McKinsey on Corporate & Investment Banking

Number 2, July 2006

McKinsey&Company

Better **operational-risk** management for banks

Operational risks are costly, but they can be conquered when high-ranking executives join the battle.

Cindy B. Levy, Hamid Samandari, and Antonio P. Simoes

Consider the trader who receives an urgent request from an unknown counterparty to enter into a sizable currency or derivatives transaction with the trader's bank. Surprisingly, the counterparty is unconcerned about price. But the deal is potentially lucrative, and no one appears to be breaking the law.

Does the trader pause, referring his or her suspicions upward, or proceed with the deal, brushing aside doubts that the counterparty may have something to hide and that the deal could well be tainted? The answer may depend on the effectiveness of the bank's operational-risk-management procedures.

This area of risk management is one that many financial players now recognize must be reviewed and perhaps radically reassessed, despite their increased spending to comply with new regulations such as Sarbanes-Oxley and Basel II. In recent years, losses incurred as a result of improper business practices, failed processes, and other operational risks have mushroomed across a range of industry sectors, including pharmaceuticals, oil and gas, and financial services. From 2001 to 2005, risk-related losses in financial services at the top 12 US banks represented 4 to 5 percent of their net income—and considerably more if unpublicized events are added to the total. In 2005 at least two large banks had operational losses that wiped out more than 10 percent of their pretax net income.

Risk management, to be sure, is a game of big numbers. Losses can be as enduring as they are large. What's more, the impact of such losses on shareholder value can be disproportionately severe. In our analysis of 350 large risk events at European and North American financial institutions since 1990, the decline in market capitalization of the institutions affected was roughly equal, in the short term, to the financial loss. But after 120 days, the decline was, on average, roughly 12 times the reported loss. The most harmful crises involved embezzlement, loan fraud, deceptive sales practices, antitrust violations, and noncompliance with industry regulations.[1]

Successful risk management is not just about limiting the downside, however. Banks with robust approaches to managing

[1] Robert S. Dunnett, Cindy B. Levy, and Antonio P. Simoes, "Managing operational risk in banking," *The McKinsey Quarterly*, 2005 Number 1, pp. 21–4 (www.mckinseyquarterly.com/links/22150).

operational risk can often take on and succeed in businesses that others are unable or unwilling to accept. Some banks, for example, created the appropriate level of separation for the prime brokerage business more swiftly than others did and could therefore scale up more aggressively. Players that added operational-risk skills and capacity in the credit derivatives back office have managed to pursue the most structured and most lucrative trades. Moreover, banks that need to hold regulatory capital against operational risk can free up funds for their investments by reducing their risk-related losses. Banks with better operational-risk practices also will enjoy improved market sentiment and, ultimately higher share prices (all other things being equal).

In our work with banks, we find that their operational-risk infrastructure remains overly focused on measuring risk rather than mitigating it. Procedures for wrestling with potentially risky business practices are rarely in place and, where they do exist, are rarely systematic. "Soft," qualitative issues such as front-office culture and the concerns of key external stakeholders are typically overlooked. Complacency at the business unit level—a consequence of the centralization of risk functions and the feeling that "it's someone else's job"—frequently goes uncorrected.

Old methods no longer work

Managing risk—which comes in many varieties, including not only operational and reputational risk but also market, credit, and regulatory risk—is inherent in almost everything banks do, from controlling inventory levels to developing new products to managing loan portfolios. Bank executives must understand that operational risk is inextricably and increasingly linked to the reputations of companies. Its management directly influences their actions and thus their reputation among stakeholders.

More specifically, operational risk is the risk of loss stemming from the inadequacy or failure of internal processes, people, and systems or from external events such as conspiracies. Reputational risk derives from the stakeholders' perceptions of companies and of their employees' behavior. It is the risk that this intangible asset will lose value and cause future financial losses—for instance, if employee turnover increases or regulators intensify their oversight of the company.

With that understanding, executives need to review and challenge some long-standing and deeply held assumptions about how to control and manage these risks. The use of traditional methods of measurement and historical data may, for example, be an effective way to manage credit or market risk, but operational risk is far less predictable, because past events give much less guidance about future ones.

Another cause of difficulty is the centralized risk function found in many banks. Centralized risk teams may be desirable for monitoring and managing regulatory developments that affect an entire bank, but these teams on their own lack the sort of insights that let managers respond quickly to changing needs.

Some companies have started to address individual areas, but piecemeal strategies can prove downright dangerous if they overlook important risks. Banks should simultaneously address business practices in the front office, the risks

that may be festering in operations, and the organizational structures that most readily guarantee consistency, reliability, and universal adherence. In addition, banks need to engage with their external stakeholders more intensively than they used to do, by understanding and shaping those stakeholders' perceptions and constantly adjusting their own risk mitigation priorities in response.

A tight grip on business practices

Let's start with business practices, keeping in mind the trader's dilemma set out at the beginning of this article. In our experience, banks need to focus on three areas: new risks, the routine business practices that permeate companies, and the culture that surrounds these practices.

Identify and deal with new risks

In most industries, and not least in banking, companies that face changing market conditions, new regulatory requirements, and intensifying competitive pressures must adjust their business practices quickly and robustly. What may seem, in isolation, like minor modifications to an operating environment can quickly assume substantial proportions.

Too often management fails to detect or act on new types of risk. Take the fast-growing global bank that put more than 300 new products onto its back-office platform in a single year. So many changes occurred so fast that senior leaders lacked a shared understanding of the client disclosure requirements in some of their highest-growth businesses. Instead of following a standardized approach, hundreds of midlevel traders had to exercise individual discretion, thereby exposing the bank to unnecessary risk.

In the context of new risks, a crucial challenge for senior management is recognizing the limitations of inexperienced, junior employees and rectifying their shortcomings. This effort might involve stopping an activity or practice to keep frontline employees out of harm's way, training or coaching them to cope with specific shady situations (such as the overhasty counterparty), providing tools to help them identify and deal with such situations, and creating policies that clarify what is and isn't acceptable.

In our trader's case, the bank's management should already have recognized and prepared for this sort of day-to-day dilemma by reassessing its priorities and giving itself sufficient time to understand the threats and prepare ways of dealing with them. A training program would highlight warning signs (such as sudden price insensitivity by counterparties) and instill in traders a willingness to avoid such deals or to refer them upward. Effective tools—for example, a structured set of what-if questions that trigger concerns about possibly shady deals—could be developed to identify gray areas and flag problem deals.

Constantly evaluate principles and practices

In other cases, a company's routine business practices may be flawed. The trader in the example of the suspect deal may lack experience because the bank has no procedures to ensure adequate training. Alternatively, the bank's incentive scheme may reward traders only for turning a profit, not for alerting management to dubious deals. Or any sanctions may be insufficient, so that even if the trader is fired, he or she will leave with reputation intact and easily find a job elsewhere. Management must review its practices

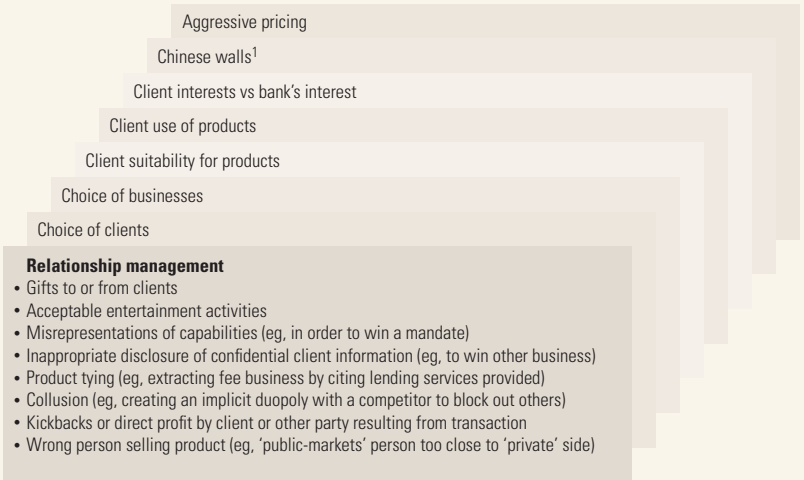
regularly and unearth such issues; it needs to create an environment that does not tolerate poor judgment on matters of operational and reputational risk.

In particular, banks need to recognize changes in their product or client mix, such as a sudden increase in the level of traded products marketed to retail customers. Other retail businesses can offer some lessons. A credit card issuer, for example, provoked outrage among consumers when it recklessly migrated customers from one product to another without persuading them of the benefits. The issuer responded to the outcry by establishing a clear taxonomy of current business practices (Exhibit 1) and highlighting those that seemed to present the greatest operational and reputational risk. It then investigated these practices in an effort to understand the risk–reward trade-offs more fully and made clear decisions about which practices to modify, and how.

EXHIBIT 1

A taxonomy of risky business

Selected business practice areas



[1]Control of information within certain parts of a company to prevent conflicts of interest.

Tackle the cultural root causes

Even if a bank does have the appropriate control, mitigation, and managerial backstops in place, its culture may not support them. Danger signs include a tendency to say one thing but do another or to measure power and status only by income generated, despite bank policies that urge employees to forgo income that would involve excessive operational risk.

Only by pursuing a combined approach to business practices and culture will banks eradicate these issues. The first step is conducting regular surveys to understand how the existing culture affects the behavior of the staff. Institutions should then take steps to ensure that employees fully understand what is expected of them, to install sound role models, and to introduce appropriate evaluation and compensation schemes. (Banks should, for example, keep records of deals refused because of the operational risk they posed and factor an operational-risk performance metric into individual rewards.)

Getting a grip on practices and culture is no one-off exercise but a continuing effort. To root out the real causes of risky practices, managers need to be alert, inquisitive, and skeptical. If employees are just operating by the book, it's time to change the book. Managers must be prepared to lead by example, to change the behavior of other employees, and to set and enforce new policies—applying tough sanctions if necessary.

Taking the risk out of operations

Most companies have already removed most excess costs from their operations, apparently leaving little scope for further gains. The next frontier involves eliminating

unnecessary operational risks from seemingly efficient back offices.

Our recent experience suggests that the savings achieved in some processes by reducing error rates (in other words, losses from operational risk) can far outweigh the savings achieved through traditional cost reduction measures. We suspect that the same thing will hold true in many cost-focused operations. Companies need to create a methodology that simultaneously tackles costs and operational risk, trading them off against each other where necessary.

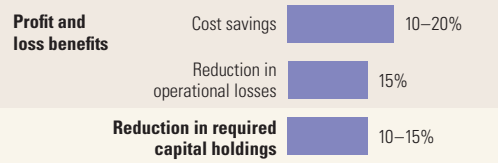
A single stream of initiatives can help banks enjoy the double benefit of reducing operational risk and cutting costs. One leading bank fortified its combined lean–Six Sigma methodology with measures to reduce operational risk. The bank found that the factors pushing up costs—waste, inflexibility, and variability—often trigger risk-related losses too.

In pursuing lean or Six Sigma process improvements (or both) that include a risk mitigation objective, experts may be nominated to serve as evangelists, disseminating new risk-aware working practices across the operating platform. One leading European wholesale bank made such evangelists the cornerstone of a two-year rollout of new products. In pilots at this bank, the savings from lower costs and reduced losses came to $60 million thanks to a smaller number of errors in the back office. Moreover, the bank holds capital against its operational risk, as mandated by the Basel II accord, so the program has led to a corresponding reduction in its regulatory-capital requirements (Exhibit 2). This result can be a strong motivator for change, but companies must realize that

EXHIBIT 2

Set it free

For disguised wholesale bank



capital release often has a significant time lag and that capital held to cover credit risk tends to dwarf any capital set aside for operational risk.

Such programs also carry symbolic weight: companies that are less tolerant of their small risks are better able to control larger and less frequent ones because they create a culture of risk awareness across the organization.

Getting the organization right

Embedding risk consciousness in every aspect of a bank's business has major organizational implications. An integrated approach means that controlling operational and reputational risk is no longer the preserve of a few special functions but becomes an active pursuit for *all* senior managers, including those who oversee compliance, audit, risk, investor relations, regulatory management, communications, and—above all—business and operations. While many companies claim that the business serves as the first line of defense, few organize themselves so that it actually does.

In our experience, banks must assign responsibility clearly to business and operations managers. Also, an appropriate role should be found for those who are formally charged with risk functions.

Management structures and responsibilities

To boost motivation and accountability, banks should assign clear responsibility for operational and reputational risk to individual business and operations managers, ensuring that they have the right skills and support to fulfill their charge. In one securities back office, the responsibility for reducing the number of failed trade confirmations was split among several managers, so no one took full ownership. Risk avoidance must be specifically written into the performance criteria and incentives of operational leaders—a difficult challenge, since lowering the level of risk in an environment seldom immediately reduces the number or size of short-term losses. Banks and other financial institutions should reward risk mitigation efforts either by providing capital relief or by implementing a charging mechanism for expected losses; the mechanism can be relaxed after action has been taken to mitigate a problem.

The role of the risk and control functions

With frontline managers and staff now occupying the first line of defense, what about the bank's traditional risk and compliance functions? We have identified four different models they can adopt within the broader organization:

1. *Full-service provider.* In this model the in-house operational-risk team has the expertise to deal with all risk-related issues. The wholesale adoption of this approach probably isn't practical, as it requires a very large risk function. However, it may be feasible to approach individual topics such as risk modeling in this way.

2. *Joint venture partner.* Operational-risk professionals and business teams share the same workspace and report jointly on specific projects. An example might be a program to improve product design and simultaneously reduce the level of operational risk inherent in the production process.

3. *Adviser.* The operational-risk team offers its expertise to specific parts of the business. The risk function could, for example, build a cadre of experts to drive down the level of risk in a number of operations. This approach was taken by the previously mentioned European bank, which loaned risk managers from a central group to the businesses, where they helped implement a lean program, returning to the center once it was complete. Another possibility might be to give middle managers expert training in the risk implications of business practices.

4. *Devolved entity.* Operational-risk professionals are fully integrated into the business units and have a permanent dual reporting line—to the manager of the business unit and to their own functional manager. They may also carry other responsibilities within the business and function, subject to the requirements of the bank's regulator.

Different models will be appropriate for different banks, according to their starting position: size, complexity, risk exposure, risk culture, and the credibility of the risk and control functions. Whatever model a bank chooses, the risk and control functions must become credible partners for the underlying businesses, and the perception that the control group is just a necessary evil (delaying approvals or appeasing internal auditors) must be altered.

Along with any model a bank may adopt, its risk and compliance functions should

continue to use traditional forms of influence—namely, measuring, quantifying, and managing the consequences of risk events. In banking, risk functions are augmenting the way banks charge business units for an expected loss, by taxing their profit figures as well as adjusting capital assigned. The most effective risk functions will find a way to make such profit and capital charges meaningful enough to prompt action across business units and other functions.

Senior managers, notably in banking, live in fear that some big operational or reputational scandal will one day shake the organization. They should confront this growing threat and rethink their entire approach to risk. Leading players are already embracing some of the initiatives we have outlined, though few have yet adopted a fully integrated approach. It's time they did. Making the mitigation of risk a routine and conscious part of the work of the whole organization can put managers in control and allow banks to reap the rewards of better risk management. MoCIB

Cindy Levy (cindy_levy@mckinsey.com) and **Antonio Simoes** (antonio_simoes@mckinsey.com) are principals in McKinsey's London office, and **Hamid Samandari** (hamid_samandari@mckinsey.com) is a principal in the Washington, DC, office.