



The failed loans and credit products that have shaken global financial markets point to the immediate need to manage enterprise risks.

Real-world ERM



BY NEIL BAKER
EDITOR, *INTERNAL AUDITING*

ILLUSTRATION BY
DOUG STERN/YACINSKI DESIGN, LLC

ENTERPRISE RISK MANAGEMENT (ERM) SOUNDS LIKE AN EXCELLENT IDEA. Embed risk in every business decision, connect the strategy-setting process to the control framework, and thread it throughout the organization — top down and bottom up. Do that, and the board has a dashboard view of all the major threats to the business. Wheat is separated from chaff. The organization enjoys the benefits of a seamless process that

identifies, prioritizes, and effectively manages *all* of its risks. The problem is, it doesn't always work. Launched with all the fanfare of an emperor slipping into his new clothes, ERM initiatives too often sink into a toxic sludge of jargon, wishful thinking, and executive ambivalence.

Look at the crisis in the global banking industry. The sector once claimed leadership in ERM, but now some of its leading players have been nationalized or forced into shotgun mergers. The Financial Stability Forum, a group of central bankers, published a report on the causes of the credit crunch in April. It castigated the financial industry for its lamentable standards of risk management. Another damning report followed shortly afterward from the Institute of International Finance,

a Washington, D.C.-based global association of financial institutions. The crisis "raised questions about the ability of certain bank boards to oversee senior managements and to understand and monitor the business," it said.

Some banks, it seems, were very good at talking about ERM, but were less effective at actually doing it. According to a recent study from the Economist Intelligence Unit, only 18 percent of banks surveyed worldwide had an ERM strategy in place that was "well-formulated and

MAKING IT REAL

There is no shortage of guidance to explain what ERM is and how to implement it, though most of this information is written for risk and control specialists. To succeed, ERM efforts need to include people with other priorities. "One thing that makes it very difficult to implement ERM is that a lot of parties need to be involved," says Ladd Muzzy, Ernst & Young's Americas Enterprise Risk Management Leader. "You have to be very pragmatic and develop an approach that

"A simple, consistent, and well-understood risk framework is vital," says John Wheeler, founder and principal at ERM consultancy Wheelhouse Advisors in Atlanta. That's especially true where people are burned out by U.S. Sarbanes-Oxley Act of 2002 compliance or are overloaded by corporate initiatives that get in the way of their "real jobs." The danger is that ERM initiatives get sidelined, and that's fatal. As John Giantzidis, compliance manager at AMAG Pharmaceuticals in Boston says: "The

"One thing that makes it difficult to implement ERM is that a lot of parties need to be involved. You have to be very pragmatic and develop an approach that people are going to be able to understand." — Ladd Muzzy



rolled out across the business." Facing a looming regulatory crackdown, financial firms will have to renew their efforts to implement ERM, the study says — if they are still in business.

The financial sector is just an example. ERM is hard to implement in any business. Too often, these initiatives run out of steam. Clearly, ERM is a very appealing idea, but how can it be made to work in the real world? What can organizations do to get beyond the rhetoric and implement ERM in a way that will be both effective and sustainable? And how can their internal audit shops help?

people in the business are going to be able to understand."

Indeed, a lack of understanding underpins each of the three main reasons why, according to Muzzy, ERM projects run into the sand. Failure to communicate the value of ERM in simple and concrete terms makes it hard to get managers to buy into the process. Failure to create a commonly understood language for talking about risk in the organization undermines efforts to develop a single approach to risk management. And failure to understand the need for visible top-level support for ERM means that executive enthusiasm wanes.

greatest issue with ERM implementation is explaining to people that ERM does not and cannot operate in isolation."

So how can an organization implement ERM in a way that people will understand? Here's one tip: drop the acronym. Paul Sobel is vice president of internal audit at energy company Mirant in Atlanta and a recognized expert on ERM. Yet, his employer does not use a formal definition of ERM and has not adopted a formal ERM framework. When Sobel discusses risk in the company of fellow professionals he, like all the experts interviewed for this article, references the *Enterprise Risk*

Management-Integrated Framework that The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published in 2004. This document gives a detailed definition of ERM and explains some of the ways in which

Embedding ERM — the holy grail of the process, whereby risk management is part of everyday work practices — has been a challenge. “Hardly anybody disagrees with the framework, the theory, and the methodology of ERM,” he says, “but the

because the methodology has changed, it’s because senior people come and go. If a new chief financial officer arrives, or an executive moves to a job in the business where his or her role in the ERM process is different, “it’s almost like you



“What really makes ERM successful is what I call a ‘risk mind-set’ — having everybody in the organization thinking about risk whenever they have to make a decision.” — Paul Sobel

it can be implemented. At Mirant, Sobel uses it behind the scenes, but not more widely across the organization. “Our sense was that the COSO framework looked too bureaucratic,” he says. “As a company, we are adopting the principles that we think make sense.” That means talking about risk management, not ERM.

“What really makes ERM successful is what I call a ‘risk mind-set’ — having everybody in the organization thinking about risk whenever they have to make a decision,” Sobel explains. “I like to talk to people about their ability to answer a few simple questions whenever a decision is made: What do I want to accomplish, what could stop me from accomplishing it, and what should I do to make sure those things don’t happen or that they can be managed? That seems to demystify it.”

Granted, he says, ERM is more complicated than that — especially the evaluation of “What could stop me?” and “What do I need to do about it?” Get managers to ask themselves these questions and, over time, they will see the value of the tools and procedures that come with ERM.

EMBEDDING ERM

Michael Head, managing director of corporate audit at online brokerage TD Ameritrade, headquartered in Omaha, Neb., has worked hard to make ERM a reality at his organization. The business is in the “mature phase,” he says, having spent the past three years maintaining and enhancing its processes.

key is ownership. If managers don’t have to own it on a day-to-day basis, and they see that as someone else’s job, it doesn’t come to life or get implemented.”

How do organizations overcome this? Remember the human element of ERM, Head says, “This is a process delivered by people.” In his organization, the process has been successful at some times and less so at others. That’s not

have to go back through an awareness training effort to make sure everybody in their new positions embraces ERM and understands their role,” he says. “Without support and understanding from the top, the likelihood of sustainable and successful implementation and maintenance is significantly reduced.”

All the ERM manuals stress the need for top-level support, but supportive

Risk Management and the Credit Crisis

Internal auditors trying to persuade their organizations to take risk management more seriously could start by reading two insightful reports on the fall-out from the credit crunch.

Climbing Out of the Credit Crunch, published by international accountancy body the Association of Chartered Certified Accountants, argues that the principal cause of the current crisis was not subprime mortgage defaults but a failure of corporate governance at banks. Bad governance encouraged excessive short-term thinking and a blindness to risk, the report says. Risk management departments in banks must have greater influence and power, the report concludes (www.accaglobal.com).

Final Report of the IIF Committee on Market Best Practices, from the Institute of International Finance, sets out a series of principles for reforming the financial sector. It says improving risk management practice is the No. 1 priority. The report’s first principle states: “A robust and pervasive risk culture throughout the firm is essential. This risk culture should be embedded in the way the firm operates and should cover all areas and activities, with particular care not to limit risk management to specific business areas or to have it operate only as an audit or control function” (www.iif.com).

In addition to these reports, internal auditors who are thinking about what role they could play in helping their organization move to ERM should read guidance that IIA-UK and Ireland published on this topic in 2004. *The Role of Internal Audit in Enterprise-wide Risk Management* provides a practical description of the “green, amber, and red” activities that internal auditing might perform. It also suggests safeguards for audit shops that engage in “red-zone” activities in the short term (www.iaa.org.uk).

words are not enough, Head argues. “All C-suite people are not equal in terms of power and influence within the company. For ERM to be effective, whoever is going to be the executive owner and sponsor of risk management has to be respected by the other executives and has to be considered a key senior leader with the chief executive officer (CEO) and chairman.”

BUILDING ON WHAT WORKS

An important way of gaining support for ERM is to build on what the organization does already, Head advises. His company had committees monitoring areas such as brokerage risk, health and safety, and financial disclosures that existed before ERM was implemented. “We wanted to implement ERM in a way that aligned

do, ranging from “green zone” activities, which are comfortable audit territory (such as process assurance), to “red zone” activities, which should be the responsibility of management (such as deciding on risk responses).

Paul Wilhelmij, partner and ERM lead practitioner in PricewaterhouseCoopers’ London-based governance and risk

“We wanted to implement ERM in a way that aligned with risk management processes that were already embedded in the company. We didn’t want to change how management managed risks.” —Michael Head



That’s because the executive sponsor has to have the influence and authority to tell key business managers to get their staff on board, Head says. “If other senior executives can say, ‘I don’t want my people worrying about risk management, that’s your job,’ then it’s not going to work,” he explains. “It helps to have all the executive peers in agreement, but when push comes to shove, the person sponsoring ERM has to be influential enough to dictate to people that they will do it.”

When it comes to ERM leadership, it’s not about frameworks or methodologies. “It’s about power and influence at the people level, not on paper or in charts,” Head says. To embed ERM genuinely it must be included with the other business objectives that managers are accountable for. “If the sponsor sits in your office and says your people aren’t doing it and, as a result, it’s going to affect your performance review and bonus if you don’t get in line, that person says ‘I hear you’ and they do it,” he explains. “It’s the difference between a company that has ERM books on its shelves and one that gets ERM embedded and working on a day-to-day basis.” This power is often lacking, in banks at least, and was one of the four root causes of the credit crunch, according to *Climbing Out of the Credit Crunch*, a report published in October by the Association of Chartered Certified Accountants (ACCA) (see “Risk Management and the Credit Crisis” on page 35).

with risk management processes that were already embedded in the company,” he explains. “We didn’t want to change how management managed risks, but to align existing processes with a top-down communication of risk appetite.”

Enhance what you’ve got and standardize where you can, he recommends, especially with regard to risk management language and reporting, but don’t replace processes or run parallel processes. “Build on what you do well, and people will feel engaged because they are contributing to a solution, not changing something that they know has worked for years.”

Muzzy agrees. “Organizations see the word *enterprise* and feel that they need to chew off everything at one time,” he says. They start too fast and run out of steam. “You need to start slow and leverage what is already in place. I’ve seen this fail a number of times where companies try to boil the ocean and create a brand new approach to risk, while failing to understand and use what the business has already invested in and the good things that it is already doing.”

AUDITING’S ROLE

Internal audit shops can play an important part in getting ERM to work. In 2004, IIA-UK and Ireland produced *The Role of Internal Audit in Enterprise-wide Risk Management*, which set out some of the work that an audit function might

compliance business, has his own tips for internal audit involvement.

- Gather internal or external examples to help managers understand the value of ERM — both to the organization and to them personally.
- Highlight the cost of risk management failures and the potential returns from managing opportunities successfully.
- Encourage senior management to set minimum mitigation standards for key risks and get business leaders to sign-off against compliance with these standards, with a statement of any exceptions and remediation plans.
- Review how key risks identified through the ERM process are managed and the extent of compliance with minimum standards.

“When challenging the coverage of key risks in the top-10 risk register, check that the big enablers or blockers to achieving the business strategy are considered,” Wilhelmij says. “Do not let the seemingly simple risks that are relatively easy to understand take attention from the big risks that are not easy to grasp, such as changes in the regulatory or competitive landscape, product complexity, and interdependencies.”

In real-world ERM, the audit shop has to be flexible, Head says. He partnered with TD Ameritrade’s finance team to get ERM started. He talked to executive management about what the audit function’s role should be, facilitated strategic

risk assessment sessions with management to identify key risks, and provided coaching. But he made it clear that management had to own ERM, establish risk levels, determine monitoring activities, and implement the process.

In practice, he did work that helped to establish ERM, but work he wouldn't be comfortable doing once it was implemented. "I've got to be in an objective and independent role," he says. With ERM established, he has stepped back into green zone activities. "Now we are doing annual audits of the risk management function and assessing and reporting on it. We independently evaluate the effectiveness of risk management and give assurance that the process is in place and working as intended."

If the audit shop needs to compromise its independence and objectivity to get ERM started, it must be clear about what it is doing and why, he says. "You have to have agreement from management that you are going to back away from that role, and you need a formal time line that says when and how that is going to happen. If you don't set down the parameters and have an action plan for how you are going to back away, you may get a job that you can never give up."

in risk and control, they have the enthusiasm needed to get ERM started. As Sobel says, "You really have to believe in this and have a passion for it, because you will come across people who are not interested."

The internal audit shop is also likely to have the focus needed to keep ERM alive. ERM is a journey, not a destination, Sobel says. "Once you say we've gotten there, that's a danger sign to me. I think it is healthier to call it a journey because it keeps you on your guard a little more."

True, there are things that an organization can and should do that, once accomplished, would allow it to say it has a robust ERM program. "But, just as for any process, this is an ever-changing world — risks change all the time. No one is capable of understanding all the risk scenarios that might be out there," he says. "As a result, I don't think anybody can have ERM fully in place in such a way that they can, with comfort, say they are not going to end up like Lehman Brothers."

Nonetheless, the prevailing attitude among many politicians and regulators is that bank boards should have foreseen and acted on at least some of the risks that pushed the sector into crisis. Remuneration policy is one example. The ACCA

to stamp out bad practice. "We want to ensure that firms follow remuneration policies which are aligned with sound risk management systems and controls and with the firm's stated risk appetite," the letter said.

Remuneration risk was not the only root cause identified by the ACCA that, arguably, bank boards should have recognized and controlled. Others include the over-complexity of financial products and a lack of management understanding of the associated risks, an over-dependence on debt, the assumption that capital costs would remain low, and the failure to appreciate the influence of cultural and motivational factors, such as rigidity of thinking and lack of desire to change — what the ACCA called "an attitude of 'it is not my problem.'" Again, all of these failings occurred in a sector that was celebrated for its risk management expertise.

Perhaps the very public consequences of risk management failure in the banking sector will encourage boards and executives in other industries to take ERM more seriously. If so, the advice from internal auditors who are making ERM work is clear: Show the value, keep it simple, and build real support. The rest of it — the jargon, acronyms,



One reason why internal audit shops might take an initial lead is that, as experts in risk and control, they have the enthusiasm needed to get ERM started.

Sobel has been through that same process. "In the early stages, sometimes internal auditing has to take the lead to get the momentum going," he says. "It may trip over the line of independence and objectivity for awhile, but you can get back on the right side of the line later, as long as you tell people this is something that management should own and you are just doing it to get it off the ground."

A JOURNEY, NOT A DESTINATION

Another reason why internal audit shops might take an initial lead is that, as experts

report cites independent surveys that highlight a growing differential in remuneration packages for CEOs compared with other board members. Also, over the past decade, remuneration of senior staff grew at a faster rate than dividends paid to shareholders. This encouraged excessive short-termism and undermined prudent risk-taking, the ACCA reports. In the United Kingdom, the Financial Services Authority has written to banks to say it is concerned that "inappropriate" remuneration schemes may have contributed to the crisis and that it wants

flowcharts, and models — can be useful behind the scenes but may get in the way when it comes to making ERM work in the real world. "Sometimes you can do ERM in a stealth-like manner," Sobel says. "We don't call it ERM because that term can't get any traction, but that's okay. As long as we are implementing the right kind of steps, I don't care what we call it."

To comment on this article, e-mail the author at neil.baker@theiaa.org.