacy of industry regulation in accounting for risk, and the performance of their companies' internal risk-management practices. Most agreed that the sector was largely free of systemic risk, but expressed a range of views on the current and evolving regulatory environment: see Luca Pancaldi, Uwe Stegemann, and Torban Swart, "The big questions for the insurance sector," chapter 10 in *The Economics, Regulation, and Systemic Risk of Insurance Markets*, ed. Felix Hufeld, Ralph S. J. Koijen, and Christian Thimann (Oxford University Press, 2016).

The value in digitally transforming credit risk management

To withstand new regulatory pressures, investor expectations, and innovative competitors, banks need to reset their value focus and digitize their credit risk processes.

Juan Antonio Bahillo, Saptarshi Ganguly, Andreas Kremer, and Ida Kristensen

External and internal pressures are requiring banks to reevaluate the cost efficiency and sustainability of their risk-management models and processes. Some of the pressure comes, directly or indirectly, from regulators; some from investors and new competitors; and some from the banks' own customers.

The impact is being felt on the bottom line. In 2012, the share of risk and compliance in total banking costs was about 10 percent; in the coming year the cost is expected to rise to around 15 percent. Overall, return on equity in banking globally remains below the cost of capital, due to additional capital requirements, fines, and lagging cost efficiency. All of this puts sustained pressure on risk management, as banks are finding it increasingly difficult to mitigate risk through incremental improvements in risk-management processes.

To expand despite the new pressures, banks need to digitize their credit processes. Lending continues to be a key source of bank revenue across the retail, small and medium-size enterprise (SME), and corporate segments. Digital transformation in credit risk management brings greater transparency to risk profiles. With a firmer grip on risk, banks may expand their business, through more targeted risk-based pricing, faster client service without sacrifice in risk levels, and more effective management of existing portfolios.

Incumbents under pressure

Five fundamental pressures that relate directly to risk management are being exerted on banks' current business model: customer expectations for digitally managed services; regulatory expectations of a high-performing risk function; the growing importance of strong data management and advanced analytics;

new digital attackers disrupting traditional business models; and increasing pressure on costs and returns, especially from financial-technology (fintech) companies (Exhibit 1).

Customer expectations. Traditionally reliant on physical distribution, banks are finding it difficult to meet changing customer needs for speed and simplicity, such as fast online credit approvals.

Regulatory and supervisory road map. Regulators are expecting the risk function to take a more active role in the context of new, digitized business models. New regulations are being put in place to address cyberrisk, automation of controls, and issues relating to risk-data aggregation. Directives pertaining to the Comprehensive Capital Analysis and Review, BCBS 239, and asset-quality reviews specify requirements for data management and the accuracy and timeliness of the data used in stress testing.[1]

Exhibit 1

Five trends are altering the current risk-management model and making digitization a 'must-have.'

Trends transforming the banking industry	Impact on risk management (examples)
1. Changing customer expectations	Customer demand for online and mobile experience: mobile payments are expected to grow four times by 2020 Internal users of risk reports (eg, chief risk officers) have heightened expectations for quality and timeliness
2. Tighter regulatory control requiring greater risk-function effectiveness	New regulations (eg, BCBS 239,[1] Basel AML/KYC[2]) Tighter supervision and increased enforcement action (eg, more than $200 billion in fines since crisis; more than 4,000 MRAs[3] still outstanding from OCC[4])
3. Growing importance of strong data management and advanced analytics in staying competitive	Robust customer-differentiation and risk-decision capabilities (eg, risk-based pricing, targeted segmentation through machine learning) Early-warning detection techniques to identify potential losses and exposures proactively
4. New attackers driving business-model disruptions	Risk management is critical in enabling banks to compete and/or collaborate with fintech companies on products and customer experience Risk can position banks favorably if fintech companies take inappropriate risks ("bets")
5. Increasing pressure, especially from financial-technology companies, on costs and returns	Return on equity for global banking remains below cost of capital despite lower risk losses JP Morgan Chase spending well over $1 billion on risk and compliance; HSBC adding more than 3,000 resources

[1]Basel Committee on Banking Supervision regulation number 239.
[2]Anti-money laundering/know your customer.
[3]Matters requiring attention.
[4]US Office of the Comptroller of the Currency.

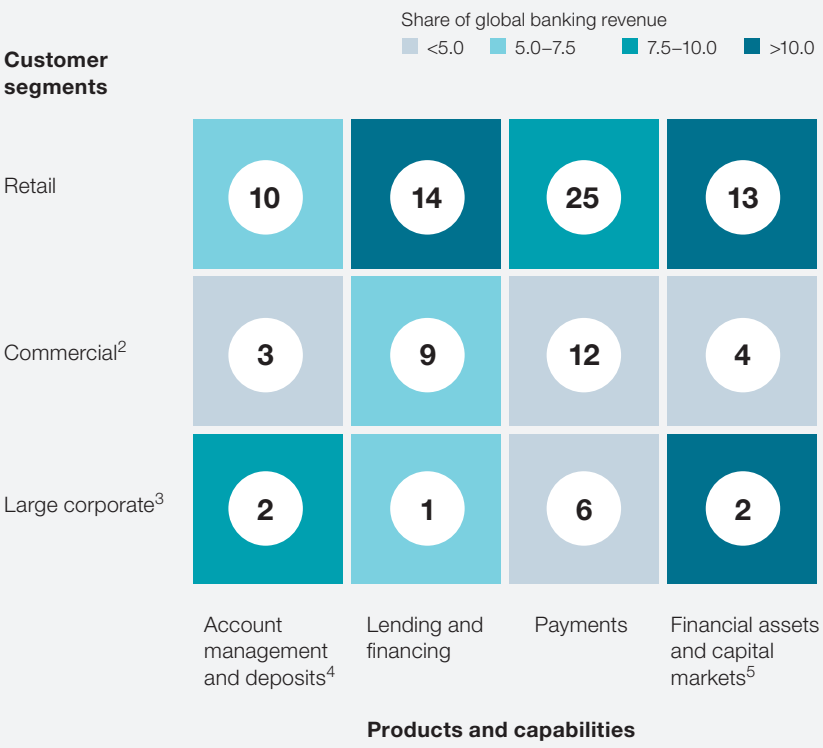
Data management and analytics. Rising customer use of digital-banking services and the increased data this generates create new opportunities and risks. First, banks can integrate new data sources and make them available for risk modeling. This can enhance the visibility of changing risk profiles—from individuals to segments to the bank as a whole. Second, as they collect customers' personal and financial data, banks are mandated to address privacy concerns and especially protect against security breaches.

Fintech companies and other innovative attackers. The digitally savvy segments have responded to innovative offerings from new nontraditional competitors, especially fintech companies and digital-only banks. These start-ups are extending innovation throughout the digital-banking space, creating a competitive threat to traditional banks but also potentially valuable opportunities for partnerships (Exhibit 2).

Exhibit 2

Financial-technology companies are extending innovation in the digital-banking space to all client segments.

Share of fintechs in digital-banking space, % of start-ups and innovations in fintech database, by segment and product[1]



Implications for risk

Faster innovation from thousands of fintech start-ups creates new opportunities in risk management

Potential partnerships are available to accelerate the risk function's transformation

Internet technology is enabling crowdsourcing and risk disintermediation—but also giving banks opportunities to increase connectivity with their clients' digital ecosystems (eg, peer-to-peer lending integration)

[1]McKinsey's financial-technology database includes >350 of the best-known start-ups, but it may not be fully representative for any one segment or product.
[2]Includes small and medium-size enterprises.
[3]Includes large corporations, public entities, and nonbanking financial institutions.
[4]Revenue share includes current-account deposit revenue.
[5]Includes investment banking, sales and trading, securities services, retail investment, noncurrent-account deposits, and asset-management factory.

Pressure on cost and returns. The new competitors are beginning to threaten incumbents' revenues and their cost models. Without the traditional burden of banking operations, branch networks, and legacy IT systems, fintech companies can operate at much lower cost-to-income ratios—below 40 percent.

Fighting back

Banks are beginning to respond to these trends, albeit slowly. Over the past several years, leading banks have begun to digitize core processes to increase efficiency—in particular, risk-related processes, where the largest share of banks' costs are typically concentrated. Most banks started with retail credit processes, where the potential efficiency gains are most significant. Digital approaches can be more easily adopted from well-established online retailers: mobile applications, for example, can be developed to enable the origination of tailored personal loans possible instantaneously at the point of sale. More recently, banks have begun to capture efficiency gains in the SME and commercial-banking segments by digitizing key steps of credit processes, such as the automation of credit decision engines.

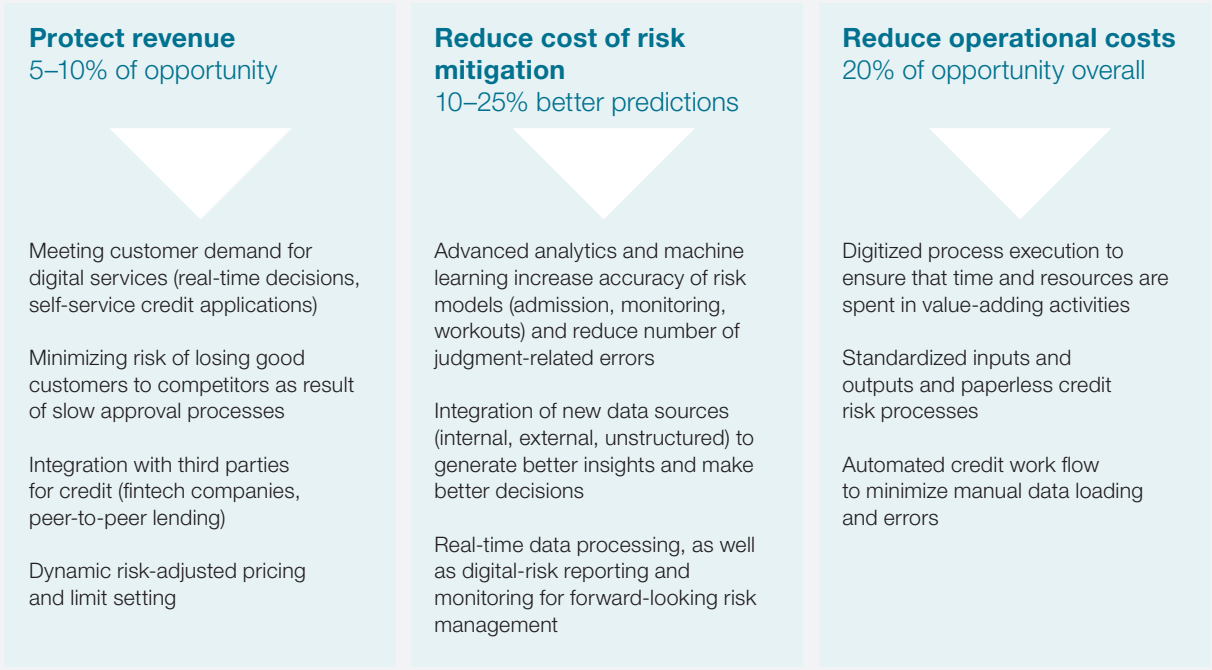
The automation of credit processes and the digitization of the key steps in the credit value chain can yield cost savings of up to 50 percent. The benefits of digitizing credit risk go well beyond even these improvements. Digitization can also protect bank revenue, potentially reducing leakage by 5 to 10 percent.

To give an example, by putting in place real-time credit decision making in the front line, banks reduce the risk of losing creditworthy clients to competitors as a result of slow approval processes. Additionally, banks can generate credit leads by integrating into their suite of products new digital offerings from third parties and fintech companies, such as unsecured lending platforms for business. Finally, credit risk costs can be further reduced through the integration of new data sources and the application of advanced-analytics techniques. These improvements generate richer insights for better risk decisions and ensure more effective and forward-looking credit risk monitoring. The use of machine-learning techniques, for example, can help banks improve the predictability of credit early-warning systems by up to 25 percent (Exhibit 3).

Good progress has been made, but it is only a beginning. Many risk-related processes remain beyond the digital capabilities of most banks. Significant effort has been expended on the digital credit risk interface, but the translation of existing credit processes into the online world falls far short of customer expectations for simple digital management of their finances.

Good progress has been made, but it is only a beginning. Many risk-related processes remain beyond the digital capabilities of most banks.

Exhibit 3 **Digital credit risk management uses automation, connectivity, and digital delivery and decision making to create value in three ways.**



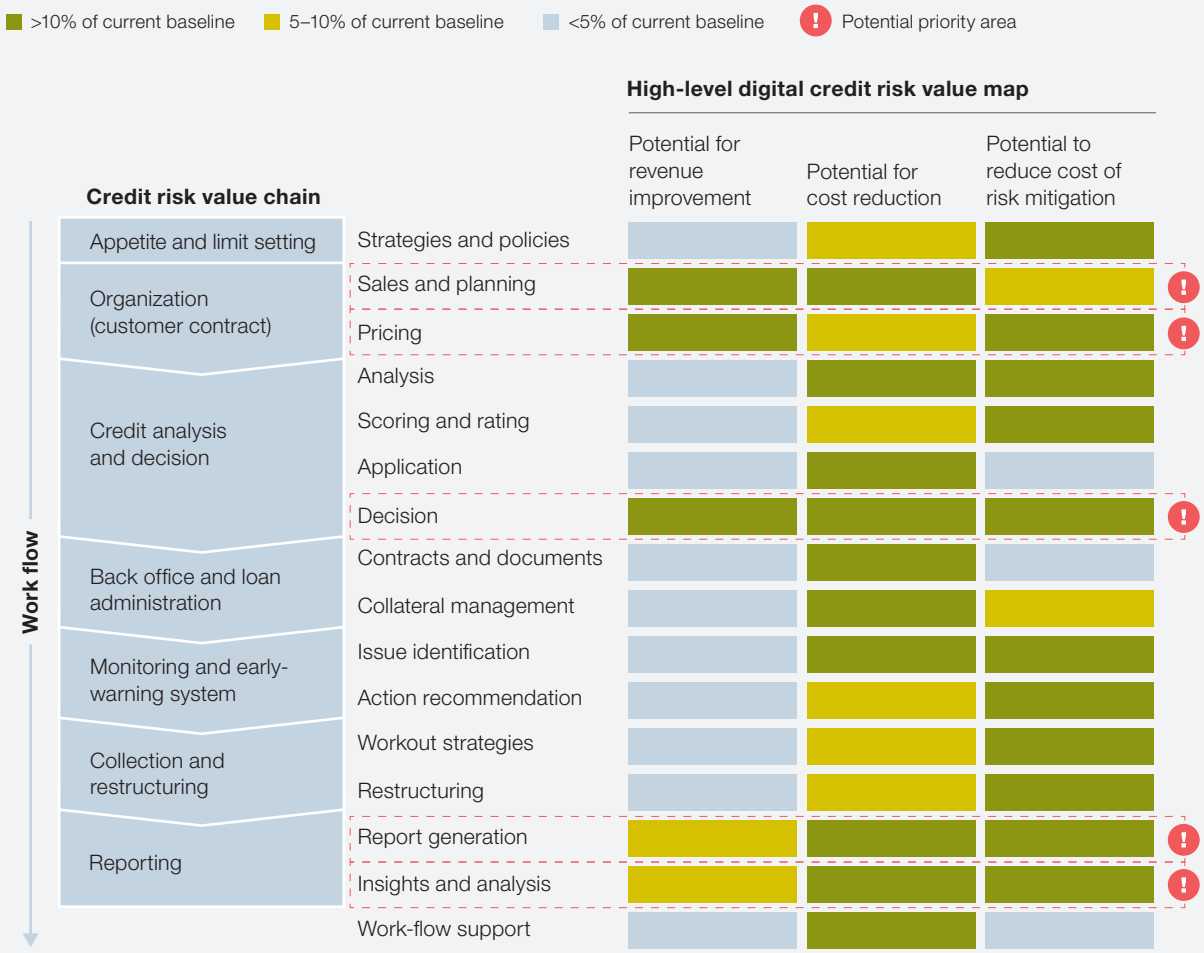
There is plenty of room for digital improvement in client-facing processes, but banks also need to go deeper into the credit risk value chain to find opportunities to create value through digitization. The systematic mapping and analysis of the entire credit risk work flow is the best way to begin capturing such opportunities. The key steps—from setting risk appetite and limits to collection and restructuring—can be mapped in detail to reveal digitization opportunities. The potential for revenue improvement, cost reduction, and credit risk mitigation for each step should be weighed against implementation cost to identify high-value areas for digitization (Exhibit 4).

Some improvement opportunities will cut across client segments, while others will be segment specific. In origination, for example, most banks will probably find that several segments benefit from a digitally connected, paperless credit underwriting process (with live access to customer data). At the stage of credit monitoring and early warning, furthermore, advanced analytics and fully leveraged internal and external data could improve risk models for identifying issues across different segments. Back-office and loan-administration tools such as straight-through processing and automated collateral valuation are also cross-cutting improvements, as are the automation and interactivity of risk reporting.

On the other hand, in credit analysis and decision making, banks will likely find that instant credit decisions are mostly relevant in the retail and SME segments, while the corporate and institutional segments would benefit more from smarter work-

Exhibit 4

To find the areas where digitization will create the most value, map the entire credit risk work flow.



flow solutions. The application of geospatial data, combined with advanced analytics, for example, can yield a high-performing asset-valuation model for mortgages in the retail segment. For collection and restructuring, automated propensity models will match customers in the retail and SME segments with specific actions, while for the corporate segment banks will likely need to develop debt restructuring-simulation tools, with a digital interface to identify and assess optimal strategies in a more efficient and structured way.

How digital credit creates value

Several leading banks have implemented digital credit initiatives that already created significant value. These are a few compelling cases:

1. *Sales and planning.* One financial institution's journey to an interactive front line involved the construction of a digital workbench for relationship managers (RMs). The challenges to optimal frontline performance were numerous and included the lack of systematic skill

building, customer-relationship-management (CRM) systems with a fragmented overview of clients, and difficulty gathering relevant client and industry data. Onboarding, credit, and after-sales processes required many hours of paperwork, drawing frontline attention away from new client meetings. By engaging RMs with the IT solutions providers, the bank's transformation team created a complete set of frontline tools for a single digital platform, including best-practice CRM approaches and product-specialist availability. The front line soon increased client interactions four to six times while cutting administrative and preparation time in half.

2. *The mortgage process.* This presents a large opportunity for capturing digital value. One European bank achieved significant revenue uplift, cost reduction, and risk mitigation by fully automating mortgage-loan decisions. Much higher data quality was obtained through exchange-to-exchange systems and work-flow tools. Manual errors were eliminated as systems were automated and integrated, and top management obtained transparency through real-time data processing, monitoring, and reporting. Decisions were improved and errors of judgment reduced through rule-based decision making, automated valuation of collateral, and machine-learning algorithms. The bank's automated real-estate valuation model uses publicly known sale prices to derive the amount of real-estate collateral available as a credit risk mitigant. The model, verified and continuously updated with new data, attained the same level of accuracy as a professional appraiser. Recognized by the regulator, it is saving the bank considerable time and expense in making credit decisions on actions ranging from underwriting to capital calculation and allocation. Losses were further minimized by automated monitoring of customers and optimized restructuring solutions. The digital engine moved decision making from 5 percent automated to 70 percent, reducing decision time from days to seconds.

3. *Insights and analysis.* By making machine learning a part of the effort to digitize credit risk processes, banks can capture nearer-term gains while building a key capability for the overall transformation. Machine learning can be applied in early-warning systems (EWS), for example. Here it can enable deeper insights to emerge from large, complex data sets, without the fixed limits of standardized statistical analysis. At one financial institution, a machine learning–enhanced EWS enabled automated reporting, portfolio monitoring, and recommendations for potential actions, including an optimal approach for each case in workout and recovery. Debtor finances and recovery approaches are evaluated, while qualitative factors are automatically assessed, based on the incorporation of large volumes of nontraditional (but legally obtained) data. Expert judgment is embedded using advanced-analytics algorithms. In the SME segment, this institution achieved an improvement of 70 to 90 percent in its model's ability accurately to predict late payments six or more months prior to delinquency.

The approach: Working on two levels

While the potential value in the digital enablement of credit risk management can be significant for early movers, a complete transformation may be required to achieve the bank's target ambitions. This would involve building new capabilities across the organization and close collaboration among the risk function, operations, and the businesses. Given the complexity of the effort, banks should embark on this journey by prioritizing the areas where digitization can unlock the most value in a reasonable amount of time: significant impact from applying digital levers can be tangible in weeks.

Rather than designing a master plan in advance, banks can in this context develop a digital approach to one area of credit risk management based on existing technology and business value. Each bank may develop initiatives based on their specific priorities. Banks that most need to increase regulatory compliance and the quality of their execution may begin with initiatives in process reengineering to reduce the number of manual processes or to build a fully digital credit risk engine. Those looking to improve customer value from greater speed and efficiency might implement such initiatives as a state-of-the-art digital credit-underwriting interface, a digitally enabled sales force, data-driven pricing, or straight-through credit decision processing. Banks needing to mitigate risk through better decision making may develop initiatives to automate and integrate early-warning and recovery tools and create an automated, flexible risk-reporting mechanism (a "digital-risk cockpit").

A credit risk transformation thus requires banks to work on two levels. First, look for initiatives that are within easy technological reach and that will also advance the core business priorities. Launching initiatives that bring in savings quickly will help the transformation effort become self-funding over time. Once a first wave of savings is captured, investments can be made in building the digital capabilities and developing the foundation for the overall transformation. Based on what has been learned in early-wave initiatives, moreover, new initiatives can be designed and rolled out in further waves. Typical first-wave initiatives digitize underwriting processes, including frontline decision making and reporting. Risk reporting is another likely candidate for early digitization, since digitization reduces production time and leads to faster decision making.

Building digital capabilities: Talent, IT, data, and culture

The experience of specific initiatives will help shape digital capabilities for the long term. These will be needed to support the overall digital transformation of credit risk management and keep the analytics and technology current. To begin, banks can examine their current capabilities and assess gaps based on the needs of the transformation. The talent focus in risk and across the organization will likely shift as a result toward a greater emphasis on IT expertise and quantitative analytics.

In addition to enhancing their talent profiles, banks will have to shift the direction of their IT architecture. The target will likely be two-speed IT, a model in which the bank's IT architecture is divided into two segments. Accordingly, the bank's core (often legacy) IT systems constitute a slower and reliable back end, while a flexible and agile front end faces customers. Without a two-speed capability, the agility needed for digital credit risk management would not be attainable.

Along with the supporting IT architecture and analytics talent, improved data infrastructure is an essential digital capability for the credit risk-management transformation. The uses of data are disparate throughout the bank and will continually change. For big data–analytics projects, great quantities of data are needed, but how they should be structured is not usually apparent at the outset. The construction of separate data sets for each use, furthermore, creates as many data silos within the organization as there are projects.

For these reasons, some leading companies are moving toward utilizing a "data lake"—an enterprise-wide platform that stores all data in the original

unstructured form. This approach can improve organizational agility, but it requires that each project has the capability to structure the data and understand data biases. All types of data infrastructure also pose security risks, moreover, which can be addressed only by IT experts. Finally, the reconfiguration of the data infrastructure needs to be done using methods that carefully respect legal privacy barriers and meet all regulatory requirements.

Last, building and maintaining a strong digital-risk culture will be of critical importance in ensuring the success of the risk function of the future. A shift in culture and mind-set is needed among employees, top executives, and regulators, as they acclimate themselves to the new digital credit environment. Here, machines and automation have a much greater role, while human capabilities are developed to support the continual improvement of the risk culture. The focus shifts from executing a risk process to managing true control systems that continuously detect, assess, and mitigate risks.

Toward a flexible digital-risk end state

From data input and management to decision making, from customer contact to execution, the initiatives should build step by step toward a seamless and interactive digital-risk function. The initiative-first approach builds in the capability of agile adaptation to changes in customer demand or the competitive and regulatory environments. The digital opportunities and the way banks address them, in other words, will continually evolve, and the digital end state must support such changes while maintaining enhanced risk-management and client-service capabilities.

The digital transformation of existing credit risk tools, processes, and systems can address rising costs, regulatory complexity, and new customer preferences. The digital enablement of credit risk management means the automation of processes, a better customer experience, sounder decision making, and rapid delivery. Digital-risk management will be the norm in the industry in five years, and banks that act now can attain enduring competitive advantage. ■

[1] The Comprehensive Capital Analysis and Review is the Federal Reserve's regulatory framework for evaluating the capital-planning processes and capital adequacy of large financial institutions; BCBS 239 is the Basel Committee on Banking Supervision's directive on addressing gaps in banks' risk-data aggregation and reporting. Both mechanisms have complex requirements and tight compliance deadlines. The asset-quality review (AQR) conducted by the European Central Bank in 2014 on 80 percent of EU banking assets helped determine capital adequacy and reduce overvaluation in balance sheets. The AQR prepared the way for the rollout of the Single Supervisory Mechanism.

Juan Antonio Bahillo is a partner in McKinsey's Madrid office, **Saptarshi Ganguly** is a partner in the Boston office, **Andreas Kremer** is a partner in the Berlin office, and **Ida Kristensen** is a partner in the New York office.

SREP: How Europe's banks can adapt to the new risk-based supervisory playbook

The first round of Europe's new supervisory process is in the books, and the next one is under way. Banks are likely to face new challenges from heightened supervisory expectations.

Giorgio Bonomo, Sebastian Schneider, Paolo Turchetti, and Marco Vettori

A new approach to bank supervision is taking hold in Europe for banks within the purview of the Single Supervisory Mechanism. This year's stress tests of the European Banking Authority (EBA) and European Central Bank (ECB) will soon be over. The results will help shape this year's Supervisory Review and Evaluation Process (SREP), an approach that introduces three fundamentally new principles to banking supervision: a forward-looking focus on the sustainability of a bank's business model (even under stressed conditions), an assessment system that uses industry best practices as a guide, and an expectation that all banks eventually will reach the same high standards.

Early this year, the ECB announced its five supervisory priorities for 2016: business model and profitability risk, credit risk, capital adequacy, risk governance and data quality, and liquidity.[1] This article will review the lessons from last year's process, explain the role of these priorities in this year's SREP, and outline banks' responses. An adequate response is crucial; banks that score poorly may face increased regulatory capital requirements and more intense supervisory scrutiny in the future.

Success—but only a trial run

The first SREP took place in 2015, and supervisors have already told banks their findings. Critically, these findings had the power of peer-to-peer comparison. Previous supervisory reviews were conducted by different national authorities, using a range of practices, which made it difficult to compare banks or to draw fair conclusions about areas such

as capital adequacy. The ECB now supervises the 129 largest banking groups in the eurozone, or about 82 percent of the banking sector's total assets, through a common supervisory approach.

The 2015 SREP assessment was a significant step forward in the creation of a level playing field for banks in the eurozone, even if disclosures on the process followed and outcomes are still limited. Bank supervisors are now able to use one yardstick to measure the capital adequacy of banks in geographies where Pillar 2 implementation lagged or where banks generally "ticked the box" rather than truly assessed their capital resilience.

Banks came through the first review with a broad range of outcomes, as expected from the first-time application of a standard assessment after years of varied supervision. The ECB reported in March that many banks did not yet have sound liquidity-management plans, and capital adequacy remains a concern. But the process also led to the creation of a cybercrime-incident database and a way for banks to report cybersecurity lapses. In general, the new process was a learning experience. Banks were required to devote more time and resources to manage extensive data and documentation requests than ever before.

Our analysis shows that some of the areas that are problematic in Europe have also been vexing US bank supervisors: inadequate corporate governance and risk-management processes and procedures, particularly as they relate to integrating a risk-appetite framework into a bank's strategic planning and operations, and inadequately involved boards of directors with limited understanding of their risk-management responsibilities. Coming from very different starting points, it seems the regions are eventually converging toward common principles.

2016 priorities

Many banks may consider their 2015 SREP experience a success. But before they get too comfortable, they must recognize that it was limited in scope. While certain topics—particularly the risk-appetite framework, board-level governance, and cybersecurity—were in the spotlight, the initial SREP was mainly a test run to get the processes in motion. This year's process is framed more broadly. Liquidity management and capital adequacy, sticking points from the 2015 review, will be examined in more detail. While no one yet knows the full impact of the recent Brexit vote, we are assessing potential scenarios. The constant among them is that increased market volatility will no doubt add further pressure on liquidity and capital management. Other 2016 priorities include business models and profitability, credit risk, and risk governance and data quality.

Beyond 2016, we expect the SREP to continue to evolve. As supervisors delve deeper into banks across borders, we anticipate that certain best practices will emerge that should be emulated. Banks' key processes (such as strategic and capital planning and day-to-day decision making) will need to show a higher level of integration with risk-management processes (for example, risk-appetite definition and stress testing), and the latter will be subject to more robust use tests.

As their risk and business teams engage with the 2016 priorities, detailed below, bank executives and boards of directors will have to demonstrate to supervisors that they are in charge of the SREP assessment dimensions. They should aim for strategic, material improvements in risk management, rather than formal compliance. They should project a positive outlook rather than solely focusing on defense of the status quo. And they should make sure that their SREP efforts are centrally coordinated, so that strategic implications are integrated into structural decision making and investments are prioritized by their relevance to the specificities of the business model. They must also be actively involved in supervisory discussions, which will improve those relationships.

Viability of business models

Although bank profitability slightly improved in 2015 and capital positions have further strengthened, European banks continue to struggle with diminished profitability in the ultra-low (or even negative) interest-rate environment. This is forcing banks to transform their business models as they search for alternative sources of income and re-base their cost structures. In fact, the German Federal Financial Supervisory Authority said in May that banks might have to consider creating a business model in which interest income plays only a minor role. While investors tend to look solely at return on equity, supervisors want to make sure that the business model and the returns it produces are sustainable, even in an economic downturn.

To meet supervisory expectations embedded in the SREP approach—in particular, in the pillar "analysis of the business model"—we believe banks must upgrade their capabilities on three key dimensions:

- *Strategic-planning process.* Banks need to demonstrate that they can promptly adapt their strategy to material changes in the macro-economic and competitive environment. To achieve this, the annual strategic-planning and budgeting process will need to become more dynamic. The coherence and consistency of the scenarios (baseline and stressed) used for strategic planning and budgeting must be continually tested and a new iteration needs to be triggered whenever such scenarios do not hold.

- *Models and methodologies for projections.* Projections used in banks' balance sheets and profit-and-loss statements have dramatically changed, mainly due to the Comprehensive Capital Analysis and Review exercises. The so-called pre-provision-net-revenue models (and all other macroeconometric models to project banks' key economics) have reached such a level of maturity and detail that they should no longer be ignored when it comes to running core decision-making processes such as strategic planning. Their value goes beyond compliance: they can provide banks with superior understanding of the behavior of their business model under different scenarios, which in turn will enhance more effective decision making.

- *Validation and back-testing.* While banks are accustomed to validating and back-testing models in areas such as credit underwriting, they are not used to doing so in strategic planning. We expect such validation and back-testing to become key elements in proving the effectiveness of the strategic-planning and budgeting process. As an example, banks may be asked to show that the number and materiality of deviations of results versus budget and strategic plans decreases over time, or to distinguish scenario-related deviations from those that stem from performance.

Credit risk: Profitability concerns from impaired assets

European banks also face significant challenges from their high levels of impaired assets. A weak economy has left banks in many countries with elevated levels of nonperforming exposures (NPEs). These remain a concern and a potential inhibition to lending growth and profitability. More important for individual banks, the level of NPEs is seen as a key factor in SREP. Across the European Union, NPEs are close to 6 percent of total loans and advances, and about 10 percent of exposures to nonfinancial corporations. The general trend shows that the smaller the banks, the higher the NPE ratios.

NPE levels are particularly high in Southern Europe, as well as in several Eastern European countries. High NPEs burn up bank capital, deteriorate funding costs, and reduce bank profitability, all of which serves to dry up credit supply. Reducing NPEs quickly is crucial to stimulating credit growth, especially for small and medium-size enterprises

that rely heavily on bank financing. But write-off rates for European banks remain extremely low. Some national supervisors have allowed banks to deal with large NPE backlogs through business-as-usual processes. In a positive development, national stress tests in some jurisdictions, coupled with the EU-wide comprehensive-assessment exercise, led to waves of write-downs. And markets for distressed debt in Europe are slowly evolving, allowing the entry of much-needed capital and expertise.

In the future, NPE levels will remain the focus of supervisors who will want to see that banks can keep the cost of credit risk under control. In the short to midterm, banks will want to leverage both organic and inorganic strategies and review their workout processes and tools to make sure they are in line with supervisory expectations. Over the longer haul, a material upgrade of credit risk-management capabilities will require strong investments in IT and technology—and analytics, which will help banks select the most suitable portfolios to meet investors' appetites.

Capital adequacy and liquidity risks

Banks often think of these as two sides of the same coin, and we will deal with both here. Banks must have "robust strategies, policies, processes, and systems" to identify, manage, and monitor liquidity and capital risks, according to the December 2015 draft guidelines for the Internal Capital Adequacy Assessment Process (ICAAP) and the Internal Liquidity Adequacy Assessment Process (ILAAP). Banks are expected to design their own forward-looking, risk-based ICAAP and ILAAP frameworks, based on both quantitative and qualitative factors.

We expect ICAAP and ILAAP to play an increasingly important role within SREP. New EBA stress-testing requirements clearly indicate that 2016 results will be used in SREP to challenge banks' own capital plans. Supervisors will also use benchmarking to derive top-down indications on capital and liquidity adequacy. Ongoing discussions in Europe also show an increasing skepticism from supervisors and investors about the possibility of using Pillar 1 capital requirements to measure capital adequacy. In this context, a sturdy ICAAP and ILAAP will represent the best chance for banks to adequately measure (and report to the supervisor) their capital and liquidity risks.

For ICAAP, a robust framework should allow a reconciliation of banks' internal stress-test results with regulatory exercises (for example, based on the EBA methodology and scenarios). Top management and the board should discuss the results to derive business implications. Results should be made consistent with the inputs used for risk-appetite setting and strategic planning, even

Over the longer haul, a material upgrade of credit risk-management capabilities will require strong investments in IT and technology—and analytics, which will help banks select the most suitable portfolios to meet investors' appetites.

if calibrated differently. The findings should be easily disaggregated by risk type and business unit with sufficient detail (for instance, at the portfolio level). Business-unit leaders should have a proper understanding of risk drivers, as well as the opportunity to challenge the results based on the outcomes of risk-identification exercises conducted at the level of the first line of defense. Most institutions won't be able to reach such a level of integration with management processes without first transforming data, infrastructure, models, methodologies, and their risk culture. Banks will need a credible program to enhance these skills to meet supervisory expectations.

Risk governance and data quality

Supervisors want to make sure that banks are collecting the right risk data and delivering the right reports to enable effective management and board decision making. Supervisors are expected to focus on data aggregation and quality this year, as well as to continue their ongoing thematic reviews of risk appetite and risk governance.

Large financial institutions, particularly the globally systematically important banks, have already complied with many of the requirements in the Basel Committee on Banking Supervision's 2013 risk-data aggregation and risk-reporting guidance (BCBS 239), which were due in January 2016. Most European banks have kept their BCBS 239 teams in place, so that they can complete work on supervisors' priorities, including infrastructure transformation, quality-control systems (data and reporting), automation, adaptability in times of stress, and regulatory-response management. These teams can also ensure compliance with new regulatory requirements (such as those arising from International Financial Reporting Standard 9 and from Basel's new Pillar 3 requirements and its Fundamental Review of the Trading Book) and independently validate the program.

As the availability, timeliness, and quality of risk information have improved, top managers and boards have come to see that their banks are less skilled at anticipating risk. Complete solutions rely on new infrastructure and models, as mentioned above, though much can be done by just reengineering the current risk-identification and measurement processes. Some institutions are moving in this direction by setting up structured risk-identification and measurement exercises, conducted at the first line of defense and coordinated by risk management.

Regarding risk appetite and governance, banks must also focus on supervisory concerns from 2015 that they have not fully addressed. We see three potential areas of attention.

To start, *banks should integrate the risk appetite with strategic planning and budgeting* from the very start of the strategic-planning process. While many banks have taken formal steps in this direction, some still fall substantially short of compliance. Strategy and risk teams should work together to formulate potential risk-return scenarios for the contemplated strategic directions. These scenarios should produce specific combinations of risk-return targets and limits and should take account of stress tests. The scenarios should then be offered to the board for approval prior to the articulation of a specific business/risk strategy.

Second, *risk-appetite policies and procedures must reach every business unit and portfolio level.* This is a challenge for many institutions, mainly because they haven't come up with the proper methodology and analytics to disaggregate risk targets and limits for each business unit and then align these with the corporate center. We suggest that banks act on several fronts, including improving risk-appetite metrics, developing key performance indicators that can link to actual

business drivers, and double-checking that tools, policies, and strategies throughout the company are consistent with the framework. Banks should also review business-unit incentive systems and train line managers (and board members of subsidiaries, where relevant) on the risk-appetite process.

Finally, the *risk appetite must cover all the potential risks a bank might face* to avoid the possibility that an overlooked risk could poison the entire risk-mitigation effort. One of the lessons learned from the financial crisis was that the institutions that used multiple measures of risk were able to avoid significant unexpected losses more than those that focused on a limited set of key metrics. That is why it is so important for banks to instill a consistent, forward-looking, and especially multidimensional set of limits across risk types, legal entities, and business divisions.

Identifying uncovered risks and developing metrics to monitor them is an enormous task; new risk categories such as nonfinancial, strategic, and model risks are continually emerging. Banks need to balance the trade-off between comprehensiveness of the risks covered and effectiveness of the risk-appetite framework as a managerial tool to steer the bank. A long list of metrics will most likely dilute the board's risk discussions, rather than enhance them. One possible way to manage risk metrics is to consider a two-level risk-appetite approach. Management informs the board on all the metrics for which it has defined a risk appetite; among the rest, it selects only representative metrics for board reporting and discussion. The remaining metrics may be tested each year to decide whether they should be included, or reported only when certain thresholds are breached.

Perhaps the best thing that banks can do to be ready for SREP is to develop a consistent habit of self-assessment, so that they can identify their own best practices—and weaknesses—before examiners come knocking on the door. Providing a good outlook rather than just defending the status quo requires an integrated program on how to correct deficiencies, have clear sponsorship from top management, and create a positive track record on the advancements. Banks that are able to show that such elements are in place will be able to outperform in the assessment and will eventually be recognized as such by the market. ■

[1] "ECB Banking Supervision publishes priorities for 2016," European Central Bank, January 6, 2016, bankingsupervision.europa.eu.

Giorgio Bonomo is a senior expert in McKinsey's Milan office, where **Marco Vettori** is a partner; **Sebastian Schneider** is a partner in the Munich office; and **Paolo Turchetti** is an associate principal in the Rome office.

July 2016
Designed by Global Editorial Services

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.