McKinsey&Company

McKinsey Working Papers on Risk, Number 46


Managing third-party risk in a changing regulatory environment

Dmitry Krivin
Hamid Samandari
John Walsh
Emily Yueh

May 2013

Contents

Managing third-party risk in a changing regulatory environment

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).

Managing third-party risk in a changing regulatory environment

The rising tide of regulatory scrutiny stemming from the 2008 financial crisis has now reached beyond banks to the companies that supply them. Under the broad notion that activities can be outsourced, but responsibility cannot, the Consumer Finance Protection Bureau (CFPB) and other regulators are holding financial institutions responsible not only for their own actions, but for those of their vendors and suppliers. Thus, in the past nine months, Capital One, Discover Card and American Express have paid a total of $525 million to settle complaints of deceptive selling and predatory behavior by their third-party suppliers.

Through these actions, and others, the nature of the due diligence firms are required to conduct is expanding well beyond the traditional assessments for supplier, operational, and IT security risks. The rules have not changed entirely, but the emphasis has. Regulators are sensitive to other risks, such as strategic and reputational risks, that even smaller third parties can create for customers, and are critical of firms' processes for monitoring these risks.

This new regulatory thrust poses a big challenge for financial institutions, which typically have more than 20,000 suppliers. Worse, firms often have only a limited understanding of the ways that suppliers interact with customers. But as they must bear the costs of suppliers' misdeeds, financial institutions now have a strong incentive to broaden and deepen the way they manage these relationships. And there is also a business case for doing so: effective third-party management is a mainstay of good operational health and cost management. We have found that the current state of the art requires firms to develop or improve along the following six elements:

- **A comprehensive inventory of all third parties with whom the firm has a relationship.** Many firms find it difficult to build this list; enterprise-wide surveys and data algorithms to reconcile data are effective tools that can help.

- **A comprehensive catalog of specific customer risks to which third parties can expose the firm.** Many institutions don't fully understand all the risks their third parties run. A master risk register, tied to the issues that the CFPB is actively pursuing, can help track them down.

- **A risk-based segmentation of the supplier base.** Not all suppliers carry the same amount of risk. Firms need to better triage their suppliers to make sure the most effort is devoted to the highest risks.

- **Rules-based due diligence testing.** Treating every supplier the same doesn't make sense. Carefully designed rules can help firms focus their investigation of suppliers.

- **A disciplined governance and escalation framework.** At many firms, third-party risk management does not have a natural owner. Establishing one and giving that group the right decision-making powers is essential.

- **Integrated technology and MIS workflow process and tools.** Adapting current risk IT applications to third-party management is tricky, and building a new one is even harder. A purpose-built off-the-shelf application is the right answer for many.

Firms that have successfully built these six elements are finding that the work is yielding the expected benefits of lower risk costs. Just as important, they say, is the advantage of being able to present a coherent approach to all the key stakeholders.

The heightened emphasis on consumer protection

Protection of consumers' interests dates back at least to 1968 and the Truth in Lending Act (Reg Z). But in the past decade, and especially since the 2008-09 financial crisis, all the major financial regulators including the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, have taken a keener interest than ever in guarding the financial consumer from the risk of predatory behavior by third parties contracted by banks and other financial institutions. The Dodd-Frank Wall Street Reform and Consumer Protection Act created the Consumer Financial Protection Bureau, an agency charged with just this kind of protection. In another example, in 2012, the National Mortgage Settlement issued $25 billion in fines and other actions against five leading mortgage servicers, in part for missteps by their suppliers, such as foreclosure law firms.

A primary theme of the CFPB's work to date is that while banks and other financial institutions can outsource activities, they cannot outsource the responsibility of consumer protection to their third parties. Since its inception, the CFPB has logged more than 79,200 consumer complaints covering 33 types of issues. Mortgage and credit card companies have generated most of the complaints, 45 percent and 29 percent respectively. In its first public enforcement case, the CFPB fined Capital One $210 million to settle charges of deceptive marketing practices on the part of some of the company's third-party suppliers. Soon after, Discover Card settled similar charges for similar amounts, and American Express agreed to pay $112 million to settle a CFPB action.

Exhibit 1 The bar on third party management has been significantly raised.

		Traditional programs	Best in class programs based on recent regulatory requirements
Scope		▪ Focused on vendors and managed as a part of the procurement process	▪ Broader scope to include all third parties (e.g., including co-brand partners, joint ventures, fee-based or add-on services)
Management approach	**Segmentation**	▪ Primarily based on vendor size resulting in lack of appropriate oversight for some high risk smaller vendors (e.g., foreclosure law firms)	▪ Risk based segmentation, driven by the nature of risk the third party poses to the bank, with suitable controls to address the risk
	Rules-based due diligence	▪ Primarily focused on financial assessment, business continuity and information security	▪ Includes assessment of compliance to regulations that govern the activity performed by vendor
	Post-contract compliance management	▪ Audit activities/ questions not focused on vendor specific risks ▪ Scorecards primarily focused on performance indicators ▪ Some systematic tracking or reporting of third party-related complaints	▪ Audit questions and materials based on key breakpoints for that third party ▪ Supplemented with compliance and QC metrics to ensure monitoring of risks in addition to performance ▪ End-to-end process to capture, track and report complaints is put in place
	Governance/ escalations	▪ Owned by the Business or vendor management ▪ Decisions made typically by vendor management and/ or business, with limited oversight ▪ Process for third party related incidents not clearly defined which resulted in inconsistent/ inadequate escalation of incidents	▪ Involvement of independent teams (e.g., compliance) in oversight activities ▪ Decisioning by senior cross functional team including representatives from Legal, Compliance, Risk and Business ▪ Detailed of escalating incidents to ensure transparency on emerging risks and executive involvement where necessary
	Technology and tools	▪ Focused primarily on tracking third party **production** performance data, with limited / no ability to track in real-time **risk** performance data ▪ Limited / No enterprise-wide workflow management tools to ensure consistent risk management ownership across BUs	▪ Comprehensive source of third party performance and risk based data with clear records of risk management owners across BUs

Caught on the back foot

Our work and experience suggest that many financial institutions are under-prepared for the organizational and tactical implications of this regulatory change. Most firms' vendor management programs have focused predominantly on risks such as business continuity, financial strength, and credit risk. The scope of regulatory oversight has broadened, to include not just these risks to the bank and the financial system, but also to consumers (Exhibit 1).

Those risks are obscured partly by the sheer size of the supply chain. At the nation's biggest banks and credit card companies, the list of third parties typically runs to more than 20,000 names; some firms might have 50,000 suppliers. Firms are quite careful about some of these relationships, especially with large and mid-size suppliers; they often have dedicated teams to manage the most complex relationships. And it is true that many of these vendors provide paper, computers, and other innocuous goods and services. But many relationships are not closely managed, and some carry hidden risks. The company that molds and prints credit cards, for example, is also entrusted with customer data, which poses any number of privacy and security risks.

Compounding the problem is the changing nature of third-party relationships. In today's marketplace for consumer financial services, most firms have signed agreements with marketing partners, co-branding partners, fee-based service providers, and others, to gain access to assets and capabilities. These are complex arrangements in which risk-sharing is sometimes poorly specified, and some risks are unaddressed.

In the face of these changes, the approaches that many firms use to manage third parties are proving insufficient, as they tend to focus on metrics of supplier performance. For example, in contracts with collection agencies, firms monitor call volumes and amounts recovered, and usually do not consider risk metrics such as the number of customer complaints or the level of potential reputational risk to the firm.

Excellence in third-party risk management

As a result, some leading banks and credit card companies are developing and embracing several best practices that together form a comprehensive approach to third-party risk management. Based on our work, we see six critical components to such a program. Many of these elements can be built in parallel.

A comprehensive inventory of third parties

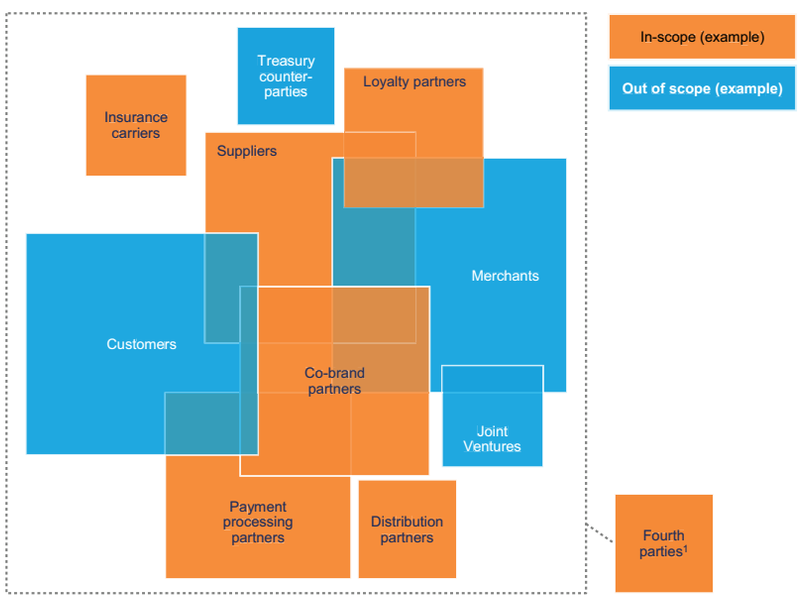
Collating an exhaustive list of third parties is a big undertaking. Risks cannot be assessed and mitigated until they are found, but most financial institutions have tens of thousands of supplier relationships. Regulators are expecting institutions to have an understanding of who their third parties are, as well as a detailed understanding how each third party interacts with the consumer and the activities it performs.

Most firms don't have the information needed. Supplier databases are incomplete, and some of the most sensitive risks often turn out to reside in some relationships that are not found in supplier databases. Co-branded partnership, joint ventures, sponsorships, and other similar relationships can comprise up to 80 percent of the spending that some business units assign to suppliers. But these relationships are often managed in ways that emphasize commercial goals, with only a secondary focus on risk.

Even where suppliers are known, many organizations lack fundamental information on the risks these companies run. There are few if any reliable sources of information on fraud allegations and convictions among small businesses, for example. Sometimes different business units track their suppliers in different ways, leading to difficulties of comparison and collation across the enterprise. Our experience suggests that best-in-class third-party databases include coverage of all third parties, defined as any non-customer entity with whom the financial institution engages in a business relationship (Exhibit 2). An enterprise-wide survey is a good way to get started. An effective algorithm for collating and reconciling businesses' various data models can help speed the task, and reduce the time needed from 9 to 6 months.

Exhibit 2 How regulators define the universe of third parties.

Per the OCC, the term, "third party" includes "all entities that have entered into a business relationship" with the financial institution.



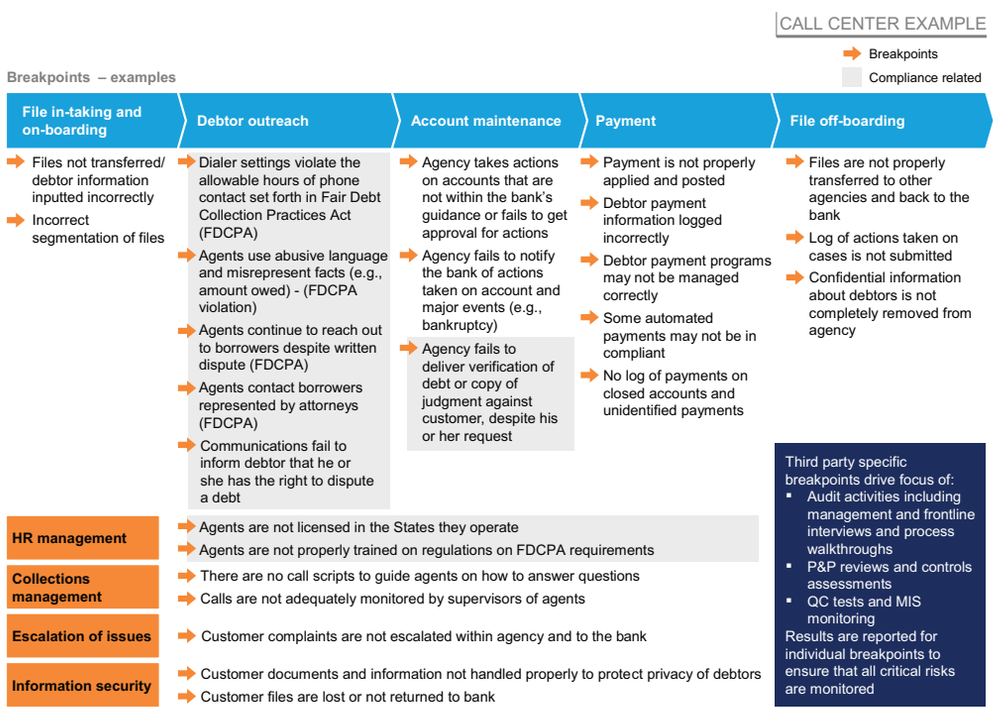
[1] Fourth parties are sub-contractors to third parties (i.e., third parties of third parties)

A comprehensive catalog of third-party risks

Third parties can expose their customers, and their customers' customers, to a wide range of risks. Developing a comprehensive list of these risks and breakpoints is essential for the success of audit routines and the scorecards used to monitor risk. For example, if a third-party call center has a risk of agents misrepresenting product information to customers, the bank will monitor this specific risk in an audit (e.g., through call monitoring) and request regular reports on call quality and customer escalation metrics. (Exhibit 3 shows an example of a detailed breakpoint analysis). Naturally, the inventory of customer risks will vary across categories of suppliers, depending on the nature of the interaction with consumers. Higher risk categories will typically have 20-30 potential risks or "breakpoints."

Financial firms face two challenges in developing the risk catalog: identifying the relevant breakpoints for each category of suppliers, and determining the relative weight and importance of each breakpoint. Our work suggests that a master register of breakpoints and their risk weights in each category is broadly relevant to almost all firms, and can be adapted to the particular circumstances of individual institutions. With the help of the master register, this element can be built in three months. That adaptation is an essential step, as it helps the firm understand the true drivers of its risk, and guides its program of mitigation.

Exhibit 3 Tailoring oversight to third-party specific risks/breakpoints are critical for mitigation of risks—collections agency example.



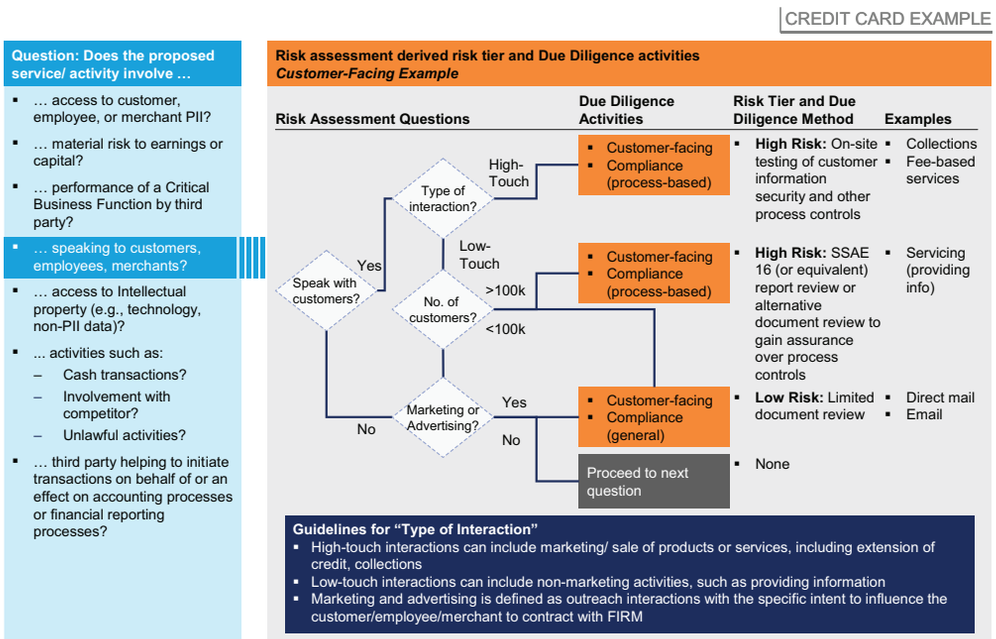
A risk-based segmentation

With a complete inventory of third parties and their relative risks in hand, the firm can then categorize its supplier relationships based on the level of risk to customers. Even a simple system of "high," "medium," and "low" risk categories can be useful. In our experience, most leading institutions have 200 to 300 high-risk relationships at a time, irrespective of the total number of third parties they contract. An effective segmentation helps the firm efficiently allocate resources, by conducting more risk and due diligence activities to higher risk relationships, and conducting routine and potentially automated routine reviews of its lower risk suppliers.

We have seen firms use two approaches to assign their third parties to risk tiers. In the score-based approach, the firm conducts due diligence across all dimensions, and uses the results to develop a composite risk score. While very thorough, the approach can be onerous and resource-intensive for many organizations. In a rules-based approach, the firm defines some rules or criteria tied to breakpoints to streamline the assignment to a risk category. This approach is about 40 to 60 percent faster than a score-based approach, as it entails only the risk assessment and due diligence activities needed (Exhibit 4).

Designing the approach can take 2 to 3 months, and refining it and testing it with business leaders another month or two. Given these requirements, leading institutions invest heavily in getting the design right; typically they identify a core team of risk experts to drive the design, the fine-tuning, and the implementation.

Exhibit 4 A systematic risk assessment process should drive tailored diligence and control.



Rules-based due diligence testing

With the shift in regulatory emphasis, the nature of the due diligence required is becoming increasingly rigorous. Traditional approaches match a set of diligence activities to the level of risk identified by the risk-based segmentation. A supplier in the high-risk category receives the full treatment of all available diligence investigations. As discussed above, this tends to be overly onerous and resource intensive.

Here too the rules-based approach can be a better answer, because it triggers the right set of diligence activities for the risks identified. For example, even if a third party is deemed high risk, if it does not hold customer PII (personal identifiable information), there is no reason to conduct an information security or data privacy screening. We have found that the rules-based approach can save up to 40 percent in time and labor costs.

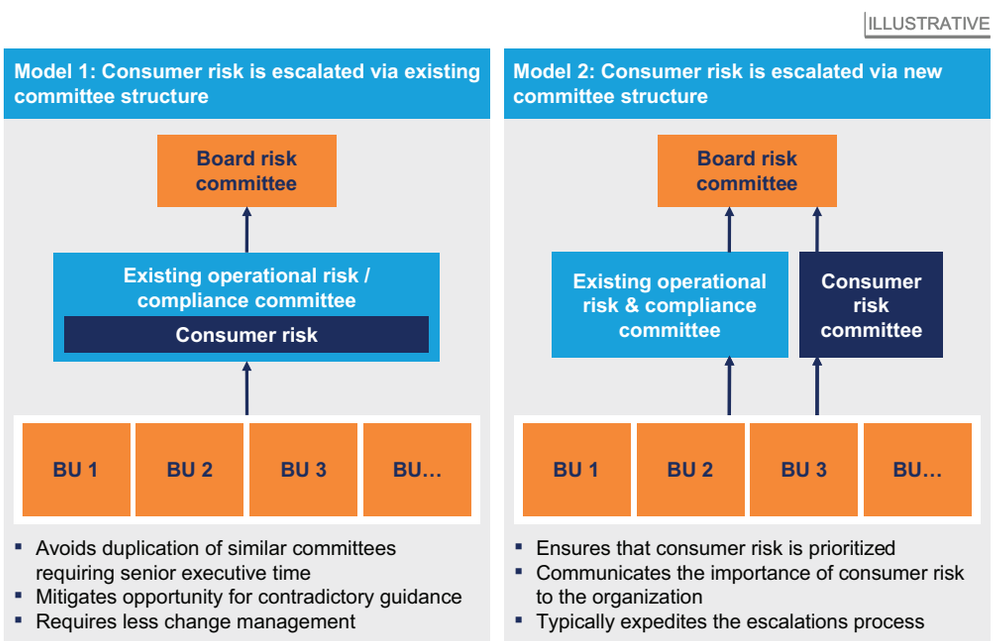
Disciplined governance and escalation process

Creating organizational alignment is particularly important in the new emphasis on broad and deep third-party management, where decision-making rights are spread across businesses and functions such as procurement, compliance, operational risk management, and others. Establishing upfront the structures and processes to address misalignments will enable a timely resolution of challenges when they arise.

Governance can be either centralized or decentralized; both approaches, and some hybrids of the two, can be successful (Exhibit 5). The centralized model, naturally, keeps most major decisions (such as risk "tiering" and due diligence activities) within a single group, such as procurement or a shared services team. While this approach yields a clear and accountable owner, it can sometimes generate tension between the business units that "own" the working relationship with the third party and the centralized body accountable for risk assessments.

A decentralized model lets the business units that own the relationship also manage the risk. This too has its drawbacks; it can sometimes result in duplication of resources (for example, a major third-party supplier

Exhibit 5 Consumer risk can be governed within the existing committee structure or by creating a new committee.



might be assessed by several business units for very similar contracts and relationships). And a decentralized approach can see inconsistent application and misalignment of risk standards between, say, procurement and operational risk. A hybrid approach, carefully tailored to the organizational context, can help mitigate potential challenges of the other two models, but must be monitored closely to ensure lines of risk ownership are not lost.

An escalation framework is needed to resolve disagreements and challenges that exceed the decision-making limits set out in the governance structure (such as requests for exception, and resolution of third-party breach). While most organizations have an operational risk management group, its governance model and mandate might not be sufficient to address the additional volume of third-party issues. In our experience, leading financial institutions are choosing to assign new responsibilities to standing committees rather than create new ones to support third-party escalations. Each organization must find an appropriate approach given its risk appetite and culture.

Designing the governance model and escalation framework can take up to six months; expect to spend another six months to “stand it up” in the organization.

Integrated management reporting and workflow process and tools

Clear, actionable management reports and well-designed workflow systems are essential for accountability across the first line of defense (the business units), as well as the second (compliance) and third (audit). To work well, these tools must track and monitor all the relevant data, of course, but more importantly they must do two other things: aid workflow not just within but across business units; and give managers the right information to get a true picture of risk, in near-real time, and recommendations to act on it. In our experience, most organizations currently have tools that address one or two of these functional needs, but to our knowledge none has a single tool that performs all three functions.

Building a new third-party risk application from scratch is of course a big undertaking; so too is enhancing a current risk tool to do the new jobs. Firms should prepare for the project with a strong, dedicated team, and budget 3 to 6 months. One solution that some firms are using is an off-the-shelf workflow and risk management tool that can be easily customized to the organization's specific needs.

- Do we have a single repository of all third parties (including traditional suppliers such as IT call centers, co-brand partners, fee-based services, joint venture partners, distribution partners)? If not, what will it take to build one?

- Do we have an inventory of due diligence tests? Are they clearly defined, with owners for each of due diligence tests, and with adequate training for the associates performing the test?

- Are the processes and standards consistent across BUs? Is there a robust governance and escalation framework?

- Do we have an effective risk-based segmentation (e.g., are small collection agencies appropriately categorized as high risk)?

- Do we actively monitor third parties for compliance to regulations that govern their activities? For example, do we audit calls made by call centers, review their internal policies, audit their operations to ensure adherence to letter and spirit of regulations? Do we have decent workflow tools to help with this?

- Do we have adequate documentation and an up-to-date narrative to demonstrate progress to the regulators?

The answers to these questions will determine the nature, length and required resources for the transformation.

John Walsh is a senior adviser to McKinsey & Company in the Washington, DC, office and former head of the OCC. **Hamid Samandari** is a director, **Dmitry Krivin** is an associate principal, and **Emily Yueh** is an engagement manager, all in McKinsey's 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**
   André Brodeur and Gunnar Pritsch
3. **Incorporating risk and flexibility in manufacturing footprint decisions**
   Eric Lamarre, Martin Pergler, 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**
   Andrew Freeman, Gunnar Pritsch, and Uwe Stegemann
6. **Probabilistic modeling as an exploratory decision-making tool**
   Andrew Freeman and Martin Pergler
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**
   Eric Lamarre and Martin Pergler
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**
    Gabriel Brennan, Martin Fest, Matthias Heuser, Luca Martini, Thomas Poppensieker, Sebastian Schneider, Uwe Stegemann, and Eckart Windhagen
13. **Developing a postcrisis 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
21. **Credit underwriting after the crisis**
    Daniel Becker, Holger Harreis, Stefano E. Manzonetto, Marco Piccitto, and Michal Skalsky

McKinsey Working Papers on Risk

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

35. **So many stress tests, so little insight: How to connect the 'engine room' to the boardroom**
Miklos Dietz, Cindy Levy, Ernestos Panayiotou, Theodore Pepanides, Aleksander Petrov, Konrad Richter, and Uwe Stegemann

36. **Day of reckoning for European retail banking**
Dina Chumakova, Miklos Dietz, Tamas Giorgadse, Daniela Gius, Philipp Härle, and Erik Lüders

37. **First-mover matters: Building credit monitoring for competitive advantage**
Bernhard Babel, Georg Kaltenbrunner, Silja Kinnebrock, Luca Pancaldi, Konrad Richter, and Sebastian Schneider

38. **Capital management: Banking's new imperative**
Bernhard Babel, Daniela Gius, Alexander Gräwert, Erik Lüders, Alfonso Natale, Björn Nilsson, and Sebastian Schneider

39. **Commodity trading at a strategic crossroad**
Jan Ascher, Paul Laszlo, and Guillaume Quiviger

40. **Enterprise risk management: What's different in the corporate world and why**
Martin Pergler

41. **Between deluge and drought: The divided future of European bank-funding markets**
Arno Gerken, Frank Guse, Matthias Heuser, Davide Monguzzi, Olivier Plantefeve, and Thomas Poppensieker

42. **Risk-based resource allocation: Focusing regulatory and enforcement efforts where they are needed the most**
Diana Farrell, Biniam Gebre, Claudia Hudspeth, and Andrew Sellgren

43. **Getting to ERM: A road map for banks and other financial institutions**
Rob McNish, Andreas Schlosser, Francesco Selandari, Uwe Stegemann, and Joyce Vorholt

44. **Concrete steps for CFOs to improve strategic risk management**
Wilson Liu and Martin Pergler

45. **Between deluge and drought: Liquidity and funding for Asian banks**
Alberto Alvarez, Nidhi Bhardwaj, Frank Guse, Andreas Kremer, Alok Kshirsagar, Erik Lüders, Uwe Stegemann, and Naveen Tahilyani

46. **Managing third-party risk in a changing regulatory environment**
Dmitry Krivin, Hamid Samandari, John Walsh, and Emily Yueh

McKinsey Working Papers on Risk
May 2013
Designed by Global Editorial Services

www.mckinsey.com