

McKinsey on Risk

Highlights



12

Nonfinancial risk today:
Getting risk and the business aligned



18

Protecting your critical digital assets: Not all systems and data are created equal



23

From scenario planning to stress testing: The next step for energy companies

Number 2, January 2017

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:

© kksteven/Getty Images

Editorial Board:

Kyra Blessing, Richard Bucci, Raúl Galamba de Oliveira, Maria Martinez, Theodore Papanides, Thomas Poppensieker, Kayvaun Rowshankish, Anthony Santomero, Himanshu Singh, Mark Staples

Manager of Risk External

Relations: Kyra Blessing

Editors: Richard Bucci, Mark Staples

Contributing Editors:

Lisa Getter, Jonathan Turton

Art Direction and Design:

Leff Communications

Managing Editors:

Michael T. Borruso, Venetia Simcock

Editorial Production:

Elizabeth Brown, Heather Byer, Roger Draper, Torea Frey, Heather Hanselman, Gwyn Herbein, Katya Petriwsky, John C. Sanchez, Dana Sand, Karen Schenkenfelder, Sneha Vats, Belinda Yu

McKinsey Practice Publications

Editor in Chief:

Lucia Rahilly

Executive Editors:

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

Copyright © 2017 McKinsey & Company. All rights reserved.

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

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

Table of contents



3

Sustainable compliance:

Seven steps toward effectiveness and efficiency

Banks do not control the demand for compliance, but they can optimize the effectiveness and efficiency of their response.



12

Nonfinancial risk today:

Getting risk and the business aligned

Both must be deeply involved to avoid costly errors.



18

Protecting your critical

digital assets: Not all systems and data are created equal

Top management must lead an enterprise-wide effort to find and protect critically important data, software, and systems as part of an integrated strategy to achieve digital resilience.



23

From scenario planning to stress testing: The next step for energy companies

Utilities and oil and gas firms have long used scenario analysis, but extraordinary times call for new measures.



29

The evolution of model risk management

An increasing reliance on models, regulatory challenges, and talent scarcity is driving banks toward a model risk management organization that is both more effective and value-centric.



37

Digital risk: Transforming risk management for the 2020s

Significant improvements in risk management can be gained quickly through selective digitization—but capabilities must be test hardened before release.

Introduction

Welcome to the second issue of *McKinsey on Risk*, the journal offering McKinsey’s global perspective and strategic thinking on risk. Our focus is on the key risk areas that bear upon the performance of the world’s leading companies—including 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.

Response to our first issue exceeded expectations and generated strong interest among risk leaders and senior executives generally. An overarching theme in those articles was the importance of breaking through siloed approaches to achieve an enterprise-wide view of risk, with the strategic response centered on the needs of the business. The articles in this issue deepen our commitment to these themes. Areas of focus are automation and digitization—specifically, how leading companies are applying technological innovation to control costs while improving risk effectiveness.

We begin with a consideration of how financial institutions can manage compliance risk sustainably, by addressing its root causes rather than adding layers of control. A second article takes up a related theme, focusing on nonfinancial risk and a unified risk-assessment system to help companies avoid or reduce the impact of failures. The urgent topic of cybersecurity is addressed in the next piece, which argues for an enterprise-wide approach that prioritizes key risks based on the business and its value chain. Then we discuss how, in a volatile global environment, energy companies can use stress testing in strategy development and to avoid the normalizing biases of traditional financial scenario analysis. Model risk is the topic of a further piece, which presents insights from McKinsey’s experience with leading global banks and indicates an evolutionary path for model risk management toward capturing value. Our final article discusses “digital risk”—all the technological advances that improve the effectiveness and efficiency of risk management, from process automation to advanced analytics and machine learning to artificial intelligence and robotics.

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, the previous issue of *McKinsey on Risk*, and many others at McKinsey.com and on the McKinsey Insights app.



Raúl Galamba de Oliveira
Chair, Global Risk Editorial Board,
for McKinsey’s Global Risk Practice



© olaser/Getty Images

Sustainable compliance: Seven steps toward effectiveness and efficiency

Banks do not control the demand for compliance, but they can optimize the effectiveness and efficiency of their response.

Piotr Kaminski, Daniel Mikkelsen, Thomas Poppensieker, and Kate Robu

The cost of regulatory compliance in banking rose dramatically in the years after the financial crisis. Some of the increase came from investment in technology, but most of it was—and remains—driven by additional staff. The crisis triggered numerous critical control failures that required immediate remedy. Institutions responded, appropriately enough given the urgency, by adding layers of control. An idea of what resulted can be seen in a typical example. At a large universal bank, a quarter of one business unit's resources is now dedicated to control, significantly reducing the share focused on the business (Exhibit 1). While the exact numbers will vary by institution and business unit, what's certain is that more resources than ever before are being

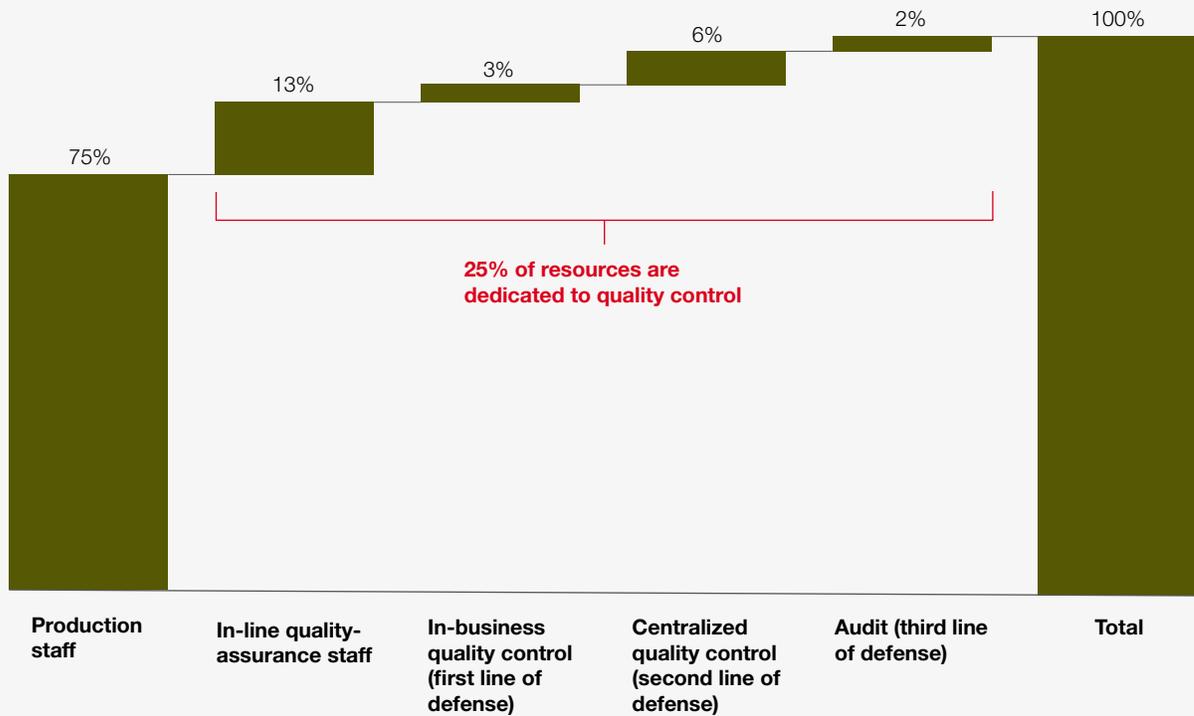
dedicated to testing, monitoring, and other oversight responsibilities—at the expense, given budget limits, of production resources.

The investments have magnified industry resilience and improved the quality of risk management. The high cost, however, is now coming into focus. At many financial institutions, business, compliance, and risk practitioners are beginning to question the sustainability of the resource-intensive approach to managing compliance risks. We believe they are asking the right question. Banks are still adding layers of control as the remedy of choice for compliance issues. The result is an unwieldy “system” of overlapping controls that is difficult to automate and does not address the true root

Exhibit 1

More resources than ever before are being dedicated to testing, monitoring, and other oversight responsibilities.

Breakdown of FTEs¹ across lines of defense,² US banking example



¹ Full-time equivalents.

² Figures may not sum, because of rounding.

causes of risk. Arising issues are approached one at a time and in isolation; remediation efforts are inadequately measured and tracked.

Fragmented efforts, manual processes, mountains of data

We analyzed the time spent on remediation at one global financial institution according to the importance (materiality) of the issue. We found that first- and second-line compliance staff were spending 80 percent of this time on issues of low or moderate materiality, and only 20 percent on critical high-risk issues. The issues were approached individually, according to an “issue log” with

thousands of entries. Unsurprisingly, separate remediation initiatives and audit reports were often directed at the same processes and had the same underlying causes. These could have been addressed systematically, but individual projects did not have the budget to take that on. Only when the institution took an enterprise-wide view did the case for IT investment become clear.

The status quo approach to compliance does not allow for an integrated view across the enterprise. The approach to risk assessment is fragmented: some risks are covered by multiple assessments and others not at all. Nor does a consistent

understanding of the material risks emerge, as the varying standards of materiality and testing produce conflicting results across the organization. Compliance, activities relating to banking secrecy and anti-money laundering (BSA/AML), operational risk, third-party risk, and other assessments are performed frequently by separate teams applying different approaches, and much effort is expended in reconciling the outputs. At one large financial institution, we found that business leadership teams are required to participate in 20 or more risk-assessment activities annually, led by the various control functions. Yet despite all this labor, top management still cannot obtain a reliable view of the institution's biggest compliance exposures nor on the state of controls governing them.

Many leading institutions have tried to shift compliance frameworks toward a more risk-based approach. They have struggled to escape an orientation to procedural adherence and refocus on residual risk (outcomes). Metrics present another challenge. Rather than forward-looking measures of risk, many are ill defined and generate data with unclear implications. As mountains of details pile up, critical exposures can get lost easily. Legacy controls remain in use as new metrics are added. Many intermediate controls and testing can be removed, however, as a recent efficiency effort at a bank's consumer business demonstrated. The needed solution (expanded sample-based quality-assurance testing on executed affidavits) was simpler, less time consuming, and more effective in disclosing material exposures. And it was less costly than the existing haphazard system.

The value in sustainable compliance

The aim of a sustainable compliance program is to improve the bank's risk profile through a more effective and efficient compliance function focused on the most important risks. The approach both centers on material risk and eliminates inefficient activities. In our experience, it can free up to

30 percent of the compliance function's capacity (Exhibit 2). The size of the opportunity depends on the starting point of the bank: leaner institutions will benefit from effectiveness improvements, while institutions with heavier quality-assurance, control, and audit structures will additionally benefit from meaningful efficiency savings.

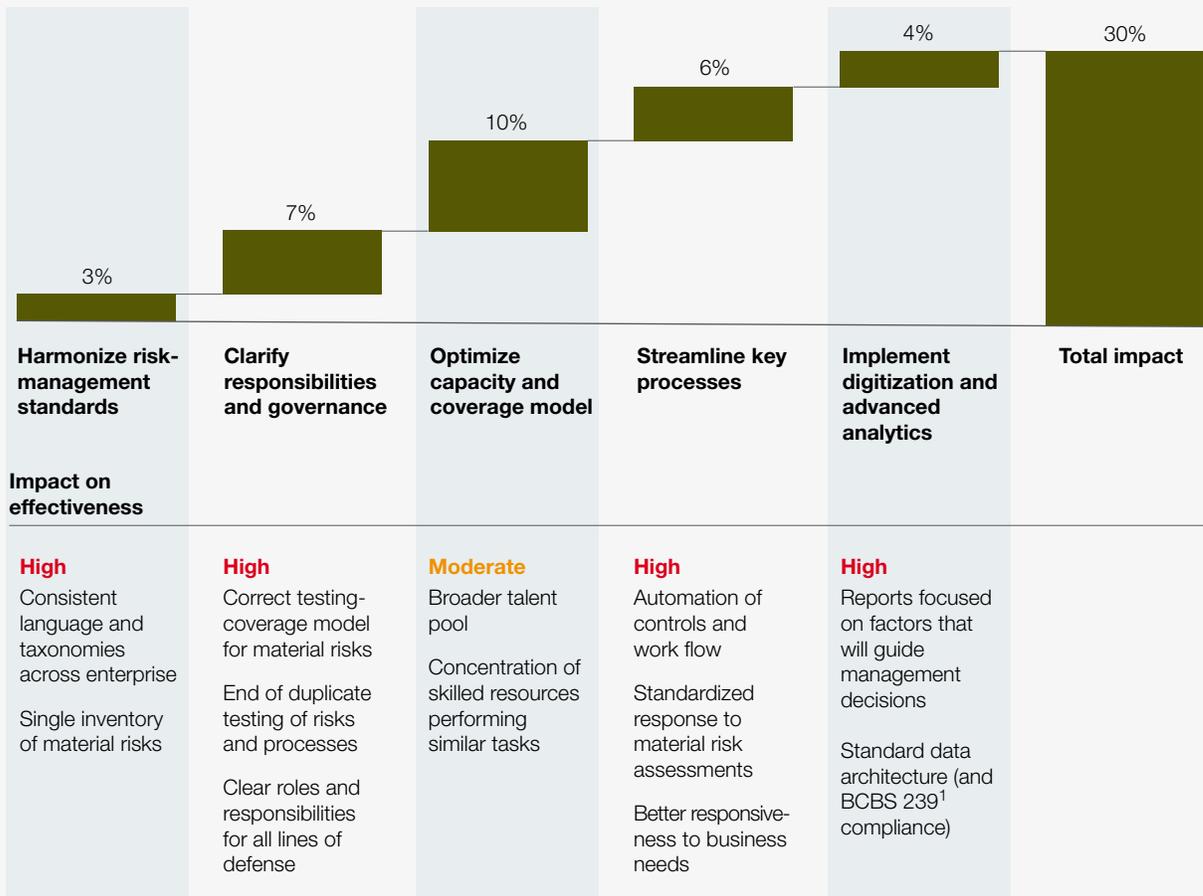
One global financial institution recently developed a set of initiatives to free up 20 percent of capacity in its risk and compliance functions. The starting point was organizationally heavy: the two second-line functions accounted for one-third of corporate function expenses. The resource footprint was 95 percent concentrated in high-cost metropolitan areas with very competitive talent markets. At the same time, effectiveness was inadequate, as evidenced by a growing backlog of regulatory issues and audit findings. Risk-management standards, including taxonomies and tolerances, varied across and within lines of defense; "shadow" testing and monitoring activities were being performed by business lines (the so-called one-and-a-half line of defense); and modeling, analytics, and reporting activities were fragmented across the first and second lines.

The improvement program prioritized initiatives that enhanced the effectiveness of compliance and risk-management activities and their efficiency, to achieve a sustainable operating model to support future growth. Better effectiveness was sought by taking a proactive approach to help the business manage material risks. Rather than reacting to issues, the bank would diagnose root causes and translate regulations into operational requirements. Effectiveness was further fostered through timely and adequate transparency into the state of risks and controls, and increased confidence that no material risk would be left unattended. The functions became more efficient through the automation of tasks and controls and easier access to qualified talent. The resource footprint was optimized, aligning it with

Exhibit 2

A program for sustainable compliance can free up to 30% of the function’s capacity, improving the effectiveness of risk management.

Potential impact on total compliance capacity



¹ Basel Committee on Banking Supervision’s regulation number 239.

business and strategic needs. Resource allocation could then focus on material risks, boosting staff productivity. Nonessential work was minimized, including the remediation of low-materiality risks. Testing, reporting, and other activities were rationalized across the three lines of defense; duplication, especially in the control functions (such as remediation tracking and risk identification and assessment), was largely eliminated.

Building it: Seven steps to sustainable compliance

Compliance practitioners point out that compliance activities are triggered by regulatory requirements and by how well businesses manage regulatory risks. Regulatory demands, they argue, are outside the control of the compliance function, while the adroit management of regulatory risks takes time to mature. In our view, the key to sustainable

compliance is how well the compliance function responds to these demands. Below we lay out seven practical steps that institutions can take to move closer to sustainable compliance.

1. Transform frontline units into a true first line of defense.

At many institutions, frontline units have “outsourced” a significant portion of their compliance responsibilities to the second line of defense, relying on the compliance function for everyday compliance-related business and control decisions. At other institutions, both lines of defense are involved in similar activities, leading to duplication and fragmentation of effort. These two faulty approaches are avoided when roles and responsibilities are appropriately defined. There is real value in having a strong first line of defense handling everyday business and in-line control activities. The role of the second line varies based on the type of compliance requirements. Some regulations can be translated into a set of clear operational requirements—this is called “rules-based compliance.” Other regulations, such as consumer protections, reflect regulatory intent for a desired outcome. This is called “principles-based compliance,” which does not easily convert into specific operational and control requirements.

For rules-based compliance, the second line needs to define clear standards and shift in-line execution and approval (such as consumer disclosures) to the first line of defense. For principles-based compliance, some decisions (such as the suitability of marketing materials) need to be embedded in the first line with adequate training, certification, and monitoring. Conduct risk in retail banking, for example, will present challenges in defining first- and second-line roles and testing and monitoring responsibilities. The compliance function will need to clearly articulate regulatory requirements for disclosures, adverse action, advertising, and

privacy—and then provide technical expertise as business lines translate those requirements into operational procedures, practices, and controls. Compliance also needs to define requirements for training and certification (including in general areas such as product design and usage and fair and nondiscriminatory treatment), and ensure that they are met by all relevant stakeholders. The execution of control, such as authorizing accounts or approving new products, should, however, be embedded in the first-line processes. The second line will focus on independent approval and risk-based testing to ensure that controls do indeed work as intended.

As the second line, the compliance function defines and monitors control standards; the complementary role for the first line is to manage those controls more strategically. Accordingly, the control office in each business unit organizes how the front line manages its control environment—the front line reviews the business setup against the controls in the context of the inherent risk profile and business complexity. When global banks streamline their business footprint (for example, by offering products across markets or the customer portfolio), the related business processes and systems become essential in managing the inherent risk profile.

2. De-risk and reengineer business and compliance processes.

The demand for compliance resources can be significantly reduced by reengineering labor-intensive activities for core compliance processes, such as onboarding or transaction approvals. For control breaches, root-cause analysis is critically important. This will ensure that the true underlying drivers will be revealed for effective, lasting remediation. Further similar breaches—and the consumption of further resources, such as the addition of more checkers—are eliminated by the automation and redesign of the exposure areas. An

additional important measure is the development of consolidated risk-assessment requirements across control functions for key business decisions. This way, duplicate functional controls—such as legal, BSA/AML, information security, and compliance requirements for new clients—can be eliminated and businesses freed from repetitive requests.

For one wealth-management company, automation of know-your-customer (KYC) controls reduced the turnaround time for the new-customer-onboarding process from five or six days for the most complex institutional accounts to 24 hours. The cost of KYC was reduced by more than 70 percent and the customer experience dramatically enhanced. These savings of time and money were possible because the institution tackled KYC requirements, along with credit-process digitization, as an integrated reengineering and automation program. The initiative was built on the understanding that the end-to-end process is no faster than its weakest link—which is often the compliance requirements.

3. Optimize the compliance operating model.

The compliance resources needed to support the business units can be configured most effectively and efficiently by consolidating subject-matter expertise and core activities in centers of excellence and utilities. This will help ensure that the best expertise is applied across channels in business-unit-facing compliance teams. Additionally, the opportunity in optimizing the location strategy for compliance is often sizable. A new look at location could lead to lower structural costs for compliance and offer access to global talent markets to tackle the challenges posed by talent scarcity in traditional locations. A diversified geographic footprint also ensures greater resilience in the face of adverse business or market events.

4. Focus on what matters.

Compliance with laws, rules, and regulations is viewed by banks as a zero-tolerance activity.

Nevertheless, the time spent on each compliance demand must be differentiated according to the bank's highest sensitivities and biggest risks in noncompliance. Time and resources, that is, should be allocated to the risks that matter most. Usually at the top of the list are finance laws and customer and market conduct.

Detailed adjustments can be made in the frequency of testing and sample sizes, depending on the level of inherent exposure in a given operational area. Moreover, testing and remediation activities can be risk-ranked and embedded in resource- and investment-allocation processes. Compliance priorities can then be regularly reassessed to account for new risks, defective controls, and business or regulatory changes.

Ongoing prioritization based on risk requires that organizations objectively measure residual risk exposures and know where in the business process controls can potentially fail. Understanding where the critical breakpoints occur in business processes and having a manageable set of quantitative, forward-looking metrics for each process breakpoint are critical capabilities. For risks that are difficult to quantify (such as internal conduct or fair and responsible banking), banks can develop qualitative risk markers. Trends in staffing levels or changes in business processes and technology often correlate with increased risk. Even if quantitative metrics that directly measure residual risk cannot be defined, qualitative tracking of these trends can alert the institution about potentially increased exposure. With AML compliance, for example, some exposures can be measured through quantitative key risk indicators, while others will require qualitative risk markers (Exhibit 3).

5. Actively manage controls and management-information systems.

The portfolio of controls needs to be actively managed over the life cycle of each control. Old

Exhibit 3

The effectiveness of anti-money-laundering controls can be measured by quantitative key risk indicators or qualitative risk markers.

□ KRI example □ Risk marker

Requirements	Key risk indicators (KRIs) or risk markers	Residual risk	Test questions
Customer risk assessment	New customers not risk-rated appropriately or in a timely manner	Medium	Customer due-diligence requirements obtained and risk appropriately rated? If high risk, was customer added to high-risk log?
	High-risk customers not reviewed appropriately or in timely manner		
Report filing	Customer-transaction reports (CTRs)	High	Was assessment of money-laundering risk completed in time?
	Monetary-instrument logs		
	Suspicious-activity reports (SARs)		
Customer identification program (CIP)	New customers not provided with CIP notice at or before account opening	Low	
	New accounts with inadequate verification of identity		
	Existing customers without timely, complete, or correct due-diligence review		
Employee incentives	Reporting forms (SARs, CTRs, CTR exemptions) completed by the same employee who made the decision to file the reports or grant the exemptions	Medium	Risk marker indicates misaligned incentives due to lack of segregation of duties
	Volume of CTRs in relation to volume of exemptions (did additional exemptions significantly reduce CTR filings?)		
	Growth in higher-risk operations ¹ without proportional increase in CTRs and SARs		

¹ Higher-risk-customer examples: foreign financial institutions, deposit brokers, cash-intensive businesses, nongovernment organizations. Higher-risk-product examples: ATMs, private banking, foreign-correspondent accounts, trade finance, foreign exchange.
Source: FDIC, BSA/AML Office of Foreign Assets Control regulation; Federal Financial Institutions Examination Council, *BSA/AML Examination Manual*

controls, testing strategies, and management-information systems (MIS) should be discontinued quickly when no longer needed or when deemed ineffective. Clearing away unneeded controls saves compliance and business resources and

helps ensure that material risks are not missed. Many controls are redundant or obsolete—such as reports for a particular issue that no longer exists. Others have been added to old processes where underlying problems have not been remediated.

The result is layers of detective controls but few preventative controls. For many activities, controls are overabundant and it is unclear which are the key controls that truly make a difference. A bank can have hundreds of mostly weak controls in its trading chains without understanding that 20 are the most important (and should be perfected and tightly monitored to mitigate risk). Finally, controls are often ineffective because they are insufficiently understood and consequently undermanaged (for example, supervisors may not understand their roles and control responsibilities).

Markets businesses are a particularly challenging area for managing controls. These involve many frontline and middle- and back-office units, as well as risk and finance. We have encountered situations where more than 500 controls are in place, from supervisory controls in the front office to extensive reconciliation and reporting controls. A source of the challenge is the separation between units where risks emerge and those in charge of the controls. For example, frontline conduct risk may arise from ill-defined trader mandates or trade and booking data structures, while control responsibility rests with middle- and back-office units. These units, like compliance or control and settlement, might react by adding layers of control without identifying and addressing root causes upstream.

By rationalizing the control portfolio, most banks will be able to reduce monitoring and testing activities significantly. The remaining controls should then be automated, where this is possible (such as system checks or work flow). In-line quality controls, such as document-quality tollgates, can replace manual checkers for controls that cannot be fully automated.

For example, according to a legacy requirement of a consumer business unit at one bank, post-underwriting quality control of all new loan applications was performed by both an internal

quality-control team and external attorneys. This triple-checking was replaced by quality tollgates much earlier in the process and automated data pulls that prevented errors. That eliminated most of the rework and expensive back-and-forth communications by attorneys, production, and the quality-control team.

6. Optimize testing and monitoring activities.

Duplication and overlap should also be eliminated from testing and risk-assessment programs, including BSA/AML, operational risk, IT risk, and first-line-of-defense activities. Furthermore, monitoring and testing standards need to be aligned with compliance standards in the first line of defense. These should be clearly tied to the inventory of material risks, associated key risk indicators, risk markers, and MIS. These measures will provide a clear line of sight to the risks the organization should focus on, what is being measured, and how the information will be used to make management decisions and prioritize resources.

Having eliminated overlap, banks can streamline the remaining testing and monitoring activities. For rules-based compliance, subjective assessments can be replaced with objective measures of residual risk—actual defect rates for critical regulations. Meanwhile, manual testing methods should, where possible, be replaced with system-driven exception reporting, such as timeliness and accuracy of customer disclosures based on time stamps and figures in the system of record. Advanced analytics can be deployed to analyze financial, operational, and control performance and identify patterns and hot spots. This level of automation of manual tasks can provide an early warning of failing controls, obviating headaches down the road. For monitoring and testing activities requiring manual intervention, a testing utility can be created to standardize tests and improve load balancing. This will help ensure that capacity is utilized efficiently and according to target quality standards.

7. Effectively manage supervisory and audit issues.

At many banks, remediation of supervisory and audit issues accounts for a large part of the compliance budget and the related change-the-bank budget. In most cases, banks handle supervisory and audit issues individually. Each major finding results in a separate project, and little thought is given to related control issues and root causes. In our experience, the attendant costs of this approach can be significantly reduced by moving to a more integrated portfolio-management approach.

Projects need to be managed on two dimensions: the underlying issues and the affected business areas. Supervisory issues related to client onboarding in the commercial-banking business unit, for example, need to be consolidated to avoid duplicating enhancements of core business processes. Effective KYC management for global banks in fact requires a centralized, cross-division view of customers and their business activities. Without this view, suspect activities could escape detection, or inconsistent client onboarding approaches and decisions may result. To address related BSA/AML issues, furthermore, banks will likely require a comprehensive and integrated approach to control design, to avoid uncoordinated technology efforts.

Supervisors rightly value an adequate focus on the root causes of issues. Banks that have this focus are able to design changes to core business processes that stop issues from arising in the first place. When issues are addressed individually, the solution is often to put in place additional layers of manual controls. Root-cause analysis helps an institution become more resilient in its business environment while reducing reliance on costly manual controls.

Where manual controls are still required to plug an existing gap, banks need to develop plans to automate them and/or redesign the underlying business process. Appropriate cost-benefit

analysis should accompany such plans and help prioritize automation projects across the portfolio of remediation activities. Many banks would also benefit from comprehensive management reporting to measure the cost and effectiveness of remediation activities and make the best possible use of subject-matter experts and technology budgets to “buy down” the risks.

Effective remediation governance—with clear responsibilities and effective implementation monitoring—can also reduce complexity and lower costs. This means clearly delineating responsibilities for all remediation activities among the compliance function, business lines, and other control functions.



The cost of regulatory compliance in financial services has spiked over the past decade. In particular, resources in the first and second lines of defense have expanded dramatically. As a result, the industry has become more resilient and the quality of risk management has improved. The current resource-intensive approach to managing compliance is not, however, sustainable in the long run. While the demand for compliance activities is largely out of banks’ control, these seven practical steps can optimize how banks respond to that demand and allow meaningful progress toward a sustainable compliance function over time. ■

Piotr Kaminski is a senior partner in McKinsey’s New York office, **Daniel Mikkelsen** is a senior partner in the London office, **Thomas Poppensieker** is a senior partner in the Munich office, and **Kate Robu** is a partner in the Chicago office.

Copyright © 2017 McKinsey & Company.
All rights reserved.



© Mint Images/Getty Images

Nonfinancial risk today: Getting risk and the business aligned

Both must be deeply involved to avoid costly errors.

Joseba Eceiza, Piotr Kaminski, and Thomas Poppensieker

Ask senior managers at any company if they have nonfinancial risk under control, and the answer is likely to be yes. But as managers of companies in automotive, banking, oil and gas, pharmaceuticals, and many other sectors can attest, the reality is often very different. And as personal liability for corporate actions takes hold, board members—both executive and nonexecutive—are on the hook not just for their personal involvement in risk- and compliance-related issues but also more broadly for the company’s whole risk profile and enterprise-wide compliance.

Nonfinancial risk¹ has typically been addressed by one-off showcase initiatives based on a specific regulation or requirement, and left to experts in each field. What principles exist typically focus on adhering to formal standards and providing

evidence that appropriate controls are in place. They are usually not embedded in the business but are instead delegated to risk and compliance departments, which have a limited understanding of how to manage risk and compliance within the business context.

In other cases, the business takes all the responsibility for managing risk, but without any link to the company’s formal compliance, risk, and control framework. Quality control, for example, is embedded in the day-to-day management of manufacturing organizations, but those responsible are not involved in determining enterprise risk, leaving a major gap.

Both shortfalls have led companies from all sectors to be caught off guard when failures occur. And those failures have led to catastrophic incidents

and destroyed shareholder value time and again. Over the past 15 years, companies around the world have ended up in dire predicaments through such control failures. In all these cases, the formal risk-management approach has been criticized for being insufficient. In concrete terms, litigation and settlement of nonfinancial risk-control failures have cost the financial-services and corporate sectors several hundred billion dollars over the past ten years—and that does not include the additional impact of reputational damage.

The impact on management has been just as significant, including damaged reputations and personal prosecution, not only where senior management has been directly linked to wrongdoing but also where it was found not to have established a robust approach to risk and control management.² As this article will explain, there is a better way—one that needs to be adopted before a major incident occurs, and not after.

Risk matters, but not in isolation

Leading companies have established frameworks for risk and control management (R&CM) that help management balance the risk-management imperatives and the needs of the business—in other words, an approach to risk that accurately reflects the business context, while ensuring that risk and compliance management is embedded across the entire organization. This means going beyond implementing yet another checklist or improving the links between business units. It requires an explicit management dialogue about nonfinancial risk—about where it can occur and how it is being mitigated—and extends to questioning where the cost of control may be too high, given the value at stake. For many companies, this implies a full cultural transformation, so that a new set of risk-management processes can be as effective as possible. Until that changes, the same mistakes will be repeated year after year, and companies will be at risk as the threat to their value is overlooked.

Key objectives of a well-founded framework

Risk managers may argue that the basic principles of R&CM are well established, and indeed enshrined, in industry standards. The concepts may be broadly known, but they are applied in such a scattered fashion that they are not fit for purpose. A board that wants to get on top of nonfinancial risk management needs to have three clear objectives:

- It must facilitate better decision making. A robust R&CM framework should help management better understand the company's risk profile so that it can make informed decisions, such as where to accept risk and where to mitigate it in the context of overall risk appetite and risk strategy. The framework needs to help businesses prioritize the risks and controls to address, based on their likelihood and potential impact on the business. It should form the basis for continuous risk management through a business view on value chains, processes, and embedded risks and controls.
- It must provide evidence for internal and external stakeholders of the adequacy of the controls that are in place (or that should be implemented), and it should clarify who is responsible for what regarding risk ownership and control execution. This gives senior management a way to assess the effectiveness of the organization, delegate responsibilities, and address legal implications.
- It must reinforce an adequate risk and compliance culture that should be as deeply embedded into a company's management approach as revenue and cost management.

The resourcing and costs of the R&CM approach should be aligned with the company's structure, business model, and risk profile. For example, an oil and gas company might choose to focus on regulatory and counterparty risks in markets where it operates, while financial firms might target

product mis-selling. The approach should also provide guidance on the efficiency of the control environment as much as its effectiveness, by showing, for instance, the gap between the inherent risk and the residual risk after the control is implemented.

The business case for R&CM

Assessing, managing, and mitigating risk must be justifiable on business grounds. Running an effective and efficient R&CM, in our experience, can deliver a payoff of more than ten times the investment. There is no doubt that implementing R&CM is beneficial for companies across all industries. It can help reduce losses and the cost of control, which together should more than offset the up-front investment needed to set up the methodology and the recurring costs of maintaining it. And regulators approve, too.

Cut your losses

Organizations typically experience five types of losses from nonfinancial risk: recurring low-severity losses (such as credit-card fraud); one-off, high-severity losses (for instance, senior-management wrongdoing); regulatory fines; the imposition of greater capital requirements for banks; and reputational damage (where examples are legion).

A sound R&CM framework helps to reduce these losses by ensuring the right controls are in place. For example, a company might develop a coordinated plan with its telecom providers to prevent and counter distributed denial-of-service attacks, or take out insurance against cyberattacks. Preventing or reducing the impact of risk also reduces remediation costs—such as the cost of reviewing thousands of files or of setting up call centers to handle customer complaints. R&CM also helps reduce regulatory fines and can help smooth the conversation with supervisors.

Spend less on mitigation

At the heart of a strong R&CM framework is the prioritizing of risks and controls. This means that

resources are focused where they will have the greatest impact and that duplicative controls are removed. In automotive, for instance, quality control is vital in production processes, but not all processes are equally important; therefore, it is important to invest in controls where both the likelihood of a risk event and the resulting impact are highest.

Aside from cherry-picking the most critical controls, an R&CM framework that has a unified and aggregated risk-assessment system immediately makes the control function more efficient and cost effective. This is essential when 5 percent of the workforce can be employed in control-related activities.

Identifying key risks also helps ensure the right insurance policies are in place. In addition, those policies should be more efficient and cheaper, because risk identification is more targeted and because it becomes clear how specific controls help mitigate risk.

Keep setup costs low

Setting up an R&CM framework is typically a multiyear effort, but strong management focus will ensure maximum effectiveness and efficiency. Furthermore, consolidating different control frameworks can deliver significant synergies from aligned management processes, system consolidation, and integrated reporting. Most important, setting up a robust R&CM framework permits a sharper focus on identifying and mitigating risk, through an objective fact base and clearer policy standards. If set up properly, it also provides all the evidence required for the formal reporting to the risk or audit committees under COSO, ICS, ERM, or CMS standards.³

The regulatory benefits

A strong R&CM approach not only makes good business sense—it's also becoming more of a legal requirement. Several international regulators are pushing for clearer definitions of, and better

connections among, the “first line of defense” (the business), the second line (the risk and compliance functions), and the third line (internal audit). This three-lines-of-defense model is increasingly used as a way of explaining the relationship among these functions and as a guide to how responsibilities should be divided.

How to get it right

The key components of a best-practice R&CM approach revolve around unified taxonomies, assessment tools, data and reporting tools—and ultimately the process that ensures the framework becomes part of the whole company’s day-to-day life.

Get everyone talking the same language

Very few companies have a truly unified way of talking about risk or controls. Comparable risks may never be recognized as such, simply because they are described differently by different parts of the business. This can be as simple as, for example, identifying employee behavior and employee conduct as identical, when, in fact, the two are never linked—and thus the total risk level is misreported.

Clear risk definitions need to be shared across the company in order to identify which risks to actively manage and monitor.

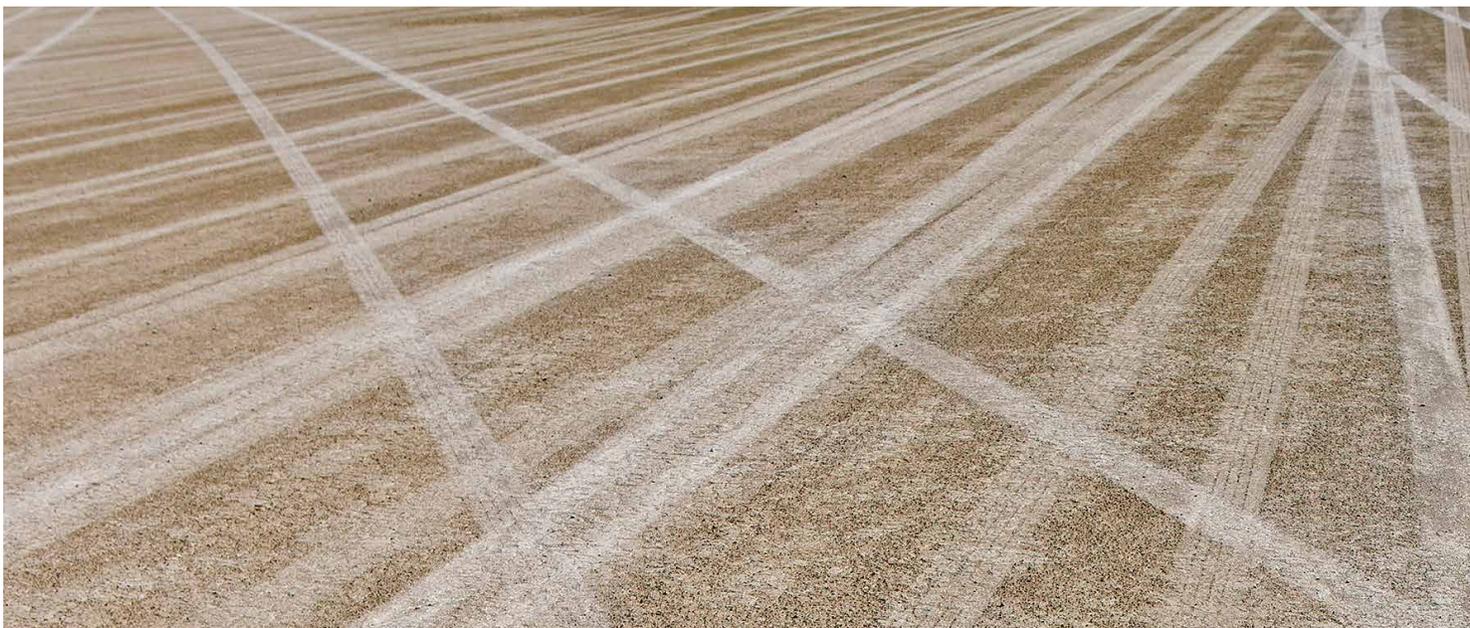
Exactly the same problem applies to controls. For example, identity control and access-management control might mean the same thing in the same company, but if that is not recognized, then their relevance could be underestimated.

The challenge is to ensure that the taxonomy is at the right level of granularity to help identify risk, but not so granular that it becomes unwieldy.

Map the risk

Once everyone is using the same language, the company can then identify where material risk for the organization exists.

A groupwide process map that represents the company’s business model is a good starting point. Companies often struggle to find the right level of granularity in process maps: too high a level (for example, eight or nine processes for the entire



institution), and the maps are of limited value; too granular (for instance, more than 100,000 processes at one European bank), and the effort required to create and maintain them is too burdensome. Mapping at the value-chain level is typically a good way to begin, and then, over time, the exercise can become more granular.

At an automotive manufacturer, for example, the first step was to identify and define specific compliance requirements by country (such as emissions, certification, and safety) and to understand their importance for car models across their life cycle. These were then mapped into the company's processes (from R&D to manufacturing), taking into account the complex structure of the supply chain, which involved dozens of nodes and locations.

Using the map and the risk taxonomy, therefore, a business can profile the risk in each process and assess both the probability and severity. This information is aggregated from the R&CM unit level to the enterprise level.

Understand the controls

Knowing which risks exist is only half the equation. The other half is knowing how to mitigate them. Organizations struggle to tie controls to risks for many reasons, which range from unclear definitions of controls to a limited understanding of how effective the controls actually are. This means that the business reviews hundreds of controls. But without a clear view on which are the most relevant and effective, no clear management perspective on the overall control strategy will be developed. To take an extreme example, in a nuclear-power plant, controls that monitor the performance of the core should have a much higher priority than controls that focus on avoiding outages on steam turbines through preventative maintenance. Both matter, but not to the same extent.

If an organization assembles only a list of controls, with no hierarchy, then that list is useless for

management decision making within the business—and instead only serves as a way for compliance or risk functions to document the weaknesses that it identifies.

Leading players, therefore, undertake a fact-based control assessment: they find out which controls are used to mitigate which specific risks, determine how effective and efficient they are, and link them to the policies and operating procedures that clarify control standards, accountabilities, and training and communication that ensures the organization is fully aware of the risks. The assessment should draw on multiple sources of data, such as internal and external loss and incident data, audit-review results, supervisory findings, key risk indicators, and key control indicators.

Report back—and act

To make sense of the assessments, management must have a consistent view of nonfinancial risks and the underlying controls, with systematic reporting to the board. This requires an integrated management-information system. Typically, these are bespoke versions of externally available packages that broadly match the company's specific R&CM requirements, or internally developed platforms. When selecting commercial packages, companies must be careful not to tailor them to a point where system upgrades become difficult to manage.

Where identified risks fall outside the company's risk appetite, concise and action-oriented risk and control reporting recommends where, how, and when the risk is mitigated. The actions might range from redesigning the entire control environment to reinforcing supervisory responsibilities, or even removing the product or process that is creating the risk. Ultimately, the reporting, based on the risk and control assessments, should enable the company to prioritize controls, based on specific context. Of course, any change to a control must happen within the organization's existing control framework in order to retain clear accountability.

Run the process company-wide ... and keep running it

As we saw at the start, the R&CM framework must be applied across the entire company, otherwise individual units, functions, or people can inadvertently create enormous risk. The process also needs to be aligned with both the company's management and accountability structure and its fundamental business processes and value chains. This way it can identify individual risk by area as well as control dependencies across the value chains (which extends to outsourcing arrangements via third parties).

Business units are prone to receiving overlapping requests to assess the risk of particular processes and assets from different risk-management groups (for example, cyber risk, or operational risk). By coordinating and sharing information, the operational impact of participating in the R&CM processes is reduced, which leads to higher-quality risk information. Nevertheless, organizations can end up running hundreds of workshops each year as they attempt to identify risk and controls, and therefore clearly defined process and expectations for business units and control functions are crucial. Careful planning of R&CM entities and identifying those with similar profiles (such as all sales or production units) becomes paramount.

An annual risk-assessment exercise will never be sufficient; what's needed are both "trigger-based assessments" when incidents occur, when certain indicators breach thresholds or processes change, and ongoing monitoring. The model needs to be particularly strong given the interaction between the business-division risk owners who identify and assess the risks (the first line of defense) and the control functions that challenge the results (the second line of defense).



As senior management's personal liability for corporate risk increases, the traditional way of tackling nonfinancial risk management could leave many facing uncomfortable times in front of their boards, their regulators, and quite possibly their courts. A new framework for risk and control management is needed—one that is cost effective and explicitly ties risk to business value, and one that helps management have a fruitful conversation with stakeholders.

The risk and control management approach outlined here achieves this. By bringing the business into the risk-management discussion, corporate risk changes from a topic that someone else worries about to being a keystone of every employee's role in the organization. ■

¹ For the purposes of this article, nonfinancial risk is broadly defined as all risk that is not balance sheet related (for example, excluding credit, foreign-exchange, commodity-price, and liquidity risk). Nonfinancial risk comprises compliance risk (for instance, the requirement to adhere to all relevant rules and regulations) and operational risk (such as process, production, technology, and cyber risk).

² This is reflected by the "business judgement" rule, which requires company management to establish processes regarding risk and compliance that are in line with industry practices for a business model of this complexity.

³ COSO: Committee of Sponsoring Organizations of the Treadway Commission; ICS: frameworks for the internal control system; ERM: enterprise risk management; CMS: compliance-management system.

Joseba Eceiza is a partner in McKinsey's Madrid office, **Piotr Kaminski** is a senior partner in the New York office, and **Thomas Poppensieker** is a senior partner in the Munich office.

Copyright © 2017 McKinsey & Company.
All rights reserved.



© Hoxton/Tom Merton/Getty Images

Protecting your critical digital assets: Not all systems and data are created equal

Top management must lead an enterprise-wide effort to find and protect critically important data, software, and systems as part of an integrated strategy to achieve digital resilience.

Piotr Kaminski, Chris Rezek, Wolf Richter, and Marc Sorel

The idea that some assets are extraordinary—of critical importance to a company—must be at the heart of an effective strategy to protect against cyber threats. Because in an increasingly digitized world, protecting everything equally is not an option. The digital business model is, however, entirely dependent on trust. If the customer interface is not secure, the risk can become existential. System breaches great and small have more than doubled in the past five years, and the attacks have grown in sophistication and complexity. Most large enterprises now recognize the severity of the issue but still treat it as a technical and control problem—even while acknowledging that their defenses will not likely keep pace with future attacks. These defenses, furthermore, are often designed to protect

the perimeter of business operations and are applied disjointedly across different parts of the organization.

Our research and experience suggest that the next wave of innovation—customer applications, business processes, technology structures, and cybersecurity defenses—must be based on a business and technical approach that prioritizes the protection of critical information assets. We call the approach “digital resilience,” a cross-functional strategy that identifies and assesses all vulnerabilities, defines goals on an enterprise-wide basis, and works out how best to deliver them. A primary dimension of digital resilience is the identification and protection of the organization’s digital crown jewels—the data, systems, and software applications that are essential to operations.

Burgeoning vulnerabilities, finite resources, fragmented priorities

In determining the priority assets to protect, organizations will confront external and internal challenges. Businesses, IT groups, and risk functions often have conflicting agendas and unclear working relationships. As a result, many organizations attempt to apply the same cyber-risk controls everywhere and equally, often wasting time and money but in some places not spending enough. Others apply sectional protections that leave some vital information assets vulnerable while focusing too closely on less critical ones. Cybersecurity budgets, meanwhile, compete for limited funds with technology investments intended to make the organization more competitive. The new tech investments, furthermore, can bring additional vulnerabilities.

The work to prioritize assets and risks, evaluate controls, and develop remediation plans can be a tedious, labor-intensive affair. Specialists must review thousands of risks and controls and then make ratings based on individual judgment. Some organizations mistakenly approach this work as a compliance exercise rather than a crucial business process. Without prioritization, however, the organization will struggle to deploy resources effectively to reduce information-security risk. Dangers, meanwhile, will mount, and boards of directors will be unable to evaluate the security of the enterprise or whether the additional investment is paying off.

All data and systems are not created equal

In any given enterprise, some of the data, systems, and applications are more critical than others. Some are more exposed to risk, and some are more likely to be targeted. Critical assets and sensitivity levels also vary widely across sectors. For hospital systems, for example, the most sensitive asset is typically patient information; other data such as how the emergency room is functioning may even be publically available. Risks to priority data include breach, theft, and even ransom—recall that a Los Angeles hospital paid a \$17,000 Bitcoin ransom to a hacker that had

seized control of its systems. An aerospace-systems manufacturer, on the other hand, needs to protect intellectual property first and foremost, from systems designs to process methodologies. A financial-services company requires few controls for its marketing materials but is vulnerable to fraudulent transactions; its M&A database, furthermore, will need the best protection money can buy. Attackers can be individuals or organizations, such as criminal syndicates or governments with significant resources at their command. The attacks can be simple or sophisticated, the objectives varying from immediate financial reward to competitive or even geopolitical advantage.

Cybersecurity spending: When more is less

In the face of such diverse threats, companies often decide to spend more on cybersecurity, but they are not sure how they should go about it.

- A global financial-services company left cybersecurity investments mainly to the discretion of the chief information-security officer (CISO), within certain budget constraints. The security team was isolated from business leaders, and resulting controls were not focused on the information that the business felt was most important to protect.
- A healthcare provider made patient data its *only* priority. Other areas were neglected, such as confidential financial data relevant to big-dollar negotiations and protections against other risks such as alterations to internal data.
- A global mining concern focused on protecting its production and exploration data but failed to separate proprietary information from information that could be reconstructed from public sources. Thus, broadly available information was being protected using resources that could have been shifted to high-value data like internal communications on business negotiations.

These examples illustrate the need for a unified, enterprise-wide approach to cyber risk, involving the business and the risk, IT, and cybersecurity groups. The leaders of these groups must begin to work together, identifying and protecting the organization's critical digital assets as a priority. The process of addressing cyber risk will also have to become technologically enabled, through the implementation of work-flow-management systems. Cybersecurity investment must be a key part of the business budget cycle, and investment decisions must be more evidence based and sensitive to changes.

The business-back, enterprise-wide approach

The key point is to start with the business problem, which requires a consideration of the whole enterprise, and then to prioritize critical risks. This work should be conducted by an enterprise-wide team composed of key individuals from the business, including those in product development, and the cybersecurity, IT, and risk functions. The team's main tasks are to determine which information assets are priorities for protection, how likely it is that they will be attacked, and how to protect them. To function, the team must successfully engage the leaders of several domains. They need to work together to discover what is most important—no mean challenge in itself. The best way to get started is to found the team on the agreement that cyber risks will be determined and prioritized on an enterprise-wide “business back” basis. In other words, the team will first of all serve the enterprise. Critical risks, including the impact of various threats and the likelihood of occurrence, will be evaluated according to the dangers they pose to the business as a whole.

Guiding principles

The following principles can help keep companies on track as they take the unified approach to prioritizing digital assets and risk:

- ***Start with the business and its value chain.*** The effort should be grounded in a view of

the business and its value chain. The CISO's team, particularly when it is part of the IT organization, tends to begin with a list of applications, systems, and databases, and then develop a view of risks. There are two major flaws to this approach. First, it often misses key risks because these can emerge as systems work in combination. Second, the context is too technical to engage the business in decision making on changes and investments. By beginning with the business, the team encourages stakeholder engagement naturally, increasing the likelihood that systemic exposures will be identified.

- ***The CISO must actively lead.*** In addition to being a facilitator for the business's point of view, the CISO should bring his or her own view of the company's most important assets and risks. By actively engaging the business leaders and other stakeholders as full thought partners, the CISO will help establish the important relationships for fully informed decision making on investments and resource allocation. The role of the CISO may thus change dramatically, and the role description and skill profile should be adjusted accordingly.
- ***Focus on how an information asset can be compromised.*** If an information asset is exposed by a system being breached, the vulnerability of this system should be considered, even if the system's primary purpose does not relate to this information asset.
- ***Focus on prioritization, not perfect quantification.*** The team needs only enough information to make decisions on priority assets. It does not need highly precise risk quantifications—these would be difficult to produce and would not make a difference in deciding between investment options.

- *Go deeper where needed.* The same level of analysis is not needed to quantify all risks. Only for particularly high-impact or complex risks should the team invest in deeper analyses. It should then decide on and acquire the information needed to make more informed investment decisions.
- *Take the attacker's view.* Risk reviews and vulnerability analyses must not focus solely on the value of the information to the company and the ascertainable gaps in its defenses. The profiles of potential attackers are also important: Who wants the organization's information? What skills do they possess? Thinking about likely attackers can help identify new gaps and direct investment to protect the information that is most valuable to the most capable foes.

A flexible systematic process with a designed platform

The object of the enterprise-wide approach is to identify and remediate gaps in existing control and security systems affecting critical assets. The solution, in our experience, will be an end-to-end process, likely requiring multiple development iterations, including a detailed account of hundreds of assets. A work-flow system and asset database would be an ideal tool for supporting this complex process, allowing focus on prioritizing risks. A flexible, scalable, and secure online application can be easy to use while managing all the inventory and mapping data, the rigorous risk and control evaluations, sector-specific methodologies, and rationales for each risk level. The platform can also support detailed data to be used when needed as the team undertakes analysis of the priority assets and gaps and makes the recommendations that will shape remediation initiatives.

In developing this approach, consider the following five key steps:

1. *Identify and map digital assets*, including data, systems, and applications, across the business value chain. This can be accelerated by applying a generalized-sector value chain and a common taxonomy for information assets and then customizing these to the organization.
2. *Assess risks for each asset*, using surveys and executive workshops. By basing this analysis on the business importance of the asset, the organization will have identified its crown jewels.
3. *Identify potential attackers*, the availability of assets to users, and current controls and security measures protecting the systems through which access can be gained to the assets, using similar surveys and workshops as in step two.
4. *Locate where security is weakest* around crown-jewel assets and identify the controls that should be in place to protect them, by comparing the results of these assessments using dashboards.
5. *Create a set of initiatives* to address the high-priority risks and control gaps. Implementation will involve a multiyear plan, including timelines for follow-up reviews. Once the initial assessment is complete, this plan becomes a living document, regularly refreshed to reflect new data, systems, applications, risks, and mapping, as well as progress to remediate known vulnerabilities (see sidebar, "An institution's progress").

The process promotes cyber-risk transparency, answering key stakeholder questions: What are our inherent information risks? Where is our organization vulnerable? How big (and where) is the residual exposure? What remediation actions should we prioritize? How do we know if what we did is working? Information-risk trade-offs can be defined based on a perspective on value at risk across the company. This helps the C-suite and board discuss information-security risk using measures such as

An institution's progress

One financial institution that used the approach described in this article was able to identify and remediate gaps in its control and security systems affecting critical assets. The change program began with a risk assessment that highlighted several issues. Business and IT priorities on cybersecurity spending were found to be somewhat out of alignment, while communication on risks and risk appetite between risk management and businesses was less than optimal. The lack of agreement among stakeholder groups consequently stalled progress on a mitigation plan for cyber risk.

In response, the company established a unified group that developed a work plan to protect critical data. The team inventoried all systems and applications in all business units, validating the results with key stakeholders to ensure completeness. They then identified critical data and performed a risk assessment with input from the stakeholders. The

team was now able to identify the critical information assets based on potential risk impact. The level of control in each system was also evaluated, as the team mapped information assets to the systems and applications where they reside and isolated gaps between current and needed controls.

The critical data assets requiring additional protection were identified globally and by business unit. The systems and applications holding critical data that needed remediation could then be addressed. The team developed a series of detailed scenarios to reveal system vulnerabilities and help stakeholders understand what could happen in a breach. A comprehensive set of prioritized initiatives and a multiyear implementation plan was then created. The data resulting from this process are continually updated and provide guidance in budgeting decisions and board reviews on an ongoing basis.

enterprise value, providing transparency on what risks they are willing to accept and why.

Results inform budget and investment decisions, helping to satisfy both regulatory and shareholder expectations. With investments targeted to best protect the most sensitive digital assets, costs are held down as the digital resilience of the organization is elevated. To build digital resilience into their operations, furthermore, the process can help organizations create periodic assessments to highlight trends and new gaps. Risk managers can then develop new initiatives prioritized to the enterprise's global needs.



Organizations in sectors with higher digital maturity will benefit the most from this approach, including financial services, manufacturing, and healthcare.

They face the tough task of fully protecting their most important assets while not stifling business innovation. To achieve this balance, the business, IT, risk, and other functions will have to work together toward the same enterprise-wide end—to secure the crown jewels so that senior leaders can confidently focus on innovation and growth. ■

Piotr Kaminski is a senior partner in McKinsey's New York office, **Chris Rezek** is a senior expert in the Boston office, **Wolf Richter** is a partner in the Berlin office, and **Marc Sorel** is a consultant in the Washington, DC, office.

The authors wish to thank Oliver Bevan and Rich Cracknell for their contributions to this article.

Copyright © 2017 McKinsey & Company.
All rights reserved.



© Danita Delimont/Getty Images

From scenario planning to stress testing: The next step for energy companies

Utilities and oil and gas firms have long used scenario analysis, but extraordinary times call for new measures.

Sven Heiligtag, Susanne Maurenbrecher, and Niklas Niemann

Strategic and financial scenario analysis has a long, venerable history at energy companies. Shell Oil popularized the technique in the 1970s, and almost all of them have adopted it as a vital part of their decision-making processes. But as executives know well, scenario planning has its pitfalls; 40 percent of the leaders we surveyed in 2013 said that it didn't meet their expectations. Often, companies fall prey to one of several tendencies, such as availability or stability bias, that hinder the exercise and produce unusable results.

Energy companies are finding that in today's volatile world, one flaw of scenario planning is particularly acute: when business leaders consider a range of scenarios, they tend to "chop the tails off the distribution" and zero in on those that

most resemble their current experience. Extreme scenarios are deemed a waste of time because "they won't happen" or, if they do, "all bets are off." But this approach leaves companies dangerously exposed to dramatic changes.

Consider the shocks and disruptions of recent years. The 2010 Deepwater Horizon disaster had far-reaching effects on the oil companies involved, and many others. The 2011 Fukushima earthquake and tsunami upended nuclear policy in Japan and elsewhere, changing the industry's structure. Geopolitical shocks have upset the plans of energy companies in too many countries to name. Most recently, the rise of antiglobalization sentiment has thrown a new wrench into energy planning.

It's hard to overstate the consequences of events like these. Take the German experience of *Energiewende*, the nation's transition to sustainable energy. To predict the effects on electricity prices, most energy companies relied on the classic scenarios—a base case, with best and worst cases that skewed slightly to either side. However, the Fukushima disaster vastly accelerated the switch to renewables. The price of power tanked by more than 50 percent—far worse than the gloomiest projections (Exhibit 1). The effect has been devastating: power producers had to write off tens of billions of euros.

Enter stress testing

At most companies, scenario analysis looks for the likely development of core risk factors over time. That approach can work well in an era of gradual change. But at times like the present, it is extreme risks, not the everyday ones, that should most concern energy companies. Likewise, it is the prospect of chaotic overnight change, not gradual shifts, that should keep energy executives awake at night.

Enter stress testing, a form of scenario planning focused on the tails of the distribution. Scenario planning and stress testing are methodologically identical; they differ only in the likelihood of the scenarios they consider. Stress testing therefore requires a shift in mind-sets. In today's environment, the sum of low-probability events quickly adds up to a high probability that one of them will actually happen. The banking industry offers an example: the financial system has become so volatile, and subject to so many unexpected disruptions, that regulators now require banks to conduct comprehensive stress tests.

Let's be clear: stress testing will not prevent stress. Nor can it identify, with total confidence, precisely which stressful scenarios might play out in the future—especially those that feature “unknown unknowns.” But it can help senior executives to

consider some previously overlooked sources of stress, the potential magnitude of their impact, and the adequacy of the company's risk-bearing capacity to absorb them. Stress testing should be only one element of a risk-management system, but done well, it can be a tool to build the resilience that today's environment requires.

What 'extreme' means

Companies need to be bold as they imagine extreme scenarios; almost nothing is too strange or ridiculous to consider. To show the range of ideas that energy firms might contemplate, we offer five extreme scenarios covering several kinds of risk, from compliance and legal risk to business-model disruption to full-bore crisis.

Energy for free

Real-time energy-consumption data are increasingly seen as crucial for a knowledge of customers and their behavior patterns. Smart meters can identify the appliances in operation. Combining data sets on electricity use, heating use, and mobility could provide even more detailed insights. Data-driven companies such as Amazon might challenge incumbent utilities by offering “energy for free” in exchange for personal data. In this scenario, utilities lose the customer relationship and are reduced to mere suppliers of commoditized power. Given the negotiating power, agility, and customer-centricity of digital giants, margins erode significantly.

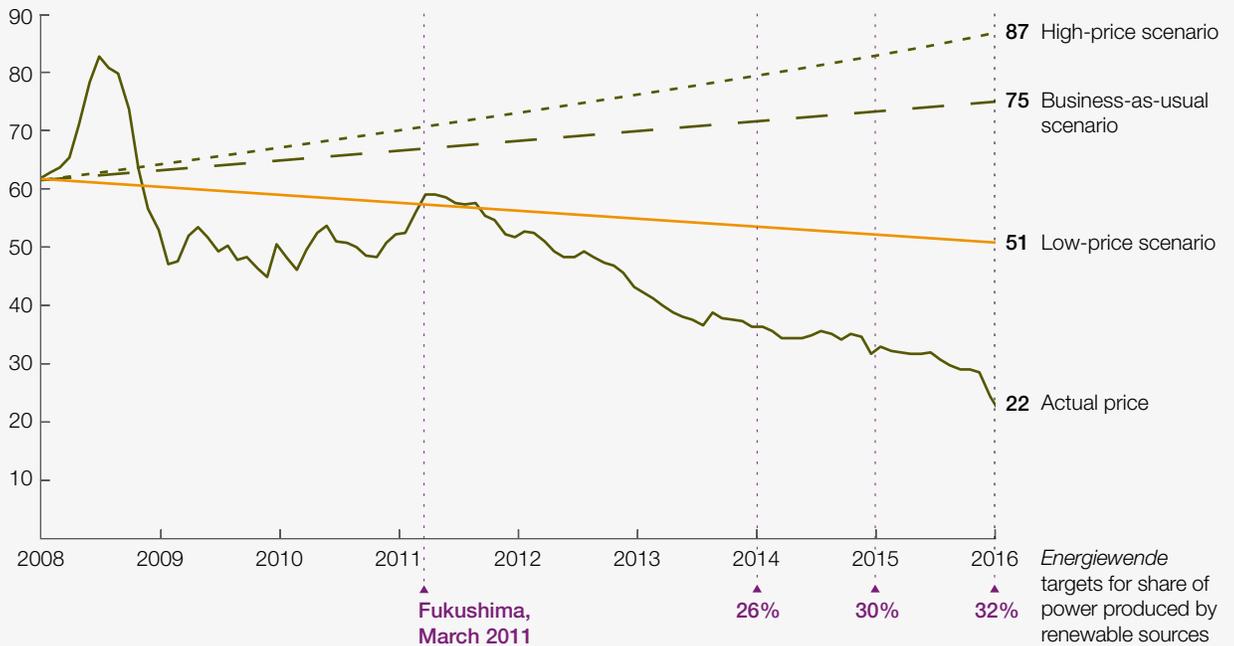
A decentralized energy landscape

New entrants focus on serving customers in a completely decentralized energy regime, bundling solar photovoltaic rooftop systems with power-to-heat technologies, powerful batteries, and electric cars. An integrated solution and a strong, emotionally compelling brand (such as Tesla's) help these attackers to reduce residual demand for grid-based power substantially and to capture the customer relationship. As in the first scenario,

Exhibit 1

German power prices far underperformed even the low-price scenario.

German wholesale power prices, 2008–15,
€/MWh



Source: BBC; European Energy Exchange; Umweltbundesamt; McKinsey analysis

utilities are reduced to suppliers of commodity power, infrastructure operators, and backup providers. Volumes and margins shrink quickly in the wholesale and retail businesses, and generation assets lose value rapidly.

An emissions fraud

A data leak reveals that a power company has manipulated processes affecting human health—say, flue-gas purification at a coal plant or the handling and disposal of waste—and has thus emitted substantially more pollution than allowed. Subsequent investigation shows that the manipulation was deeply anchored within the

organization: top leaders knew that analyses and impact assessments had intentionally been skewed. As a result, all energy companies suffer a loss of public and political trust. They are then subjected to intense scrutiny of their assets and processes, and this leads to increased regulation, massive penalties, and personal liability in the form of substantial fines and imprisonment.

A cyberattack on critical infrastructure

Popular movies have frequently exploited the idea that the infrastructure of modern life is vulnerable to well-staged cyberattacks. But the real-world Stuxnet virus succeeded better than anything out

of Hollywood in proving that power plants and other nuclear assets can indeed be sabotaged. A cyberattack that takes critical infrastructure offline is more probable than ever now that power and gas grids, street lighting, and traffic control are more and more connected; the Internet of Things is beginning to reach into every home and building; and autonomous, connected vehicles are set to emerge over the next few years. In such a scenario, terrorists hack into the distribution network and shut down national power systems or even make key assets malfunction or self-destruct. Public trust would disappear, and energy companies would be subject to enormous pressure from regulators. Those deemed vulnerable to further attacks might even lose their operating licenses.

Radical price transparency

Price-comparison websites, such as Verivox in Germany, have established a strong position in several European countries. They greatly increase price transparency in retail markets for power, gas, mobile telecommunications, banking, auto rentals, and broadband, so retail customers change suppliers more frequently. In a transparency scenario, price-comparison portals help customers to change their electricity and gas providers regularly—for example, by acting as energy agents or through an automated process that selects the cheapest offer at the end of a contract. Verivox recently announced the first steps in such a process.

With such rapid churn, utilities may lose many customers—even some who have never indicated any desire to change their suppliers. Once again, companies might be reduced to providers of commoditized electricity. Retail margins would wilt in the face of the negotiating power, agility, and customer-centricity of energy agents.

Assess the stress

To understand the potential impact of these five extreme scenarios, we modeled their effects on

the profits and losses, balance sheet, and cash flow of a hypothetical utility for each of several business segments: generation, renewables, trading, distribution, and retail. After modeling the effects of a scenario separately for each business, we combined them to show the effect on the enterprise. To be clear on the overall effects, you must understand, in detail, that the scenarios have specific impacts on different business units.

Exhibit 2 offers a heat map of these effects, highlighting the areas of greatest impact. For example, it shows that the energy-for-free and decentralized-energy-landscape scenarios would of course have a direct and massive impact on revenues, leading to a substantial loss of equity and an increase in net debt. On the other hand, an emissions fraud or cyberattack would have almost no relevance for revenues—but equity would suffer substantially.

This exhibit also highlights the key drivers of these effects: for example, in the energy-for-free scenario, B2C volumes and market share would decline sharply, and retail prices would fall by 5 percent. In an emissions-fraud scenario, operating and maintenance costs would soar by 50 percent, and utilities would pay regulatory penalties of up to 5 percent of revenues. If a cyberattack should take down a national grid, affected utilities would have to write off 5 percent of their physical assets; to replace them, they would boost their budgets for property, plant, and equipment by 7.5 percent. Earnings would crash, though the effect would be milder after taxes and depreciation.

The financial implications would be considerable across the scenarios, though none would necessarily bankrupt a company. Significant profit and liquidity risks appear, especially in the generation and retail businesses. In the absence of successful countermeasures, all five scenarios lead to negative recurring earnings before interest and taxes, revealing major risks for the sustainability

of the current business portfolio. Furthermore, the scenarios suggest a 10 to 60 percent drop in equity and a 5 to 40 percent increase in net debt—which might trigger liquidity concerns.

Get ready to improve resilience

Of course, utilities can forestall or mitigate many of the effects of stress. Hedging and insurance offer some protection. Establishing a crisis-response team is a no-regrets move for most companies.

Better preparation, such as stronger analytics and more transparent reporting, can help identify problems such as legal fraud or cyber vulnerabilities and help companies negotiate with regulators. The German government, for example, asked utilities to stress test their balance sheets and cash flows for a planned change in the disposal and storage of nuclear waste. As a result of the tests, the government took responsibility for these activities.

Exhibit 2 Stress tests show the material impact of a scenario.

■ Impact <5% ■ Impact <15% ■ Impact >15%

Effects of extreme scenarios on finances of hypothetical utility

Key scenario drivers

	Revenue	EBITDA ¹	EBIT ²	Capital expenditures	Equity	Net debt	
Current	100	13	2	6	18	34	Revenue set at 100; all other financial indicators indexed to revenue
Energy for free	83–94	9–12	–5–0	6	11–16	36–41	<ul style="list-style-type: none"> Total volume/market share decrease in B2C segment by 25–75% Reduction of retail prices by 5%
Decentralized	82–93	12–13	–7––2	6	9–14	35–38	<ul style="list-style-type: none"> B2C volume decreases by 20–50% Shutdown of underutilized plants and 5–10% write-off of grid and generation assets Decrease of wholesale prices by 5–10%
Emissions fraud	100	9	–9	9	7	48	<ul style="list-style-type: none"> O&M³ costs in generation increase 50% One-off penalty: 5% of total revenue €0.5 billion cost for external services No customer loss in B2C retail business
Cyberattack	99	8	–6	10	10	43	<ul style="list-style-type: none"> 5% PP&E⁴ one-off write-offs 7.5% PP&E one-off investment 10% increase in grid field-crew expenses No customer loss in B2C retail business
Price transparency	92	9	–3	6	13	39	<ul style="list-style-type: none"> Reduction of retail prices by 15% 20% loss of B2C customers 20% staff reduction, with severance payments of 150% of annual salaries

¹Earnings before interest, taxes, depreciation, and amortization.

²Earnings before interest and taxes.

³Operations and maintenance.

⁴Plant, power, and equipment.

Source: McKinsey analysis

A cyberattack taking critical infrastructure offline is now more probable, as power and gas grids, street lighting, and traffic control are highly connected.

Energy companies should also monitor external developments closely. Today, many utilities are watching the development of battery costs, since if they fall sharply, as they have in solar photovoltaics, generation and retail businesses would be vulnerable. Some utilities are partnering with or investing in battery companies. Many long-term strategic options are available, including nimble resource allocation and the transformation of companies into digital utilities.

All these techniques for building resilience are well covered elsewhere. Our point is that only by building a stress-testing capability can a company know where to focus its efforts for resilience. Leaders need to make stress testing an integral part of the DNA of decision making. They can start by defining a set of suitable stress tests in two ways: conducting a thorough review of the business system (to see around corners) and questioning basic assumptions. Then they can quantify the potential impact of any risks and assess the resilience of the company and its individual business units.

Adding a stress-testing capability isn't onerous. Companies will probably need one or two additional researchers to complement their current market-intelligence and analytics teams. In all likelihood, the scenario-planning models currently in use can be repurposed for stress tests.

The strategy function is stress testing's natural owner, as part of the main strategic-planning process and linked to financial planning. The businesses should offer input much as they do today. Decision-making groups (such as the executive, strategy, or investment committees) should use stress-test results in their work, integrating the new capability into the organization. The traditionally strong links among strategy, finance, and operations should insure smooth integration and interaction. ■

Sven Heiligtag is a partner in McKinsey's Hamburg office, where **Susanne Maurenbrecher** is a consultant; **Niklas Niemann** is a consultant in the Cologne office.

Copyright © 2017 McKinsey & Company.
All rights reserved.



© polygraphus/Getty Images

The evolution of model risk management

An increasing reliance on models, regulatory challenges, and talent scarcity is driving banks toward a model risk management organization that is both more effective and value-centric.

Ignacio Crespo, Pankaj Kumar, Peter Noteboom, and Marc Taymans

The number of models is rising dramatically—10 to 25 percent annually at large institutions—as banks utilize models for an ever-widening scope of decision making. More complex models are being created with advanced-analytics techniques, such as machine learning, to achieve higher performance standards. A typical large bank can now expect the number of models included within its model risk management (MRM) framework to continue to increase substantially.

Among the model types that are proliferating are those designed to meet regulatory requirements, such as capital provisioning and stress testing. But importantly, many of the new models are designed to achieve business needs, including pricing, strategic

planning, and asset-liquidity management. Big data and advanced analytics are opening new areas for more sophisticated models—such as customer relationship management or anti-money laundering and fraud detection.

The promise and wider application of models have brought into focus the need for an efficient MRM function, to ensure the development and validation of high-quality models across the whole organization—eventually beyond risk itself. Financial institutions have already invested millions in developing and deploying sophisticated MRM frameworks. In analyzing these investments, we have discovered the ways that MRM is evolving and the best practices for building a systematically

value-based MRM function (see sidebar, “Insights from benchmarking and MRM best practices”). This article summarizes our findings.

Model risk and regulatory scrutiny

The stakes in managing model risk have never been higher. When things go wrong, consequences can be severe. With digitization and automation, more models are being integrated into business processes, exposing institutions to greater model risk and consequent operational losses. The risk lies equally in defective models and model misuse. A defective model caused one leading financial institution to suffer losses of several hundred million dollars when a coding error distorted the flow of information from the risk model to the portfolio-optimization process. Incorrect use of models can cause as much (or greater) harm. A global bank misused a risk-hedging tool in a highly aggressive manner and, as a result, passed its value-at-risk limits for nearly a week. The bank eventually detected the risk, but because the risk model it used was inadequately governed and validated, it only adjusted control parameters rather than change its investment strategy. The consequent loss ran into the billions. Another global bank was found in violation of European banking rules and fined hundreds of millions of dollars after it misused a calculation model for counterparty-risk capital requirements.

Events like these at top institutions have focused financial-industry attention on model risk. Supervisors on both sides of the Atlantic decided that additional controls were needed and began applying specific requirements for model risk management on banks and insurers. In April 2011, the US Board of Governors of the Federal Reserve System published the Supervisory Guidance on Model Risk Management (SR 11-7). This document provided an early definition of model risk that subsequently became standard in the industry: “The use of models invariably presents model risk,

which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.” SR 11-7 explicitly addresses incorrect model outputs, taking account of all errors at any point from design through implementation. It also requires that decision makers understand the limitations of a model and avoid using it in ways inconsistent with the original intent. The European Banking Authority’s Supervisory Review and Evaluation Process, meanwhile, requires that model risk be identified, mapped, tested, and reviewed. Model risk is assessed as a material risk to capital, and institutions are asked to quantify it accordingly. If the institution is unable to calculate capital needs for a specific risk, then a comprehensible lump-sum buffer must be fixed.

The potential value in mature MRM

The value of sophisticated MRM extends well beyond the satisfaction of regulatory regimes. But how can banks ensure that their MRM frameworks are capturing this value thoroughly? To find the answer, we must first look more closely at the value at stake. Effective MRM can improve an institution’s earnings through cost reduction, loss avoidance, and capital improvement. Cost reduction and loss avoidance come mainly from increased operational and process efficiency in model development and validation, including the elimination of defective models.

Capital improvement comes mainly from the reduction of undue capital buffers and add-ons. When supervisors feel an institution’s MRM is inadequate, they request add-ons. An improved MRM function that puts regulators in a more comfortable position leads to a reduction of these penalties. (The benefit is similar to remediation for noncompliance.) Capital inefficiency is also the result of excessive modeler conservatism. To deal with uncertainty, modelers tend to make conservative assumptions at different points in the models. The assumptions and attending

Insights from benchmarking and MRM best practices

Model risk management (MRM) was addressed as a top-of-mind concern by leading global banks in recent surveys and roundtables conducted in Europe and the United States by McKinsey and Risk Dynamics. The overall number of models varied widely, ranging from 100 to 3,000 per bank; the number of full-time equivalents (FTEs) dedicated to MRM and validation is also highly variable, with European banks dedicating an average of 8 FTEs per €100 billion of assets, while for US banks this average is 19. MRM groups have grown considerably in recent years, and that growth is expected to continue. Most banks said they still rely heavily on the support of external consultants for validation. The time period for validation varies, depending on model intensity. For European banks, model validation can take anywhere from a few days to 30 weeks, whereas

in the United States, we found that variation takes between one and 17 weeks. For both US and EU banks, pass/fail rates vary widely by model. The scope of MRM activities varies widely as well, especially for ongoing model monitoring and model implementation. With respect to governance, most of the MRM groups report directly to the chief risk officer (CRO), or to his or her direct report; the boards of these banks typically discuss MRM in at least six meetings per bank.

In probing the model risk management terrain more closely, our research identified important trends and defined a model life cycle, from planning and development through model use, risk appetite, and policies.¹ Our research also revealed the key questions on the agenda of chief risk officers (exhibit),

Exhibit CROs can address the model life cycle with key questions about model risk management.



Questions for chief risk officers (CROs)

Model planning and development

- In model development, what is the relationship between the corporation and its functions and business units?

Model validation

- For validation, what is the level of centralization and reporting?
- Is the outsourcing of validations an adequate practice? How should outsourcing be managed?

Model implementation

- What models are within the scope of model risk management? Do they include regulatory and nonregulatory models?
- How should models be prioritized (model “tiering”)?

Model control and monitoring

- Is the control unit independent of the validation unit?
- How can compliance with the line-of-defense framework be ensured?

Model use, risk appetite, and policies

- Is a model risk appetite in place?
- Is model risk being quantified systematically?
- Is top management aware of the importance and potential issues of model risk management (MRM)?
- How is the MRM organization designed, and who is in charge of each of its parts?

and the extent to which these questions are being addressed in some of the most important areas.

Model planning and development

Model planning should be well coordinated across the whole bank. While taking great care to maintain the independence of validation, the model-development group should work closely with validation, an approach that controls costs by reducing the number of iterations and overall development time.

Banks are increasingly centralizing model planning and development, with best-practice institutions setting up “centers of excellence”—advanced-analytics centers acting as service providers to business units. They have created three location models: a local model with the bulk of the work close to model owners, each of them with dedicated teams; a hybrid model; and a centralized model, with the bulk of the work performed in the dedicated corporate center.

As talent demands rise, the highly specialized skills needed to develop and validate models are becoming increasingly scarce. Nearly three-quarters of banks said they are understaffed in MRM, so the importance of adjusting the model risk function to favor talent acquisition and retention has become pronounced. Banks are now developing talent solutions combining flexible and scalable resourcing with an outsourcing component.

Validation

Best-practice institutions are classifying models (model “tiering”) using a combination of quantitative and qualitative criteria, including materiality and risk exposure (potential financial loss), and regulatory impact. Models are typically prioritized for validation based on complexity and risk associated with model failure or misuse. Model risk is defined according to potential impact (materiality), uncertainty of model

parameters, and what the model is used for. The level of validation is located along a continuum, with high-risk models prioritized for full validation and models of low risk assigned light validation. In the majority of banks we surveyed, validation is highly centralized and situated in the risk organization. Outsourcing is increasing at both European and US institutions, as a result of talent constraints.

Most US banks have strengthened the independence of validation, with the head reporting directly to the CRO. In the United States, material models have to be validated in great detail, with systematic replication and the use of challenger models. This approach is not uniformly applied in Europe, where “conceptual” validations are still accepted in many cases. Likewise, model implementation (in operational and production systems) is not validated consistently across EU banks.

Control and monitoring

In the United States, the Federal Reserve is strict about proper deployment of the three lines of defense, with all stakeholders playing their roles: model developers need to continuously monitor their models; validation must make periodic reviews and audits, relying on the right level of rigor and skills. In Europe, implementation of the three lines remains less defined. The regulatory focus is mainly on regulatory models, as opposed to the US approach, where proper control is expected for all material models, whatever their type. Consequently, in the European Union, few banks have a control and governance unit in charge of MRM policies and appetite; in the United States, nearly all banks have an MRM unit.

Model use, risk appetite, and policies

In accordance with best practices, approximately half the surveyed banks have integrated model risk within their risk-appetite statement, either as a separate element or within nonfinancial risks.

Only around 20 percent, however, use specific key performance indicators for model risk, mainly based on model performance and open validation findings on models.

All banks have a model governance framework in place, but 60 percent of the group uses it for the main models only (such as internal ratings based or stress testing). Half of the survey group has a model risk policy. For 60 percent of the group,

model ownership is held by users, representing the preferred option for institutions that are more advanced in model management, allowing a better engagement of business on data and modeling assumptions. Risk committees authorize model-use exceptions in around 70 percent of cases.

¹ The research was performed by McKinsey Risk Dynamics, which specializes in model risk and validation.

conservatism are often implicit and not well documented or justified. The opacity leads to haphazard application of conservatism across several components of the model and can be costly. Good MRM and proper validation increases model transparency (on model uncertainties and related assumptions) and allows for better judgments from senior management on where and how much conservatism is needed.

This approach typically leads to the levels of conservatism being presented explicitly, at precise and well-defined locations in models, in the form of overlays subject to management oversight. As a result, the total level of conservatism is usually reduced, as end users better understand model uncertainties and the dynamics of model outcomes. They can then more clearly define the most relevant mitigation strategies, including revisions of policies governing model use.

Profit and loss

With respect to improvement in profit and loss (P&L), MRM reduces rising modeling costs, addressing fragmented model ownership and processes caused by high numbers of complex models. This can save millions. At one global bank, the capital budget for models increased sevenfold in four years, rising from €7 million to €51 million. By gaining a better understanding of the model landscape, banks are

able to align model investments with business risks and priorities. By reducing model risk and managing its impact, MRM can also reduce some P&L volatility. The overall effect heightens model transparency and institutional risk culture. The resources released by cost reductions can then be reallocated to high-priority decision-making models.

Systematic cost reduction can only be achieved with an end-to-end approach to MRM. Such an approach seeks to optimize and automate key modeling processes, which can reduce model-related costs by 20 to 30 percent. To take one example, banks are increasingly seeking to manage the model-validation budget, which has been rising because of larger model inventories, increasing quality and consistency requirements, and higher talent costs. A pathway has been found in the industrialization of validation processes, which use lean fundamentals and an optimized model-validation approach.

- **Prioritization (savings: 30 percent).** Models for validation are prioritized based on factors such as their importance in business decisions. Validation intensity is customized by model tiers to improve speed and efficiency. Likewise, model tiers are used to define the resource strategy and governance approach.

- **Portfolio-management office and supporting tools (savings: 25 percent).** Inefficiency can be reduced at each stage of the validation process, with predefined processes, tools, and governance mechanisms. These include development and submission standards as well as validation plans and playbooks.
- **Testing and coding (savings: 25 percent).** Automation of well-defined and repetitive validation tasks, such as standardized testing or model replication, can further lower costs.

The evolution toward capturing value systematically

To manage the P&L, capital, and regulatory challenges to their institutions' advantage, leading banks are moving toward a robust MRM framework that deploys all available tools to capture efficiencies and value. The path to sophisticated model risk management is evolutionary—it can be usefully

discussed as having three stages: building the elements of the foundation, implementing a robust MRM program, and capturing the value from it (Exhibit 1).

Building the foundational elements

The initial phase is mainly about setting up the basic infrastructure for model validation. This includes the policies for MRM objectives and scope, the models themselves, and the management of model risk through the model life cycle. Further policies determine model validation and annual review. Model inventory is also determined, based on the defined characteristics of the model to be captured and a process to identify all models and nonmodels used in the bank. Reports for internal and external stakeholders can then be generated from the inventory. It is important to note, however, that the industry still has no standard of what should be defined as a model. Since banks differ on this basic definition, there are large disparities in model-inventory statistics.

Exhibit 1 Model risk management has three evolutionary stages.

	Stage 1 Foundational elements	Stage 2 Implementation and execution	Stage 3 Capturing value
Objectives	<ul style="list-style-type: none"> • Build foundation elements for model risk management (MRM) 	<ul style="list-style-type: none"> • Implement robust MRM 	<ul style="list-style-type: none"> • Gain efficiencies and extract value from MRM
Key elements	<ul style="list-style-type: none"> • MRM policy • Model inventory • Manual work-flow tool • Model governance and standards • MRM organization <ul style="list-style-type: none"> – Governance team – Validation team 	<ul style="list-style-type: none"> • MRM policy • Control and process • Training for stakeholders • Automated work-flow tool 	<ul style="list-style-type: none"> • Center of excellence for model development • Industrialized validation • Transparency in model quality • Process-efficiency tracking • Optimized resource management

Most North American banks are in stage 2 of MRM evolution, while many European peers are still in stage 1.

Governance and standards are also part of the MRM infrastructure. Two levels of governance are set up: one covering the steps of the model life cycle and one for the board and senior management. At this point, the MRM function will mainly consist of a small governance team and a team of validators. The governance team defines and maintains standards for model development, inventory, and validation. It also defines stakeholder roles, including skills, responsibilities, and the people who will fill them. The validation team conducts technical validation of the models. Most institutions build an MRM workflow tool for the MRM processes.

Implementing a robust program

With foundational elements in place, banks can then build an MRM program that creates transparency for senior stakeholders on the model risk to the bank. Once model-development standards have been established, for example, the MRM program can be embedded across all development teams. Leading banks have created detailed templates for development, validation, and annual review, as well as online training modules for all stakeholders. They often use scorecards to monitor the evolution of model risk exposure across the institution.

A fundamental objective is to ensure high-quality, prioritized submissions. Model submissions missing key components such as data, feeder models, or monitoring plans reduce efficiency and increase delivery time. Efficiency can be meaningfully enhanced if all submissions adhere to standards before the validation process begins. Models are prioritized based on their importance to the business, outcome of prior validation, and potential for regulatory scrutiny.

Gaining efficiencies and extracting value

In the mature stage, the MRM function seeks efficiencies and value, reducing the cost of managing model risk while ensuring that models are of the highest quality. In our survey of leading financial

institutions, most respondents (76 percent) identified incomplete or poor quality of model submissions as the largest barrier for their validation timelines.¹ Model owners need to understand the models they use, as they shall be responsible for errors in decisions based on those models.

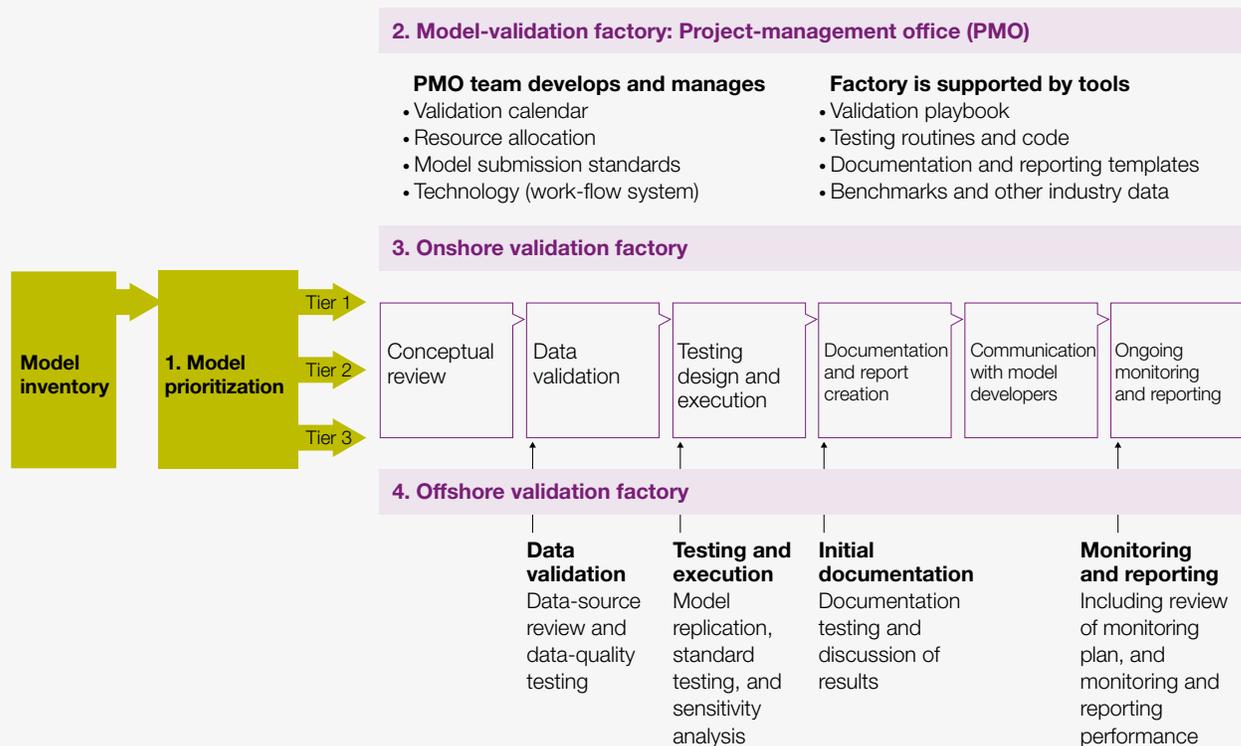
One of the best ways to improve model quality is with a center of excellence for model development, set up as an internal service provider on a pay-per-use basis. Centers of excellence enable best-practice sharing and advanced analytics across business units, capturing enterprise-wide efficiencies. The approach increases model transparency and reduces the risk of delays, as center managers apply such tools as control dashboards and checkpoints to reduce rework.

Process automation defines MRM maturity, as model development, validation, and resource management are “industrialized” (Exhibit 2). Validation is led by a project-management office setting timelines, allocating resources, and applying model-submission standards. Models are prioritized according to their importance in business decisions. An onshore “validation factory” reviews, tests, and revises models. It can be supported by an off-shore group for data validation, standards tests and sensitivity analysis, initial documentation, and review of model monitoring and reporting. The industrial approach to validation ensures that models across the organization attain the highest established standards and that the greatest value is captured in their deployment.

The standards-based approach to model inventory and validation enhances transparency around model quality. Process efficiency is also monitored, as key metrics keep track of the models in validation and the time to completion. The validation workflow system improves the model-validation factory, whose enterprise-wide reach enables efficient resource deployment, with cross-team resource

Exhibit 2

Industrialized model validation defines mature model risk management.



sharing and a clear view of validator capabilities and model characteristics.

Consistent standards for model planning and development allow institutions to develop more accurate models with fewer resources and in less time. In our experience, up to 15 percent of MRM resources can be conserved. Similarly, streamlining the model-validation organization can save up to 25 percent in costs. With the significant regulatory spending now being demanded of institutions on both sides of the Atlantic, these savings are not only welcome but also necessary.



The contours of a mature stage of model risk management have only lately become clear. We now know where the MRM function has to go in order

to create the most value amid costly and highly consequential operations. The sooner institutions get started in building value-based MRM on an enterprise-wide basis, the sooner they will be able to get ahead of the rising costs and get the most value from their models. ■

¹ Many fewer respondents cited a lack of sufficient resources (14 percent) and the need to validate each model comprehensively (10 percent).

Ignacio Crespo is an associate partner in McKinsey's Madrid office, **Pankaj Kumar** is an associate partner in the New York office, where **Peter Noteboom** is a partner, and **Marc Taymans** is a managing partner in McKinsey's Risk Dynamics group.

Copyright © 2017 McKinsey & Company. All rights reserved.



© Agsandrew/Getty Images

Digital risk: Transforming risk management for the 2020s

Significant improvements in risk management can be gained quickly through selective digitization—but capabilities must be test hardened before release.

Saptarshi Ganguly, Holger Harreis, Ben Margolis, and Kayvaun Rowshankish

Digitization has become deeply embedded in banking strategy, as nearly all businesses and activities have been slated for digital transformations. The significant advantages of digitization, with respect to customer experience, revenue, and cost, have become increasingly compelling. The momentum to adopt the new technologies and operating models needed to capture these benefits continues to build. The risk function, which has seen significant growth in costs over the past decade, should be no exception. Indeed, we are starting to see digital transformations in risk create real business value by improving efficiency and the quality of risk decisions. A digitized risk function also provides better monitoring and control and more effective regulatory compliance.

Experience shows that the structural changes needed to bring costs down and improve effectiveness in risk can be accomplished much like digital transformations in other parts of the bank. The distinguishing context of the risk environment, however, has important implications. First, risk practitioners in most regulatory jurisdictions have been under extreme pressure to meet evolving regulatory requirements and have had little time for much else. Second, chief risk officers have been wary of the test-and-learn approaches characteristic of digital transformation, as the cost of errors in the risk environment can be unacceptably high. As a result, progress in digitizing risk processes has been particularly slow.

This status quo may be about to change, however, as global banking leaders begin to recognize how substantial value can be unlocked with a targeted digital agenda for risk featuring fit-for-purpose modular approaches. In addition to the objective of capturing value, this agenda incorporates risk-specific goals. These include ensuring the ongoing effectiveness of the control environment and helping the risk function apply technology to better address regulatory expectations in key areas—like risk measurement, aggregation, and reporting.

What is digital risk?

Digital risk is a term encompassing all digital enablements that improve risk effectiveness and efficiency—especially process automation, decision automation, and digitized monitoring and early warning. The approach uses work-flow automation, optical-character recognition, advanced analytics (including machine learning and artificial intelligence), and new data sources, as well as the application of robotics to processes and interfaces. Essentially, digital risk implies a concerted adjustment of processes, data, analytics and IT, and the overall organizational setup, including talent and culture.

Three dimensions of change: Processes, data, organization

To realize the full benefits of process and decision automation, banks need to ensure that systems, processes, and behaviors are appropriately fitted for their intended purpose. In the risk environment, prioritized use cases are isolated in such areas as credit underwriting, stress testing, operational risk, compliance, and control. In most banks, current processes have developed organically, without a clearly designed end state, so process flows are not always rational and efficient. Operational structures will need to be redesigned before automation and decision support can be accordingly enabled.

Data, analytics, and IT architecture are the key enablers for digital risk management. Highly fragmented IT and data architectures cannot provide an efficient or effective framework for digital risk. A clear institutional commitment is thus required to define a data vision, upgrade risk data, establish robust data governance, enhance data quality and metadata, and build the right data architecture. Fortunately, processes and analytics techniques can now support these goals with modern technology in several key areas, including big data platforms, the cloud, machine learning, artificial intelligence, and natural-language processing.

The organization and operating model will require new capabilities to drive rapid digitization. Although risk innovation takes place in a very specific, highly sensitive area, risk practitioners still need to create a robust culture of innovation. This means putting in place the right talent and nurturing an innovative “test and learn” mind-set. Governance processes must enable nimble responses to a fast-moving technological and regulatory environment. Managing this culture of innovation in a way that is appropriate for risk constitutes a key challenge for the digitized risk function.

Adapting digital change to the risk context

Most institutions are digitizing their risk functions at a relatively slow pace, taking modular approaches to targeted areas. A few have undertaken large-scale transformation, achieving significant and sustainable advances in both efficiency and effectiveness. Either way, in the risk context, care must be taken when adapting test-and-learn pilots commonly used in digital transformations in other parts of the bank. Robust controls must be applied to such pilots, as the tolerance for bugs and errors in risk is necessarily very low. When digitizing processes relating to comprehensive capital analysis and review (CCAR), for example, solutions cannot be

introduced into production before thorough testing has convinced designers and practitioners of their complete reliability and effectiveness. In certain other risk areas—such as monitoring and early-warning systems in commercial credit risk—banks can use test-and-learn approaches effectively.

Sizing the opportunity

Our experience suggests that by improving the efficiency and effectiveness of current risk-management approaches, digital risk initiatives can

reduce operating costs for risk activities by 20 to 30 percent. The state of risk management at most global, multiregional, and regional banks is abundant with opportunity. Current processes are resource intensive and insufficiently effective, as indicated by average annual fines above \$400 million for compliance risk activities alone (Exhibit 1).

The potential benefits of digital risk initiatives include efficiency and productivity gains, enhanced risk effectiveness, and revenue gains. The benefits of

Exhibit 1 Digital risk management can significantly reduce losses and fines in core risk areas.

Impact from digitization: ■ High ■ Medium ■ Low

Risk areas	Representative global bank			Representative regional bank		
	Losses 2015, \$ billion	Fines, 2009–15, \$ million		Losses 2015, \$ billion	Fines, 2009–15, \$ million	
		Year avg.	Top decile		Year avg.	Top decile
Credit risk	20–40	30–50	600+	3–5	5–10	150+
Operational risk	2–4	300–600	4,500+	0.2–0.3	10–20	225+
Compliance risk		400–600	1,850+		15–30	350+
Market and liquidity risk	<0.5	75–150	500+	<0.1	20–40	300+
Stress testing	NA	NA	NA	NA	NA	NA

The greatest financial opportunities from digitization for both universal and regional banks are in the areas of operational and compliance risk

Note: Credit risk losses are gross charge-offs; operational and compliance risk losses do not include opportunity costs (such as unearned revenue due to operational risk events); the average total yearly fines are given for banks fined at least once in the period 2009–15.

Source: Bank holding company Y9C reporting forms; *Financial Times*' bank-fines data; McKinsey analysis

greater efficiency and productivity include possible cost reductions of 25 percent or more in end-to-end credit processes and operational risk, through deeper automation and analytics. Risk effectiveness can be strengthened with superior transparency, gained through better management and regulatory reporting and the greater accuracy of model outputs due to better data. Revenue lift can be achieved through better pricing or an enhanced customer and frontline experience—for example, by reducing the know-your-customer (KYC) cycle time from one week to under one day, or the mortgage-application process to under 30 minutes, from 10 to 12 days. Improved employee satisfaction can also be achieved through focusing talent on high-value activities.

Target risk processes: Credit risk, stress testing, and operational risk and compliance

The possible action areas for digital risk are extensive, but in our view three specific areas are optimal for near-term efforts: credit risk, stress testing, and operational risk and compliance. Although no one bank has fully digitized all three of these areas, we are seeing leading banks prioritize digital initiatives to realize discrete parts of the total savings available. The following discussion is based on actual digital risk initiatives across risk types and processes.

Credit risk

Credit delivery is hampered by manual processes for data collection, underwriting, and documentation, as well as data issues affecting risk performance and slow cycle times affecting the customer experience. Digital credit risk management uses automation, connectivity, and digital delivery and decision making to alleviate these pain points. Value is created in three ways: by protecting revenue, improving risk assessments, and reducing operational costs.

To protect revenue in consumer credit, digital risk strengthens customer retention. It improves the customer experience with real-time decisions, self-service credit applications, and instant credit approvals. The improvements are enabled through integration with third parties for credit adjudication and the use of dynamic risk-adjusted pricing and limit setting. One European bank is exploring the potential for digital risk to expand revenue in consumer credit within the same risk appetite. Digitized credit processes will permit faster decision making than the competition while the bank maintains its superior risk assessment.

Value is also created by improving risk assessment. Advanced analytics and machine-learning tools can increase the accuracy of credit risk models used for credit approvals, portfolio monitoring, and workouts. It can also reduce the frequency of judgment-based errors. The integration of new data sources enables better insights for credit decisions, while real-time data processing, reporting, and monitoring further improve overall risk-management capabilities. Operational costs are also reduced as credit processes are digitized. A greater share of time and resources can be dedicated to value-added activities, as inputs and outputs become standardized and paperless.

In addition to improving default predictions, we have seen credit risk improvements in these areas creating a revenue lift of 5 to 10 percent and lowering costs by 15 to 20 percent (Exhibit 2).

Stress testing, including CCAR

Banks find that significant value can be captured through a targeted digitization effort for stress testing, including CCAR. The current approach is highly manual, fragmented, and sequential, presenting challenges with data quality, aggregation, and reporting time frames and capacity. The

Exhibit 2

An integrated digital risk program for consumer credit can protect revenue, improve risk assessments, and reduce operational costs.

Improvement potential: ■ High (10%+) ■ Medium (5–10%) ■ Low (0–5%)

Credit risk value chain		Digital credit risk value map			
		Revenue improvement	Cost reduction	Cost of risk mitigation	
Work flow	Appetite and limit setting	Strategies and policies	Low	Medium	High
	Front office, customer contact	Sales and planning	High	High	Medium
		Pricing	High	Medium	High
	Credit analysis and decision	Analysis	Low	High	High
		Scoring and rating	Low	Medium	High
		Application	Low	High	Low
		Decision making	High	High	High
	Back office/loan administration	Contracts and documents	Low	High	Low
		Collateral management	Low	High	Medium
	Monitoring/early-warning system	Issue identification	Low	High	High
		Action recommendation	Low	Medium	High
	Collection and restructuring	Workout strategies	Low	Medium	High
		Restructuring	Low	Medium	High
Reporting	Report generation	Medium	High	High	
	Insights/analysis	Medium	High	High	
	Work-flow support	Low	High	Low	

processes are prime candidates for digital automation and work-flow tools.

The underlying stress-testing process is the starting point. The improvement program will aim at optimizing resources. Dedication of resources will be prioritized based on materiality of risk. Institutions can achieve additional efficiency through parallel processing, centralization, and cross-training of staff, as well as better calendaring.

Templates and outputs are standardized, and “golden” sources for data are designated. The resulting process becomes increasingly transparent and effective. Process optimization is supported by digital-automation initiatives for data loading, overlays, Y14A reports, and the end-to-end review and challenge process. Real-time visualization and sensitivity analysis are digitally enabled as part of the transformation. In addition to optimizing stress testing directly, banks are also looking for

opportunities to harmonize the data, processes, and decision-making models with business planning.

We have seen digitization in CCAR and stress testing bring significant cost improvements and—even more important—free up capacity so that experts can apply more insight and improve the quality and use of outputs (Exhibit 3).

Operational risk and compliance

At many global banks, manual processes and fragmented systems have proliferated across

operational risk and compliance controls and activities. In anti-money laundering (AML), for example, processes and data have become unwieldy, costs have skyrocketed, and efforts have become ineffective. Significant opportunities to increase the effectiveness and efficiency of AML operations lie in thorough end-to-end streamlining of the alert-generation and case-investigation processes.

In alert generation, digital risk improvements ensure that reference data available for use in the analytic engine is of high quality. Advanced-analytics tools

Exhibit 3

There are many ways digitization can improve efficiency and effectiveness of comprehensive capital analysis and review (CCAR) and stress testing.

■ High impact ■ Medium impact ■ Low impact

Core CCAR elements	Supporting activities	How to digitize
Risk identification	<ul style="list-style-type: none"> Risk assessment Risk aggregation and reporting 	Implementation of tool to collect and aggregate risks
Scenario	<ul style="list-style-type: none"> Forecast development Macro forecasts 	“Appification” of scenario syndication by lines of business, senior executives, and board
Data, models, and forecasting	<ul style="list-style-type: none"> Data preparation Model development 	Adoption of end-to-end data-hosting solution and model-development environment
Aggregation and reporting	<ul style="list-style-type: none"> Jump-off data and forecast execution Aggregation and schedule construction 	Automated aggregation engine with feeds from model-development environment
Review and challenge		Creation of dynamic review-and-challenge app
Internal controls		Implementation of control-monitoring and attestation tool
Documentation		Adoption of work-flow, tracking, aggregation, and storage tool

such as machine learning are used to test and refine the case-segmentation variables and support “auto-adjudication” where possible. In addition, digitization and work-flow tools can support smart investigations and automated filing of suspicious-activity reports, an improvement that enhances the productivity of the investigation units.

Our experience of digital risk initiatives in AML is that they invariably improve effectiveness and efficiency, typically in the range of 20 to 25 percent. The overall impact of such improvement is even greater, however, given the large cost base of this function across institutions and the risk of not identifying bad actors.

Digital risk is different

A digital risk program must be designed in recognition of those aspects of the risk function that distinguish it from other functions, such as frontline digital sales. For risk, regulators will not accept the characteristic approaches of traditional digital transformations. Live launches of “minimum viable products” to be tested and refined in production is not an appropriate path for most risk activities. Most approaches to digitization focus on improving the customer experience. Digital risk will involve some actual external customers, such as in credit delivery, but in most areas the focus will be on internal customers, stakeholders, and regulators. Moreover, digital risk is never a self-contained effort—it will depend on data from all businesses and functions. Development thus proceeds at a pace limited by the careful management of these interdependencies. Innovative approaches such as agile and digital labs provide effective options to implement solutions incrementally.

Direct impact will be felt in cost and risk reduction

While digital risk offers clear opportunities for significant cost reduction, the impact on revenue is less obvious but implicitly understood by leaders. Frontline digital transformations are often aimed

at direct revenue improvement; proof of this impact from digital risk programs is more elusive, since risk is an enabling function. Faster turnaround times for loan applications is a typical digital risk improvement. This will likely drive higher lending volumes and, consequently, increased revenue—even if the correlation cannot be precisely determined. Given the indirect impact on revenue, digital risk programs should focus primarily on reducing risk and cost. The exception is digital credit, where the case for revenue lift will be clearer.

Designing a program

An effective digital risk program begins with chief risk officers asking the right questions—those that point the institution toward specific initiatives for digital innovation. “Can we reduce the time needed for structured credit approvals to a few minutes?” “How can we increase straight-through processing rates?” “How can we improve the efficiency and streamlining of KYC activities to reduce pain points in the account-opening process?” “How can we make CCAR less sequential and resource intensive?” “How can we improve the timeliness of reporting to meet regulatory objectives?” “What value can we extract from better use of internal data?” “What is the incremental benefit of including new data sources?” The answers will help shape initiatives, which will be prioritized according to current resource-allocation levels, losses and regulatory fines, and implementation considerations, such as investment and time.

Digital risk programs can incorporate the familiar design features of digital transformations, such as zero-based process and interface redesign and an agile framework. The testing and refinement, however, takes place entirely within a controlled environment. The design approach, which can be modular, must also be comprehensive, based on a thorough review of risk activities, appetite, and policies.

The designs cannot be migrated into production until they have been thoroughly tested and

syndicated, often with regulatory bodies. Because of its highly sensitive environment, risk is digitized end to end over a longer timeline than is seen in customer-service areas. Specific capabilities are developed to completion and released discretely, so that risk management across the enterprise is built incrementally, with short-term benefits.

The anatomy of a transformation

A digital risk program can get a running start by capturing high-value opportunities first. The anatomy of the transformation will resemble that of other digital transformations, with the usual three stages: 1) priority initiatives are identified according to the value at stake and the feasibility for near-term implementation, 2) digital solutions are designed to capture that value and tested and revised according to stakeholder input, and 3) the improvement is introduced into production, with continued capability building to embed the design, engineering, and change management into the operating model and invest in the right capabilities and mind-sets.

The opportunities identified in stage one are matched in stage two with digital and other solutions that will reduce waste and optimize resources while improving standardization and quality. These solutions will involve work-flow automation, digital interfaces, and the use of advanced analytics and machine learning. The technology design may use a “two speed” architecture to support fast innovation in IT while allowing the main IT infrastructure to operate normally. New functionality is rigorously tested prior to migration into production, to ensure a smooth, error-free transition for critical risk functions. Iterative test-and-learn processes take place within environments featuring higher control standards than typical elsewhere. Stakeholder feedback and often regulator syndication are obtained prior to production release.

In the third stage, where the innovation is introduced into production, the organization focuses on change management. In itself, this is no different from typical digitization programs in other business areas. The focus is on embedding the design into the operating model and continuing to invest in digital capabilities to build momentum for further launches. Having the right talent in place, whether drawn from internal or external sources, is the key to a successful transition to digital risk.



The path to digital risk will be a multiyear journey, but financial institutions can begin to capture significant value within a few months, launching tailored initiatives for high-value targets. As the risk function becomes progressively digitized, it will be able to achieve higher levels of efficiency, effectiveness, and accuracy. In the future, risk management will be a lean and agile discipline, relieving cost pressures, improving regulatory compliance, and contributing to the bank’s ability to meet escalating competitive challenges. The first steps toward that future can be made today. ■

Saptarshi Ganguly is a partner in McKinsey’s Boston office, **Holger Harreis** is a partner in the Düsseldorf office, and **Ben Margolis** is an associate partner in the New York office, where **Kayvaun Rowshankish** is a partner.

Copyright © 2017 McKinsey & Company.
All rights reserved.

January 2017

Designed by Global Editorial Services

Copyright © McKinsey & Company

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

Printed in the United States of America.