TOWERS PERRIN

UNTANGLING OPERATIONAL RISK: CREATING ORDER FROM CHAOS

By Prakash Shimpi

The complexity of operational risk can be intimidating, but burying corporate heads in the sand is never the right response. Operational risk management involves preventing, controlling and managing risk, none of which is possible without support from the top down.

Precisely because operational risk can seem impossibly tangled and chaotic, companies often misdirect their attention toward smaller risks that are easier to grasp — just when they need to be taking on strategic, big-picture risk assessment. When faced with such an enormous challenge, how can companies sort out and address their operational risks?

FOCUS ON THE FIVE KEYS

Risk management is a process of measurement, prioritization, action, integration and, ultimately, building ERM into the culture of your company. One reassuring recommendation — from companies, like H.J. Heinz, that have gone through this cultural transformation themselves — is to begin building an operational risk program by narrowing your company's focus to areas that will be key to your success:

- culture
- governance
- collection of risk data
- unraveling and analyzing the data
- determining the risk information and communicating its importance.

BUILD AN ERM CULTURE

Operational risk can occur in any activity, functional unit or organization within a company and is defined in terms of *people, processes* and *systems* across all business functions — from sales to project development, control organizations (e.g., compliance and legal) to senior management, right up through the C-suite. To *implement* ERM is to *integrate* ERM, the saying goes — from senior management buy-in through business unit ownership of risk.

By far the most effective driver of accountability for risk and control ownership is CEO and senior management identifying ERM as an *important* initiative that embeds risk management targets in every business unit's goals. Sounds simple, right? Make sure your CEO is on board, talking up operational risk with senior leadership, and seeking input and involvement not only from the business unit heads, but also compliance, risk and legal directors. Perfect. But how is a case for this kind of deep commitment made to a CEO in the first place?

Help is available from seemingly unlikely sources. Jim Traut, Director, ERM, H.J. Heinz, suggests that a triggering event like the catastrophe of 9/11 or an unwelcome new regulation such as Sarbanes-Oxley (SOX) can stimulate company commitment to transforming risk chaos into productive change. For example, ERM experience at Heinz has shown that a company that has strengthened its corporate governance, ethics and finance functions through SOX-compliance efforts is already geared to successfully implement operational risk management. And agencies such as Standard & Poor's, by adding a risk component to their rating process, currently are contributing strong motivation for senior leadership to look long and hard at operational risks.

As companies build their operational risk capabilities, they will recognize that there is a difference between managing their operations risks and true operational risk. An operations risk such as business continuity can be serious enough, but is usually managed through tactical methods such as six sigma, system-driven key indicators (KRIs) or other means. Operational risks, on the other hand, are driven by "non-normal" failures — such as business practice failures in the case of the subprime crisis. Operational risk addresses an entirely different business problem and should be managed both strategically and tactically.

ADOPT GOOD GOVERNANCE

Some companies have looked on regulation compliance with suspicion, dreading the self-analysis involved as much as the disclosures to be made. Companies with successful ERM programs, however, have learned that improvements in culture and governance pay off in corporate strength in the marketplace. Meeting with regulators can speed the learning and development phase of building an ERM culture.

Some companies have looked on regulation compliance with suspicion, dreading the self-analysis involved as much as the disclosures to be made.

Regulators are not so much concerned about the risks you're aware of today — they like to think you've covered those already. What they're more interested in are the risks over the horizon, which are in your company's interest to determine. As hard as it is, senior leaders really need to think about *emerging risks* and how to address them. In fact, it's prudent to spend *quite a lot of time* looking at these potentials across each different region and business center, early adopters of ERM report.

COLLECT YOUR RISK DATA

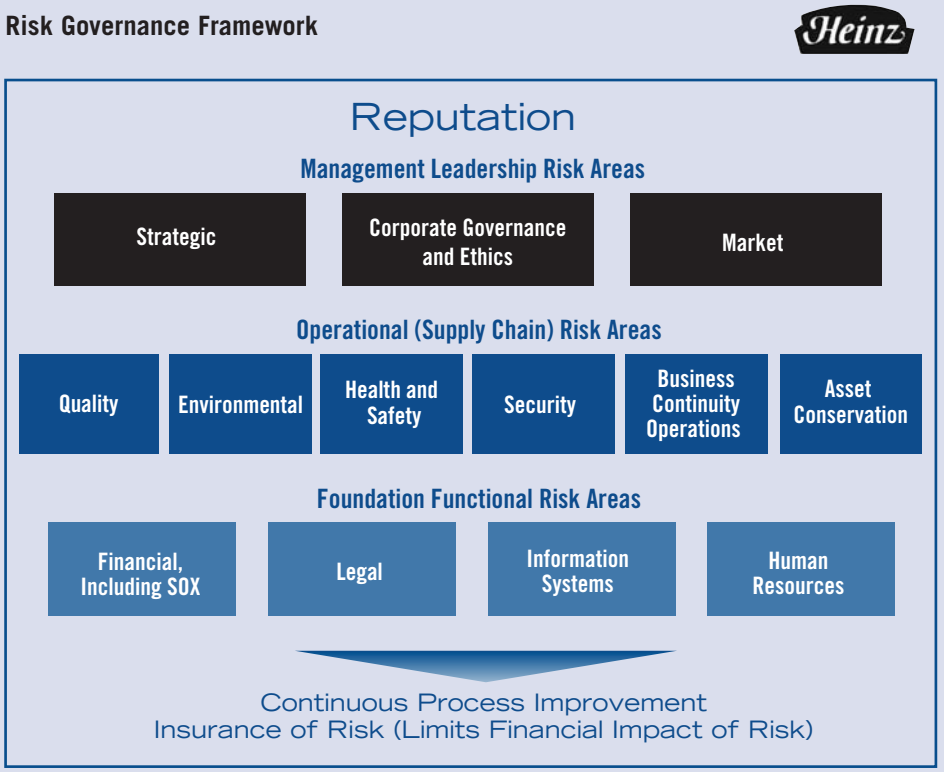
Risk is change, basically, and change itself is a big risk. So the trick is to capture data on relevant changes as well as known and emerging risks, analyze them to find the *information* the data provide — and then *communicate* the key points to business units globally to make sure you have, or get, coverage of those risks.

By collecting data centrally each quarter — from management, leadership, operational and foundational risk areas — you gain a bird's-eye view of what's going on around the world in your company — whether that involves a change in regulations, new products being launched in different regions or system changes.

PRIORITIZE THE DATA

The next step is to really *prioritize* your critical risks. This is not just a compliance exercise for SOX or a corporate audit; it's working with management teams to improve what they're doing to secure your company's future.

Risk Governance Framework



Look at the *likelihood* of each material risk as a benchmark for putting the most pressing controls in place, Traut advises. To classic likelihood assessments, some companies apply probabilistic views of risk exposure. In any case, some of the "risks" that turn up in your data may be better classified as "concerns" or "worries" and removed from your priority list. After each VP signs off on three to five risks that could prevent your company from achieving its objectives, risk resolution can be handled in teams, thus not only helping to protect vital functions but also integrating operational risk management throughout the organization.

COMMUNICATE RISK INFORMATION'S IMPORTANCE

Having worked through what your risks are and who owns them, processes can be developed to prevent or control them. A pyramid-shaped risk management model developed for Heinz structures the core values at its base, i.e., protecting the employees, products, assets, corporate sustainability and maintaining the flow of goods. The middle layer is comprised of risk-preventive processes for operational and nonoperational areas of the company. At the top, however, is the overarching goal

Having worked through what your risks are and who owns them, processes can be developed to prevent or control them.

of developing one broad approach that applies to both those areas, whether the risk issue is financial reporting or product recall. Most importantly, the model and the approach must be communicated across all regions and units of the company.

In addition, Traut stressed that risk management cannot reside at one desk or within one office. The operational risk manager, he emphasized, focuses on transfer and control actions as well as follow-up. In management teams, with full organizational support:

- *The office of risk management* is responsible for enterprise risk management, global quality and other operational risk areas.
- *A global business risk management committee,* with a mandate to assess a range of risk and control issues, provides direction to the business, initiates training and ensures that key areas are covered, results are monitored and issues are followed up.
- *A risk council or steering committee,* made up of representatives of other functions in operational and nonoperational areas, helps ensure that efforts are kept on track. An added value is the committee's ability to continually communicate across functional lines throughout the organization. Its primary function, in fact, should be company-wide communication.

A risk manager may also report to the audit committee once or twice a year, the chairman of the board quarterly, meet with corporate audit whenever there is a risk issue to team up on and, often, the disclosure committee as well. For those who think of proxy disclosures as "just a lot of legalese," Traut argues that many CFOs and COOs believe those disclosures should provide an accurate depiction of a company's top risk areas. Effective communication and transparent governance go hand in hand.

TAKE AIM, TAKE ACTION

"If we don't transfer risk, we get control over it," says Traut, speaking of Heinz. Even if you know your risks, due to a host of reasons including poor governance or lack of management focus, no action — or the wrong action — may be taken to address them. Without total and active C-suite support, transfer and control actions will not be completed, and the chaos of your "risk big picture" will increase.

Even basic resourcing of an operational risk program, for example, requires that a CEO be willing not only to talk the talk, but to walk the walk. As funding comes from the business units, they need to be told the importance of owning their own risks right from the top. Fortunately, in many cases buy-in is made easier by the fact that business units are often covering a lot of risk management ground already, just in terms of good business practices.

FOLLOW THROUGH

Managing operational risk, Traut explains, comes down to determining what situations could hurt your company — from the C-suite to the factory floor — and taking corrective actions to prevent or transfer them, then following up: Have your people completed the tasks they were directed to do?

Chances are, you'll never be able to predict the future with total accuracy or avoid every calamity, but it is essential to gain control, routinize and ameliorate the variability of — or slough off, through risk transfer or other means — potential risks that can be anticipated. Without the support of an ERM culture and responsible, transparent governance, it is very difficult to make an operational risk program stick, to ensure that it's effective and produces optimal results. An inability to recognize the degree of risk until a trigger event occurs hits at the heart, and the art, of risk management: Know *what* risks need to be controlled, and *how* to either control them through preventive processes and procedures, or *when* to transfer them. Successful operational risk management is, like most best practices, a function of process, discipline and leadership. Sounds simple, right?

Prakash Shimpi is a managing principal of Towers Perrin with global responsibility for Enterprise Risk Management (ERM). He is based in New York. This paper is taken in part from a panel discussion at the Towers Perrin & Economist Intelligence Unit 2007 Enterprise Risk Management Conference in New York. Panelists included speaker Jim Traut, Director of ERM at H.J. Heinz.

TOWERS PERRIN

ABOUT TOWERS PERRIN

Towers Perrin is a global professional services firm that helps organizations improve performance through effective people, risk and financial management. The firm provides innovative solutions in the areas of human capital strategy, program design and management, and in the areas of risk and capital management, reinsurance intermediary services and actuarial consulting.

Towers Perrin has offices and alliance partners in the world's major markets. More information about Towers Perrin is available at *www.towersperrin.com.*

TP534-08