

ENTERPRISE RISK MANAGEMENT

Risk's Rewards

Are you on board with enterprise risk management? You had better be. It's the future of how businesses will be run.

BY SCOTT BERINATO

What would you do if, two months after your company went public, one of the two major markets you sell products to simply vanished? If, in the span of seven days, \$350 million in sales just disappeared?

Would you throw your hands up and say, No one could have foreseen the events of 9/11, and then just stand by as the company tore off a half-dozen bad quarters? Would you just absorb the discomfiting cuts to your budget and your staff, and eschew any strategic plans you had set up to help the business grow, because, well, no one could have been prepared for such a catastrophe?

Or, would you be like Rockwell Collins, the supplier of military and commercial aircraft parts, which suffered the precise fate described above and yet had a contingency plan in place within 10 days? Despite the fact that Rockwell's commercial market—20 percent of its business—vanished after 9/11, IT still contributed to the business's growth.

No doubt you want your company to be like Rockwell Collins. So you ask, How did they pull it off? "Either we're the luckiest company in the world," posits Art Gemmer, the company's principal risk analyst, "or our enterprise risk management mind-set gives us insights that make us do better."

Gemmer clearly believes not in luck, but in the power of enterprise risk management (ERM)—broadly characterized as a system of managing risk across an entire company. Gemmer says ERM helps companies prepare for events on the scale of a 9/11. More important, he says, it improves the way a company handles the more predictable risks that businesses face every day. ERM allows a company to avoid bad investments, and, conversely, make investments that might intuitively seem too risky. You're already trying to improve your IT decision making through better governance. ERM makes governance better.

The few companies that have adopted risk management methodologies report fewer failed ventures and less damage from adverse events. For Rockwell Collins, ERM's value has been proven time and again. Several years ago, a project manager named John-Paul Besong implemented a bet-the-company SAP system using ERM principles. "Every decision became a risk decision," he says. The project went so smoothly that Besong was named Rockwell Collins's CIO shortly thereafter. There is no more persuasive metric at Rockwell Collins to demonstrate the effectiveness of ERM than this: The company has turned a profit every single quarter after 9/11. And in January 2004, *Forbes* called Rockwell Collins the best-managed aerospace firm in America.

Make no mistake, ERM is hard. It changes how everyone does their jobs. It took Rockwell Collins the better part of a decade to become an organization governed by risk. And while it shouldn't take you that long, because much of the trail has been blazed for you, it won't be a six-month job either.

Every risk expert we spoke with anticipated that you, the CIO, will resist ERM. "For some reason, it's like [CIOs] are snorting novocaine or something. They think they can avoid ERM," says Adrian Bowles, a risk expert with The Robert Frances Group. Bowles urges you not to be dissuaded. "The risks are coming to find you. Your job is at risk. The only defense is to be part of the effort to manage them."



TEAM AGAINST RISK: Enterprise risk management helps John-Paul Besong (left), CIO with aerospace supplier Rockwell Collins, and Art Gemmer, principal risk analyst, make better technology decisions.

This mind-set is emerging not because risk management is a trendy buzzword being volleyed around

boardrooms—though lately it is—but because balancing risk is becoming the only effective way to manage a corporation in a complex world. "We're able to react [to that complex environment] because of our risk mind-set," says Besong. "With what happened to us, our agility was called to task. And we had the risk methodology in place to handle it."

So, what is ERM?

A good rule of thumb in IT is that the number of definitions for a concept rises proportionately to the concept's buzz. ERM, for which we collected no fewer than a dozen definitions, is no exception. We'll use James Lam's definition.

Lam is an author and consultant who says he was the first chief risk officer at any company, a position that he pioneered at GE Capital. ERM, he says, is "the integrated management of business risk, financial risk, operational risk and risk transfer to maximize a firm's shareholder value." That is, making a company more profitable by creating a single view of all risks, internal and external, and an executive-level management strategy to deal with those risks. (For an example, see "Three Steps to Risk Assessment,")

Some principles underlying Lam's (or anyone's) definition of ERM include:

1. An integrated view of risk. IT, HR, finance and every other "silo" uses standardized language, metrics and tools. Many finance departments already have processes for managing risk, so it's possible that such standards will come from there. Meanwhile, Bill Sharon, CIO of advertising agency McCann Worldgroup, has borrowed heavily from a risk system developed

by Nobel Prize-winning psychologists, as described in the book *Against the Gods: The Remarkable Story of Risk*, by Peter Bernstein.

2. A pan-corporate view of risk. ERM is not collecting each silo's risks to its own silo. It's collecting each silo's risks to each other and the company. When Sherry Higgins took a position at the FBI to lead its IT modernization effort, called Trilogy, one of her first acts was to install an enterprise risk framework. Almost immediately, she realized her first deadline was only four months out and unrealistic. "The risk to the project was obvious," Higgins says. "But I was looking at the risks to the FBI. What does that mean for intelligence analysts not getting these systems on time? When you go to [Congress] and deliver this news, what does that mean to funding for the FBI as a whole? The goal of ERM is to get at these risks that span stovepipes or fall between them."

3. A bottom-line view of risk. Risks always get expressed in terms of their potential impact on the business as a whole, not in terms of their impact on any given silo. When Higgins decided she needed to hire professional project managers for Trilogy, she had to sell FBI Director Robert Mueller on that. She didn't focus on the potential for the project to fail. She sold him by explaining that the FBI ran the risk of being unable to do its job.

4. A risk office's view of risk. In a growing number of companies, ERM is facilitated by an executive-level risk office that provides the expertise and resources you don't have the time or money to acquire. Many risk experts argue that if you don't have a risk office, you're not really doing ERM.

The CIO's role is the same as every other silo leader's role—to identify risks within the department and, by collaborating with leaders from other departments, to identify risks across business units. It is a support role to the risk office but a critical one. While most risk officers are fluent in financial risk, they are counting on you to identify operational risks related to IT.

5. A longitudinal view of risk. Risk is an ongoing behavior, not a regularly scheduled process.

This stuff isn't new. Risk management hails from a lineage of related, proven practices. ERM's uncle is the quality management movement of the 1970s, when manufacturers adopted quality standards that in turn led to better products. ERM's grandfather is Nobel Prize-winning game theory, a mathematical system for optimizing



Bill Sharon, CIO with McCann Worldgroup, says managing enterprise risks eventually becomes second nature.

decisions in a competitive setting. Its principles govern risk methodologies today.

You've probably done a little bit of risk management at the project level. In a way, ERM is the same thing except, in this case, your company is the project. What is new about ERM is the breadth of its vision. ERM's idealistic goal—to unify risk management across an entire company—makes it a daunting undertaking (and so far, a rare one). George Westerman, a research scientist who is studying ERM in relation to information technology at MIT, says that in its current state, ERM reminds him of what someone once said about e-commerce in the 90s: It's like teenage sex. "Everyone wants to be doing it. Everyone thinks everybody else is doing it. Not many people are actually doing it, and no one is doing it particularly well."

"The topic is so big and scary," Westerman says, that people decide not to try. However, he adds, "It's so important to just get started."

So why now?

Just why ERM is important now is complex, but the reasons include IT as a primary risk to operations.

First, several macro-trends have accrued to expose operational risks to the business from IT that in the past were blissfully ignored. Start with Y2K—the realization that IT systems we depended on were vulnerable. Then came 9/11 and the (literally) thousands of risks to businesses that it exposed. Computer viruses have continually interrupted work, illuminating the risks of using bad software. More recently, the risks to a corporation's reputation have announced themselves in the form of massive thefts of personal data. There is, of course, terrorism, political unrest, war and weather, among other global risks to consider.

The reason these risks are suddenly being accounted for is because the systems are becoming ever more critical. Today, one bad IT decision can severely hamper—or even take down—a company.

The second factor driving ERM now is the regulatory environment, along with efforts within some industries to protect companies from the volatile global business environment.

For example, the Basel II Accord, an effort spearheaded by the Group of 10 countries' leading financial services stakeholders, dictates that by year-end 2006, a financial services company must carry a predetermined amount of capital to offset the level of risk found in the company, as determined by guidelines in the Accord. Unlike the first version of this regulation from 1988, Basel II addresses not just capital risk, but also operational risk, including the risks IT systems create for the company. In other words, it mandates some form of enterprise risk management.

Likewise, the Treadway Commission's Committee on Sponsoring Organizations (COSO), a voluntary private-sector organization formed in 1985 to combat fraudulent financial reporting, produced an enterprise risk management framework. The Information Systems Audit and Control Association (Isaca) developed Cobit (the Control Objective for Information and related Technology), a document that also lays out how to set up an enterprise risk management framework. Both are efforts designed to jump-start the use of ERM in corporations.

Of course, there's Sarbanes-Oxley too. While not the engine driving ERM, Sarbox might be the spark plug. CEOs, after all, don't want to go to jail. Says David Weymouth, CIO of Barclays, the U.K.-based financial services company: "We've spent something like [\$251 million] on a regulatory program. Noncompliance is a huge risk we need to manage."

McCann CIO Sharon says that for him, Sarbox sounds eerily familiar and provides good evidence that the time is right for risk management. Sharon worked in the financial services industry during the savings and loan scandal. To comply with a law aimed at cleaning up the financial sector, "We spent two years adopting risk [management] processes and doing backbreaking risk assessments. After a while people said, We have a business to run." Compliance became a byproduct of larger risk assessment efforts. Similarly, Sharon predicts, ERM will make compliance with Sarbox a byproduct of risk management, not the focus of it.

Finally, ERM is emerging now because of a growing body of evidence that it really works:

- Westerman at MIT has identified correlations between business-IT alignment and risk confidence. That is, the more confident a CIO was in his ability to manage his operational risk, the more aligned he said he was with the business.

- J. Davidson Frame, academic dean of the University of Management and Technology, worked with a company that introduced risk management and then made business unit vice presidents sign off, Sarbanes-Oxley style, on the risks that IT projects presented to the business. Project success rates increased immediately. Perhaps more important, the number of project initiatives taken on by this company decreased by 25 percent in three months.

This finding demonstrates a key part of ERM's appeal, which is mentioned over and over again by CIOs and risk experts: ERM improves decision making by helping a company avoid costly failures from operations that prove too risky.

"Right now, we're moving premises," says Weymouth. With enterprise risk management, business units can factor that into their plans and report what risks moving creates. "Say the group doing a telephony project tells us that moving affects their ability to successfully complete their project. We can now factor that in and minimize the risk to the company by shifting resources, putting the project on hold. Whatever it takes. We're able to make a better decision than if these factors weren't considered."

But I don't have time for this

The experts expect you to be hard-line resisters to enterprise risk management because you don't understand it. (See "Misconceptions About Risk," this page). So we posed some of your potential reservations and let them counter those reservations with reasons why you need to get on board.

Reservation: I've got a full load already, and now you're asking me to start this massive new project.

Rebuttal: Yes, some groundwork needs to be laid. But, for the most part, becoming part of an ERM-driven company doesn't mean more work or some additional bureaucratic system to administer; rather it's a new way to approach your job. If you're doing ERM right, you're not really aware that you're doing it. Besong calls it "the new normal for us." Weymouth says, "I manage through risk."

The hard part, then, is shifting your focus from a technology-centric view to a risk-centric view. For that, you can find risk experts to carry you along. See the next reservation.

Reservation: I don't have the expertise to do this or the staff with the expertise to do this. And I don't have time to take a bunch of courses or read five books.

Rebuttal: This is precisely why risk officers are here. It's the job of a corporate risk expert, such as a chief risk officer, to provide whatever tools and education IT needs to get started, says Lam.



By making educated guesses about the likelihood of IT risks, Barclays CIO David Weymouth can plan ahead to minimize their impact.

"People don't fend for themselves here," says Gemmer of Rockwell Collins. "I used to get 15 to 20 calls a year [internally] looking for help on risk. [Now] I'm getting up to two calls a week. They just know it's the right way to do things, and they want to do a good job with it."

ERM is a framework for better IT governance. It helps you make better decisions.

A risk office, whether it's one person (as Higgins had at the FBI) or a whole staff, should provide a clearinghouse of risk resources so that you don't have to learn the minutiae of, say, Monte Carlo simulations. A risk office will also enforce the standards created around your risk assessment processes and be responsible for producing digestible reports about your risks that help the company make decisions. If your company doesn't have a risk officer, you can hire a consultant to help you get started. But even the consultant will eventually recommend that you hire your own staff expert who is steeped in your business.

Reservation: I'm already instituting governance mechanisms.

Rebuttal: Peter Weill, director of the Center for Information Systems Research at MIT, has shown that good IT governance leads to more successful companies. ERM is a framework for better IT governance. "What IT and CIOs need to realize is ERM is an opportunity," says Larry Ponemon, chairman and founder of The Ponemon Institute. "It makes you more competitive. It helps you make better decisions. It makes you smarter."

Harvey Parr, a retired director with British Telecommunications (now the BT Group), remembers one IT project for a customer that looked like it was way too risky for his company to take on. "But we went through the risk process and found that the risks were controllable. Our competitors did not bid because they had the same inclination as us. So we bid on it and did it."

Reservation: Statistics!

Rebuttal: Don't be scared. Yes, companies fully immersed in risk will use a statistical approach to assessing it; probability and economic concepts, such as annual loss expectancy, are commonly applied tools. But the risk experts know enough about the numbers, and anyway, the numbers aren't as important as the qualitative analysis.

More than any other reservation, risk experts say CIOs will cite this one. It could be because IT is a profession that rewards precision, so the natural inclination of CIOs is to want to get their probability and impact statistics exactly right.

But risk—especially on the enterprise level—is not about precision. It's about accuracy. ERM isn't designed to scientifically predict terrorists using planes to attack buildings and harm the financial sector. It's designed to measure the likelihood and impact of a catastrophe on that scale, and what steps can be taken to mitigate that risk. "Look at the World Trade Center," says J. Davidson Frame. "Tens of thousands of lives were probably saved because a risk assessment a long time ago suggested that the stairways were too narrow, and the design was altered to accommodate that risk. It's unlikely that the risk process involved the stairs being highly trafficked due to a terrorist attack, but it proved useful in a terrorist attack. It wasn't a precise prediction; it was an accurate assessment."

OK, fine. How do I start?

ERM will be hard before it's easy, but Frame says the payoff for doing it will come sooner than you think. "Just start, and in six months you'll have the data to start making better decisions."

There are many methodologies that companies can lean on. Which one you're using should matter as little to you as it matters to your customers what internal IT systems you use. For example, Weymouth says Barclays bases much of its risk processes on Cobit, but that doesn't mean he's memorized the document.

Consultant Lam preaches getting started without getting stuck on the details. At first, "going through the process provides more value than the end product," he says. "The process itself will start to expose all those hidden risks, those interdependencies and risks across business units you never considered."

So, without getting stuck on particular methodologies, here is a basic chronology of what you'll be doing.

1. Risk identification. This is, basically, brainstorming. "It's almost too simple," says Higgins. "All it is is What if??" McCann's Sharon, in a previous job as a risk officer, says he handed out questionnaires asking IT staff and business end users to rate risk in five categories. You'll have meetings with the leaders of HR, IT, legal, finance

and so on to brainstorm risks to the company. IT will be asked to talk about, say, the environmental risks IT poses to the company. At Rockwell Collins, the risk that a tornado takes out the infrastructure or causes downtime might be mentioned. "But we wouldn't think about hurricanes in Iowa," where the company is headquartered, says Gemmer. The guys in Florida will bring it up. Then, the discussion moves to the enterprise: If the systems go down, what does that mean to our business? Loss of revenue? Reputational damage from call centers being unable to help customers? And so forth.

The point is to talk, and in talking, to find the risks that otherwise might have slipped through the cracks.

2. Risk assessment. You've identified your enterprise risks. Now you need to categorize them. The easiest way to start this is to map them on a probability-impact chart. A simple chart with low, medium, high? on each axis will allow you to map the probability and impact of each risk. Here's how Weymouth of Barclays explains how he manages the risk of unlicensed software: "When you've got 95,000 desktops, unlicensed software presents a risk to the company. We quantify the gross risk. In the worst case of having to buy licenses, pay fines, whatever, the amount comes to X pounds. But we mitigate that risk. We do license audits. We [raise] awareness. So after all that is laid out we believe that the worst case, mitigated, is actually .2X pounds. Then you look at the probability of that occurring to come up with a net risk."

Once again, the key here is not precision but accuracy. If Weymouth were using real numbers, .2 would be an educated guess. Even more important than accuracy is consistency. Every part of the company defines "low, medium and high" the same way.

MIT's Westerman uses the example of a global chemical company that defines high impact as something that affects 10 percent of working capital, medium impact as equaling 5 percent to 10 percent, and low as less than 5 percent. High likelihood means within a year; medium, one to five years; and low, not likely in the next five years. The point is, every department uses the same metrics and talks the same risk language.

3. Risk mitigation. Eventually, you'll have a map of your enterprise risks. From there, you'll look at how you are controlling risks, see how effective those controls are and decide what else you need to do. While you play a supporting role to the risk office in identifying risks, when it comes to mitigation, you'll be counted on to lead. The risk office can arbitrate the identification of risks, such as that of using unlicensed software. But only you can assess the countermeasures you have in place, such as routine software inventories or controls on desktop configurations, which will offset those risks.

While you play a supporting role in identifying risks, when it comes to mitigation, you will lead.

When Higgins implemented a risk management framework at the FBI, she found that one of the risks during the desktop modernization phase of her project was change management for users. If that was not properly handled, user productivity would plummet. This could severely affect intelligence analysts' ability to fight crime, a sensitive problem in the current political climate. (Note the way the risk connects from IT to the analysts to politics, and that the effect of the risk is not specific to IT.) Higgins piloted the rollout on a small scale and used data from the pilots to fine-tune the risk profile of the project.

At this stage, you're making decisions based on what the risk data tells you. You've started to manage by the principles of risk.

The Renaissance CIO

Once ERM starts, it doesn't stop. The real value of enterprise risk management comes when it becomes a continuous part of everyday business. Running a huge risk assessment once every six months will help you manage enterprise risk the same way looking at your cupboard once every six months will help you manage your grocery shopping.


Or to use a stronger metaphor, Rockwell Collins? Gemmer says that continuous enterprise risk management is like the quizzical winter sport of curling. In curling, participants hurl heavy stones down ice while teammates madly brush the ice in front of the moving stone to affect its path. The goal is to land the stone as close to the high-scoring area as possible.

The stone is your company. The hurling of it is an initial risk strategy. The brushing is continuous risk management. Gemmer puts it like this in an article on ERM: As the stone hurtles along to the goal area (which for you is overall profitability and shareholder value), "uncertainty [about the outcome] decreases, but your choices also become more limited." It's a creative metaphor, borne of Gemmer's interest in the world outside of IT. In fact, according to virtually everyone we talked to about risk management, the people who are most

successful at ERM have varied experiences, both in their careers and their personal lives.

You have a greater chance to succeed in an ERM-driven company if you are a Renaissance CIO: If you have interests outside of IT, a breadth of experience and knowledge, an ability to think outside your own silo, and an understanding of the history and culture of your corporation. "My predecessor was 10 times smarter than me about technology," says Sharon. "But he couldn't communicate risk to the business like I can."

Besong agrees that CIOs must be well-rounded. "We have this system we put on planes called TCAS, which stands for Traffic Alert and Collision Avoidance System. It constantly monitors the airspace around a plane and captures objects within 25 miles. It determines their paths, their speeds and projects their course. If [an] object's on a collision course with the plane, it alerts the pilot and suggests possible responses.

"The role of the CIO now is to do for business managers on the ground what TCAS does for pilots at 35,000 feet. It's the most challenging and invigorating work I've done." 

How do you manage enterprise risks? Contact Senior Editor Scott Berinato at sberinato@cio.com.

PHOTO OF BESONG AND COLLINS BY STEVEN VOTE; PHOTO OF SHARON BY STEVEN VOTE; PHOTO OF WEYMOUTH BY PATRICK BARTH

More Resources on Risk

I.T. AND THE ERM ENABLER

Read about the systems your company can use to collect information about risks.

RISK BIBLIOGRAPHY

A reading list on the subject of risk.
