McKinsey&Company

McKinsey Working Papers on Risk, Number 34

Driving value from postcrisis operational risk management

A new model for financial institutions

Benjamin Ellis
Ida Kristensen
Alexis Krivkovich
Himanshu P. Singh

June 2012

Contents

McKinsey Working Papers on Risk presents McKinsey's best current thinking on risk and risk management. The papers represent a broad range of views, both sector-specific and cross-cutting, and are intended to encourage discussion internally and externally. Working papers may be republished through other internal or external channels. Please address correspondence to the managing editor, Rob McNish (rob_mcnish@mckinsey.com).

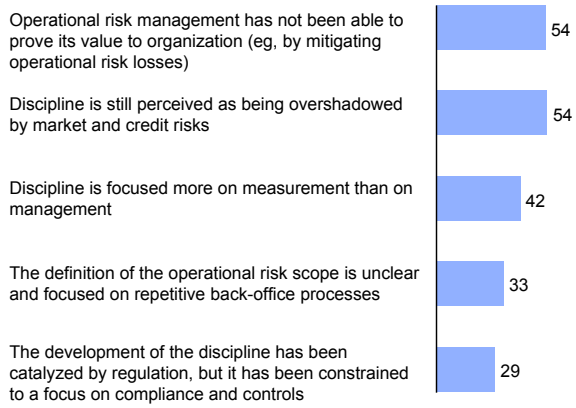
Driving value from postcrisis operational risk management: A new model for financial institutions

A series of costly, headline-grabbing operational risk incidents among financial institutions, including the regulatory settlements of US mortgage servicers and cases of "rogue trading," has once again brought operational risk management (ORM) to the forefront of CEOs' and CROs' agendas. In these and other cases, significant losses have been incurred as a result of operational failures. Improved ORM, including processes designed to flag near-misses or areas of concern (unusual volumes or a high number of exceptions, for example), might have helped to avert events that not only caused up-front losses but also did serious reputational harm and damaged investor confidence.

As the size and structural complexity of financial institutions has increased, so too has the challenge of understanding and mitigating operational risks. And heightened regulatory scrutiny has increased the costs—financial and otherwise—of operational risk events. However, while the value of effectively managing operational risk has increased significantly of late, the actual management of that risk has not evolved commensurately. Many financial institutions continue to see ORM as an immature discipline that serves as a regulatory box-checking exercise, creating an administrative and financial burden with few business benefits. These challenges were highlighted in a 2009 McKinsey study of operational risk managers and other senior bank managers (Exhibit 1).

Executed properly, improvements in ORM can lead to substantial financial benefits, as well as regulatory and compliance benefits, through increased profitability, greater financial stability, and improved customer experience. To achieve these gains, financial institutions must apply a consistent and comprehensive approach, tailored to their specific operational risks, that is fundamentally different from the approaches used for managing market and credit risks.

Exhibit 1 Operational risk management is seen as an immature discipline.



1 Joint McKinsey and Risk Management Association study on the future of the discipline of operational risk management, 2009.

Source: Study on the future of the discipline of operational risk management, 2009

Why financial institutions should worry about managing their operational risk

Ineffective ORM negatively affects financial institutions in three ways. First, actual operational risk losses represent a direct hit to the income statement, as do the costs of inefficient processes. Second, equity markets punish companies for operational risk failures, and this often well exceeds the actual financial losses experienced. Finally, operational risk failure can increase costs and complexity of compliance by raising regulatory scrutiny, affecting not just the specific failure but the institution as a whole.

Direct financial impact

One commonality that operational risk shares with credit and market risks is that all three are subject to "tail risk," creating the potential for very large losses. In recent months, this issue has come into focus following significant losses arising from rogue trading and serious operational issues related to mortgage operations.

In addition to operational losses, inadequate ORM may result in foregone revenues. One recent review of an operational risk event at a large credit-card issuer revealed a significant operational shortcoming in the loan-application process that resulted in roughly 20 percent of card applications not being properly reviewed. This increased the cost of processing loan applications and meant that the company missed out on substantial revenues. This category of operational risk—as opposed to the risk of a measurable-loss event—can have a direct financial impact, but it is often overlooked by typical operational risk approaches.

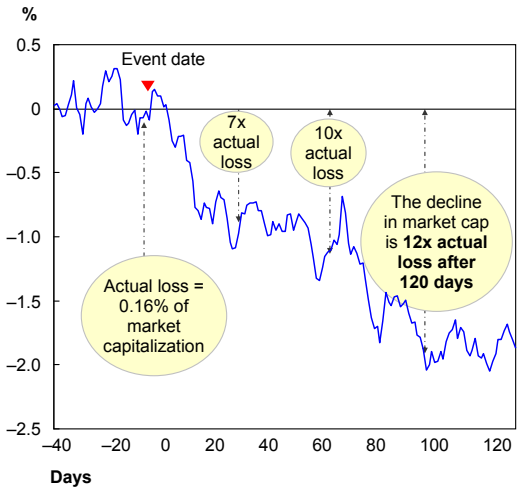
Impact on market capitalization

The financial fallout of operational risk failures typically extends beyond the initial loss to a reduction in market capitalization. Equity markets penalize institutions that incur losses because such losses suggest weaknesses in their operational risk controls. Controlling for other market factors, the negative impact on market value over a 120-day period following the announcement of an operational risk loss is roughly 12 times the amount of the actual loss (Exhibit 2).

This relationship was also recently demonstrated in a 15 times higher decline in a leading bank's market value than the actual losses suffered following its announcement of an uncontained trading loss. Such high multipliers indicate that investors lack confidence in the institution's ability to manage future loss events and expect additional losses.

Exhibit 2 The market value decline caused by operational risk failures is a multiple of the actual loss.

Impact of operational risk loss on market value, overall cumulative average abnormal returns[1]



1 Based on a sample of more than 350 operational-loss events, normalized for industry performance.
Source: Fitch; Datastream

Regulatory sanctions

Finally, inadequate ORM can lead to regulatory intervention or sanctions and, in some cases, a direct financial impact. For example, regulators required one bank in Singapore to increase its capital reserves for operational risk by an additional 200 million Singapore dollars following a data-center failure that lasted seven hours—although the bank made sure that affected customers were fully compensated. In other cases, regulators have required changes to business practices in response to operational risk failures, and these often increase the expense associated with specific business operations. For example, recent issues in US mortgage operations prompted regulators to require a single point of contact for delinquent mortgage borrowers, and the National Mortgage Settlement (announced on February 9, 2012), an agreement with the five largest mortgage servicers in the United States to address mortgage servicing, foreclosure, and bankruptcy abuses, includes more than 100 provisions that will affect mortgage-servicing processes from pre-foreclosure notices to loss-mitigation approval and appeal. Quite often, regulatory scrutiny is not limited to the proximate cause of operational failure but extends to other business processes. That increases the overall cost and complexity of compliance for financial institutions. More important, this type of regulatory intervention may be avoided if operational risk is managed more rigorously.

Five common challenges to effective ORM

While financial institutions have increased their focus on operational risk in recent years, ensuring effective oversight and management of these risks continues to be challenging for many institutions. In our experience, five key challenges must be overcome:

- **Understanding the uniqueness of ORM.** CROs and other senior leaders in risk typically have a background in either credit or market risk. A recent scan of the CROs of 25 large global, North American, and European banks and asset managers revealed that only one of these leaders had held a formal operational risk position prior to being designated CRO, while more than half had prior market- or credit-risk experience. This is likely to have at least two implications for the enterprise management of risk. First, CROs may make operational risk less of a priority than other types of risk that they are more comfortable with. Second, many CROs may be inclined to use the same type of frameworks to manage operational risk as they have previously deployed to manage market and credit risk. But operational risk cannot be effectively managed by deploying market- or credit-risk frameworks. While credit and market risk are directly linked to the balance sheet and are easily quantifiable, operational risk arises from multiple sources and is open-ended in nature; it therefore should be managed much more closely to the specific business processes where the risks arise. Furthermore, operational risks are relatively heterogeneous and thus require a broader spectrum of mitigation techniques, the vast majority of which involve deep engagement between operational managers and risk managers. Approaches that work for credit and market risk (for example, having centralized risk teams monitor the portfolio) can be manifestly ineffective for managing operational risk.

- **Making ORM decision focused.** Too often, financial institutions equate ORM with the *measurement* of operational risks and controls (potentially as part of operational risk-capital modeling). They spend too much time creating risk-identification and assessment processes (for instance, focusing on detailed risk-control self-assessments, or RCSAs, buried deep in the organization) and not enough time managing operational risks with an eye toward avoiding or mitigating losses. In one case, a large North American bank invested heavily to create an operational risk assessment that involved hundreds of employees who created tens of thousands of individual data points, only to realize that the tool did not identify their top risks or help manage operational risk. The bank subsequently had to overhaul the entire process at a significant cost. The example also demonstrates how financial institutions can fail to translate the vast operational risk data into useful information that can support business decisions and the prioritization of mitigation programs.

- **Ensuring consistency in risk evaluation and mitigation.** Management of operational risk at many financial institutions is siloed in different parts of the business, leading to inconsistency in how operational risks are measured across the enterprise and preventing a comprehensive enterprise-wide prioritization of risks and mitigation programs. People generally find it difficult to estimate the frequency and severity of low-probability events and lack even a basic taxonomy for understanding event consequences. This inherent weakness is exacerbated by institutional and organizational challenges. In one case, a large investment bank's different business units used different criteria for how to measure the frequency and severity of operational risk events, leading to inconsistent classification and an inability to compare the risks that had been identified. Correspondingly, the bank was unable to appropriately prioritize risks and optimize their mitigation programs. In another case, the business units and the centralized risk function at a large retail bank used different tools to measure and monitor operational risk, leading to similar inefficiencies and ineffective mitigation processes.

- **Clarifying roles and responsibilities.** Sound ORM requires the involvement of all of business lines, operations, and the risk function, but financial institutions often lack clarity around operational risk roles and responsibilities.

This ambiguity creates challenges for consolidating critical operational risk knowledge and may lead to unidentified risks, poorly managed risks, redundant activities, and ineffective communication to regulators and other external stakeholders. In some institutions, as many as seven different groups help manage operational risk: business operations, business IT, business risk, group risk, corporate risk, corporate IT, and compliance (with audit reviewing the full process).

- **Ensuring sufficient talent.** Successful operational risk professionals must combine a deep understanding of detailed business processes, the risk and control environment, regulatory requirements, and strong communication skills. This combination is relatively rare and takes time to develop. As the importance of managing operational risk has increased, many financial institutions have been forced to play catch-up in developing a sufficient group of skilled operational risk professionals.

Building a comprehensive approach to managing operational risks

Financial institutions have every motivation to try to overcome these challenges in order to maximize the value from their investment in ORM.

When embarking on the journey to improve the management of operational risk, each financial institution should start by asking itself: "What are the key management decisions we need to make related to operational risk?" Broadly speaking, there are three categories of decisions for managing operational risk:

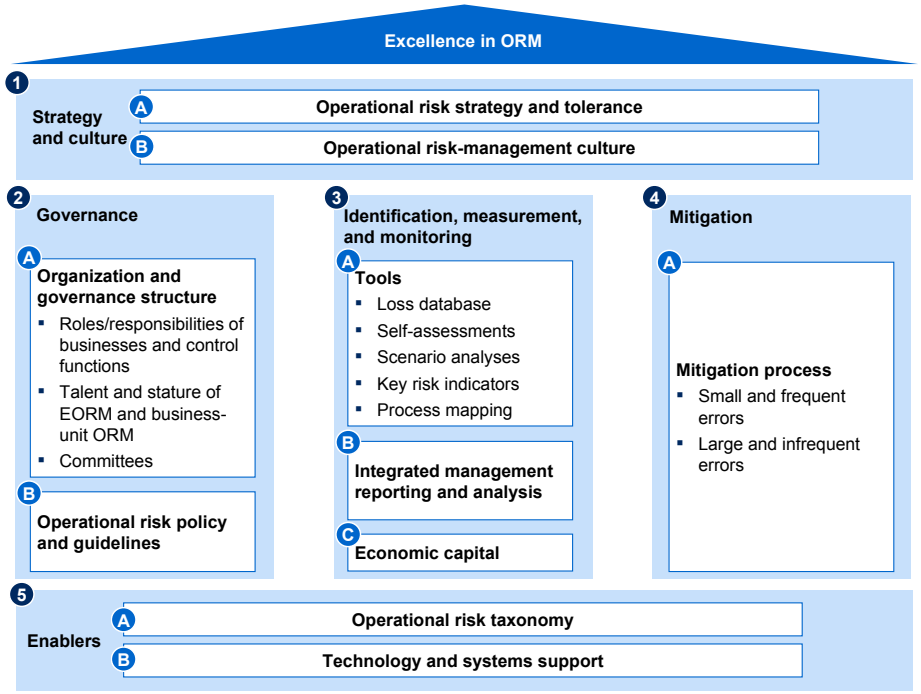
- Development and implementation of mitigation programs, including the improvement of controls (for example, by adding controls or automating controls)
- Changes to business processes (such as streamlining trade execution or redesigning the foreclosure process)
- Changes to business strategy (for instance, reducing the size or scale of a business or taking on a new business)

The goal of any operational risk framework should be to provide management with the information and resources needed to make and execute these types of decisions. The five components that collectively form an effective ORM framework are shown in Exhibit 3.

First, financial institutions need to articulate their overall enterprise-level operational risk strategy and tolerance, which will guide the level and types of operational risks they are willing to take and ensure that the organization's risk culture is consistent with its overall strategy. Due to the lack of comprehensive and detailed data for all operational risks, it is impractical to define risk tolerance in primarily quantitative terms and difficult to translate the high-level tolerance into specific business implications. In the words of one operational risk manager, "It is straightforward to say that the tolerance is for losses no larger than x dollars. But while this helps identify whether the risk tolerance has been breached, it does not help managers understand if the business is currently operating within tolerance. It is not actionable—you think you are operating within tolerance until a large loss occurs, and then, oops, it looks like you were out of tolerance after all."

Best-in-class financial institutions will therefore combine a quantitative articulation of operational risk loss levels, including tolerance for losses as well as key risk indicators (or KRIs, such as system downtime and attempted IT security breaches) with a qualitative tolerance statement covering the way in which operational risk decisions are made (for example, explicitly incorporating the reputational impact of operational risk events).

Exhibit 3 Five elements are required to ensure a comprehensive approach to ORM.



Second, they need to ensure that appropriate governance structures are in place to support the required management decisions. This includes defining clear roles and responsibilities for measuring, mitigating, and monitoring operational risks across the different lines of defense (execution, oversight, and audit), as well as ensuring effective escalation processes. To manage risks effectively, institutions should apply a top-down risk-based view, assigning clear responsibilities for all key operational risks. Effective governance also requires that sufficient talent is in place, covering all key operational risk responsibilities and doing so without impeding business execution. While this sounds straightforward, the number of natural owners for operational risk makes achieving and maintaining role clarity particularly challenging. We have seen multiple institutions where role clarity was not achieved until a dedicated effort was conducted with that specific goal.

Given the relative scarcity of operational risk talent, financial institutions are starting to take a more structured and proactive approach to developing talent. This involves mapping the skills and capabilities of risk professionals relative to those that are required, sometimes looking forward three or more years. Rotational programs (for instance, between risk and operations) and cross-hires from other parts of the organization can help broaden the pool of operational risk professionals.

Third, financial institutions need a comprehensive measurement framework for both risks and controls that incorporates extensive scenario analyses, a loss database, self-assessments (for instance, RCSA), and KRIs for all business processes. Most financial institutions have these basic building blocks in place. Nevertheless, in many cases, the outputs of these analyses are an end in themselves, and they are not sufficiently tied to underlying

processes. To be actionable from a mitigation perspective, the risk evaluation must take place at the process level; the outputs of these measurement tools must be tied to comprehensive and consistent business-process maps to have an effect.

Further, operational risk exposures should be assessed for individual business processes, evaluating historical as well as stressed KRIs. The controls available at each process level should also be evaluated to ascertain their ability to predict risks and prevent a loss event. In addition to measuring risk exposure at the process level, losses measured and maintained in the loss-events database must be tied to the processes where they originated (that is, a loss database should not only use general categories such as legal losses—it should also link particular losses to the part of the process, such as application fraud, where they occurred). The loss database and other risk-management infrastructure should use the same process maps as the business-process owners. At one large financial institution, we found that the risk function and the business units used different process maps for the same process. This lack of consistency led to inefficiencies and ineffectiveness—there were duplicative and competing measurements and the organization was not aligned on how to address the issues identified—and contributed to friction between the businesses and risk.

Connecting the measurement of operational risks and controls to the business-process level ensures that the organization captures the origin of a particular risk exposure and provides a starting point for scoping and prioritizing risk mitigation. For example, a credit-card issuer had identified more than 250 risks across about 70 level-one and level-two processes. By mapping the risks directly to the processes and quantifying their exposures, mitigation actions in six process areas were prioritized, accounting for the bulk of the risk exposure.

Scenario analysis should not only be used to quantify the frequency and severity of operational risks; it should also be an important component in ensuring the comprehensive identification of operational risks. Scenarios should be based on prior internal and external events, as well as on hypothetical stress-test scenarios. The most advanced financial institutions explicitly measure the impact of their control environment as part of their scenario analyses and use the results of the stress test to make changes to business practices and risk-mitigation efforts.

Furthermore, the risk- and control-assessment data and information must be aggregated to create a comprehensive view of operational risks across the organization and tailored to support the required management decisions on the prioritization of risk and mitigation programs. The vast amount of operational risk-assessment data makes aggregation a challenge that is not trivial. To be successful, institutions must ensure consistency in how assessments are performed, as well as in the criteria for how information is aggregated; additionally, they should be able to drill down on specific capabilities-related issues discussed in aggregated reports.

Fourth, the mitigation processes themselves are obviously a central component of sound ORM. Institutions should move beyond standard operational risk tools to develop front-to-back risk-reducing programs tailored to their processes and systems. Mitigation involves both a priori and ex-post mitigation. A priori mitigation levers may include pursuing policy changes, making strategic changes to products or businesses (including customer segments and geographies), improving business practices and processes, conducting training and risk-culture transformation programs, strengthening or adding controls, and increasing the quality of talent. A priori mitigation relies on consistent processes that assess the impact of mitigation against its costs to ensure that the activities provide net value. While this may sound obvious, the negative “noise” (and the career risk) that surrounds operational failures often contributes to a “zero tolerance” atmosphere, where mitigation costs can exceed associated risks in some areas. In one situation, we saw a financial institution design an extremely detailed and effective (but somewhat cumbersome) risk-assessment program that was applied to all vendors—even to those that posed only a negligible risk to the institution.

In our experience, ex-post mitigation, or the ability to quickly respond to operational risk events, can be as important as, or more important than, a priori mitigation. Scenario analysis can play an important role in designing ex-post mitigation plans because it allows the organization to develop appropriate responses to significant operational risk incidents. In particular, scenario analysis can highlight process areas in which detection of a failure may significantly lag the failure itself.

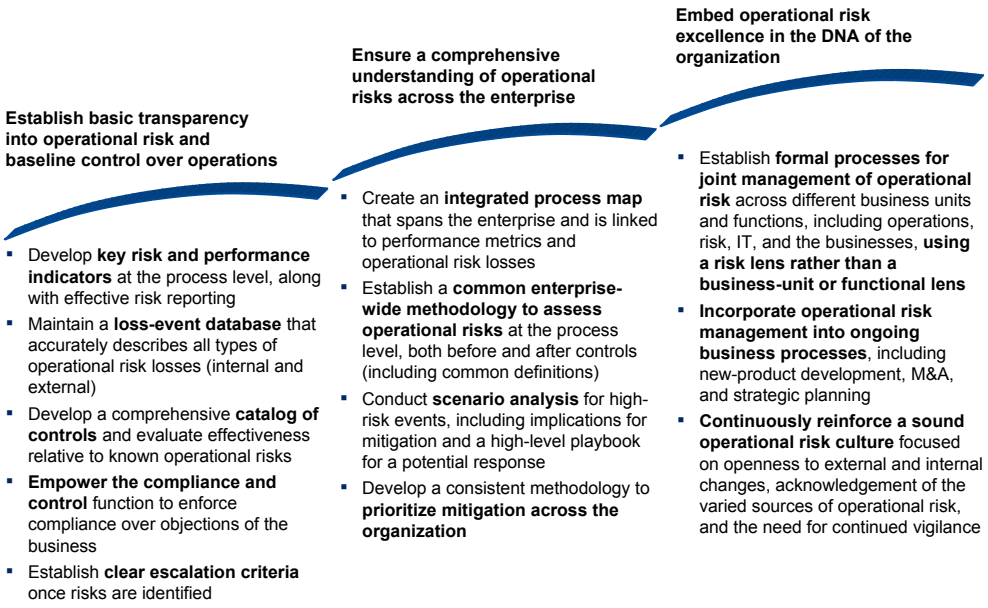
Finally, an important set of enablers is required for effective ORM. Organizations must ensure there is a common language for operational risk and controls, codified in risk policies and taxonomies, and design appropriate systems and technology support. While seemingly straightforward, using a common language throughout the enterprise to describe business processes, operational risks, and controls can help ensure the organization has consistent approaches for risk assessment, aggregation, and mitigation.

Ensuring a successful operational risk transformation

In addition to focusing on all the elements that make up good ORM, financial institutions can set themselves up for success by adhering to sound principles for organizational transformation.

In our experience, financial institutions are more likely to succeed in transforming ORM if the transformation involves all stakeholders and is essentially a joint venture between operations and risk. Ideally, operations and the businesses should lead the initiative as the first line of defense, with risk as an active and involved stakeholder. In one case, the chief operating officer of a major investment bank played a hands-on role in facilitating a comprehensive and consistent firm-wide approach for ORM by bringing all relevant stakeholders together and arbitrating in cases where opinions diverged.

Exhibit 4 The journey to excellence in managing operational risk includes three stages.



Furthermore, the transformation effort should be structured as an iterative process with clear milestones. Throughout the process, the proposed operational risk enhancements are designed, syndicated, and refined; changes are periodically assessed to make sure decisions and implementation approaches are sound. Exhibit 4 describes a typical journey involving the implementation of enhancements in a staged fashion.

Finally, it is essential to maintain strong internal and external communication—including communication with regulators and other external stakeholders—throughout the process and after the transformation to ensure short- and long-term buy-in.

Financial institutions can no longer afford to rely on a business-as-usual approach to managing operational risk. A number of factors, including the increasing size and scope of activities, the increasing operational complexity of large financial institutions, multiple large operational risk losses in the recent past, and a more assertive regulatory posture have increased the importance of ORM. By approaching it in a structured and comprehensive way, financial institutions can realize significant financial impact and benefit from an improved reputation with external stakeholders, including customers, investors, and regulators.

Benjamin Ellis and **Alexis Krivkovich** are principals in the San Francisco office. **Ida Kristensen** and **Himanshu P. Singh** are associate principals in the New York office.

Contact for distribution: Francine Martin
Phone: +1 (514) 939-6940
E-mail: Francine_Martin@mckinsey.com

McKinsey Working Papers on Risk

1. **The risk revolution**
   Kevin Buehler, Andrew Freeman, and Ron Hulme
2. **Making risk management a value-added function in the boardroom**
   Gunnar Pritsch and André Brodeur
3. **Incorporating risk and flexibility in manufacturing footprint decisions**
   Martin Pergler, Eric Lamarre, and Gregory Vainberg
4. **Liquidity: Managing an undervalued resource in banking after the crisis of 2007–08**
   Alberto Alvarez, Claudio Fabiani, Andrew Freeman, Matthias Hauser, Thomas Poppensieker, and Anthony Santomero
5. **Turning risk management into a true competitive advantage: Lessons from the recent crisis**
   Gunnar Pritsch, Andrew Freeman, and Uwe Stegemann
6. **Probabilistic modeling as an exploratory decision-making tool**
   Martin Pergler and Andrew Freeman
7. **Option games: Filling the hole in the valuation toolkit for strategic investment**
   Nelson Ferreira, Jayanti Kar, and Lenos Trigeorgis
8. **Shaping strategy in a highly uncertain macroeconomic environment**
   Natalie Davis, Stephan Görner, and Ezra Greenberg
9. **Upgrading your risk assessment for uncertain times**
   Martin Pergler and Eric Lamarre
10. **Responding to the variable annuity crisis**
    Dinesh Chopra, Onur Erzan, Guillaume de Gantes, Leo Grepin, and Chad Slawner
11. **Best practices for estimating credit economic capital**
    Tobias Baer, Venkata Krishna Kishore, and Akbar N. Sheriff
12. **Bad banks: Finding the right exit from the financial crisis**
    Luca Martini, Uwe Stegemann, Eckart Windhagen, Matthias Heuser, Sebastian Schneider, Thomas Poppensieker, Martin Fest, and Gabriel Brennan
13. **Developing a post-crisis funding strategy for banks**
    Arno Gerken, Matthias Heuser, and Thomas Kuhnt
14. **The National Credit Bureau: A key enabler of financial infrastructure and lending in developing economies**
    Tobias Baer, Massimo Carassinu, Andrea Del Miglio, Claudio Fabiani, and Edoardo Ginevra
15. **Capital ratios and financial distress: Lessons from the crisis**
    Kevin Buehler, Christopher Mazingo, and Hamid Samandari
16. **Taking control of organizational risk culture**
    Eric Lamarre, Cindy Levy, and James Twining
17. **After black swans and red ink: How institutional investors can rethink risk management**
    Leo Grepin, Jonathan Tétrault, and Greg Vainberg
18. **A board perspective on enterprise risk management**
    André Brodeur, Kevin Buehler, Michael Patsalos-Fox, and Martin Pergler
19. **Variable annuities in Europe after the crisis: Blockbuster or niche product?**
    Lukas Junker and Sirus Ramezani
20. **Getting to grips with counterparty risk**
    Nils Beier, Holger Harreis, Thomas Poppensieker, Dirk Sojka, and Mario Thaten

McKinsey Working Papers on Risk

21. **Credit underwriting after the crisis**
Daniel Becker, Holger Harreis, Stefano E. Manzonetto, Marco Piccitto, and Michal Skalsky

22. **Top-down ERM: A pragmatic approach to manage risk from the C-suite**
André Brodeur and Martin Pergler

23. **Getting risk ownership right**
Arno Gerken, Nils Hoffmann, Andreas Kremer, Uwe Stegemann, and Gabriele Vigo

24. **The use of economic capital in performance management for banks: A perspective**
Tobias Baer, Amit Mehta, and Hamid Samandari

25. **Assessing and addressing the implications of new financial regulations for the US banking industry**
Del Anderson, Kevin Buehler, Rob Ceske, Benjamin Ellis, Hamid Samandari, and Greg Wilson

26. **Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation**
Philipp Härle, Erik Lüders, Theo Pepanides, Sonja Pfetsch, Thomas Poppensieker, and Uwe Stegemann

27. **Mastering ICAAP: Achieving excellence in the new world of scarce capital**
Sonja Pfetsch, Thomas Poppensieker, Sebastian Schneider, and Diana Serova

28. **Strengthening risk management in the US public sector**
Stephan Braig, Biniam Gebre, and Andrew Sellgren

29. **Day of reckoning? New regulation and its impact on capital markets businesses**
Markus Böhme, Daniele Chiarella, Philipp Härle, Max Neukirchen, Thomas Poppensieker, and Anke Raufuss

30. **New credit-risk models for the unbanked**
Tobias Baer, Tony Goland, and Robert Schiff

31. **Good riddance: Excellence in managing wind-down portfolios**
Sameer Aggarwal, Keiichi Aritomo, Gabriel Brenna, Joyce Clark, Frank Guse, and Philipp Härle

32. **Managing market risk: Today and tomorrow**
Amit Mehta, Max Neukirchen, Sonja Pfetsch, and Thomas Poppensieker

33. **Compliance and Control 2.0: Unlocking potential through compliance and quality-control activities**
Stephane Alberth, Bernhard Babel, Daniel Becker, Georg Kaltenbrunner, Thomas Poppensieker, Sebastian Schneider, and Uwe Stegemann

34. **Driving value from postcrisis operational risk management : A new model for financial institutions**
Benjamin Ellis, Ida Kristensen, Alexis Krivkovich, and Himanshu P. Singh

McKinsey Working Papers on Risk
June 2012
Designed by Editorial Shared Services design team

www.mckinsey.com