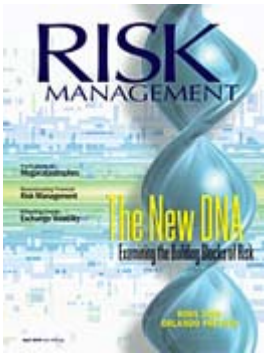

The Way Forward: Rethinking Enterprise Risk Management

by Bill Coffin
Publisher da Risk Management Magazine.

Publicado em abril/2009.

These are extraordinary times, especially for risk managers. And that is saying something indeed when one considers how the last decade has been marked by a succession of disasters that have all thrust the discipline of risk management into the spotlight.

By 1998, the dot-com bust was in full swing, displaying a magnitude of market risk that few risk managers had cause to contemplate before overheated business models deflated in record numbers.

In 2000, the Y2K bug created a level of IT risk so great that it consumed billions of dollars in loss prevention.

A year later, 9/11 redefined the scope of terrorism risk. The accounting scandals that destroyed Enron, WorldCom and Arthur Andersen in 2001 paved the way for Sarbanes-Oxley in 2002 and made corporate transparency a new watchword.

In 2003, SARS sharply raised awareness in pandemic risk, especially as avian flu was pegged as the next likely global epidemic. That summer, a massive blackout in the northeastern United States and southeastern Canada displayed the serious contingent business interruption risk posed by aging infrastructure. In Italy, Parmalat's massive accounting scandal later became "Europe's Enron."

In 2004, the Indian Ocean earthquake killed nearly 225,000 in 11 different countries, raising awareness of the catastrophic potential of tsunamis and natural disasters in general.

In 2005, this awareness reached a new level with the most catastrophic hurricane season on record. Some 28 storms, including a record-breaking 15 hurricanes, pummeled the shores of North America, with Hurricanes Katrina, Rita and Wilma causing unprecedented damage and making disaster preparedness and business continuity all top-level business concerns.

In 2008, extensive product liability issues surfaced concerning a string of Chinese product recalls, while the effects of the subprime lending crisis became too large to ignore, presaging the ongoing credit crisis-the worst financial disaster the world has seen since the Great Depression.

In each of these events, an element of risk management was brought to the fore in ways that forced executives to realize that these were hazards that needed to be managed. Risk managers were ideally suited to address such problems, and for many who had long toiled in obscurity, each fresh disaster provided a new chance for them to shine. In a grim way, the last 10 years have been very good for risk managers-even if they have been bad for just about everyone else on the planet.

Yet all of these aforementioned disasters, even when combined, do not carry the global magnitude of the current financial crisis, especially in terms of failed risk management. The cause of the credit crisis is fairly easy to summarize: unfettered greed promoted the sale of mortgages to unworthy buyers from an industry that simply stopped practicing any meaningful due diligence on the risks it was buying and selling, thereby creating a line of financial dominoes that led from Main Street to Wall Street and back again. And when the dominoes fell, everyone lost.

With every other risk management disaster of the past decade, the effects were ultimately localized by geography or industry. The credit crisis is the first truly universal risk management disaster, and it calls into question both the current state of the discipline and its future.

The State of Risk Management

Back in the 1970s, there was a remarkable transformation of the risk management discipline as insurance buyers elevated themselves into risk managers responsible for, and capable of, handling a wide range of business challenges that often could not be addressed with insurance coverage alone. Risk managers had to learn the decision-making processes and how organizations gauge, analyze and manage their risks. It was a sea change not just for the discipline but for how companies looked at the very concept of risk.

But even as risk management became an ever more sophisticated line of work in the decades that followed, it could never shake its intrinsic link to insurance coverage. Ultimately, "insurance management" tethered the discipline to a certain strata of decision making. Risk managers, by and large, were not invited to weigh in on top-level, strategic decisions-even though their expertise could surely benefit such discussions. In time, some firms became more accepting of risk management and the function received some C-level representation as risk managers transformed themselves into chief risk officers or, more commonly, chief financial officers took what they could learn from the risk management department and brought it to the CEO and the board.

Even now, risk management does not always have a clearly defined presence at the top level of enterprises. Why should it? After all, for most risk managers to become the chief risk officer, or its equivalent, one must carve away authority from whoever else already has it. But no self-respecting CFO would give away a critical component of his or her reason for being, so risk practitioners find their best opportunities to expand their mandate in times of crisis, under reactionary circumstances and amid a sense of urgency, perhaps even panic.

These are not the ideal conditions to further the evolution of a discipline as important as risk management, yet we have seen exactly that for the past decade. After all, the great advances in risk management did not occur during the salad years of the 1990s' market booms. They have occurred in the wake of the disasters that followed. And they have shown that risk managers are still regarded as a largely unwanted resource-until they are absolutely needed. No wonder why so many enterprises repeat their failures.

But What About ERM?

Isn't this supposed to be the next big thing for risk management? It is, and rightly so. Just as risk management as we know it today was the future of insurance management, ERM is the future of risk management.

Enterprise risk management entails a quantum leap forward in how risk awareness factors into the tactical and strategic decision-making of any enterprise regardless of size, scope or industry. ERM is the way for any operation to discuss risk frankly and openly across all of its own internal divisions, making truly informed choices on how that risk must be handled. And yet, for all of this, ERM is very incomplete.

To begin with, there is still no single definition of ERM. There are some very good ones out there, but no one definition unifies the global discussion on what ERM is and how it should be carried out. This is a problem, especially since it is easy to see that ERM means different things to different organizations when examined on a micro level. It is a methodology that adapts to those using it to the point where even companies with advanced ERM programs cannot truly make, as they say, an "apples to apples" comparison of what they have accomplished. ERM is simply too amorphous to allow for that.

It might not always be this way. But as long as it does, ERM will have a hard time becoming that glue that binds all risk professionals under a single philosophy on how their discipline should factor into the very DNA of business operations.

Separate But Equal?

For some time now, there have been two different groups of professionals who use the term "risk management." First are those who we might consider to be "operational risk managers." They handle insurance programs, as always, but also address the many other risks that threaten to keep the operation from carrying out its daily business. Among the operational risk manager's chief concerns are legal liabilities, worker safety, crime prevention, fire prevention, environmental contamination and many other important duties.

The other group of people who engage in risk management are those who we might consider "financial risk managers." They primarily come from the financial or auditing side of the organization and concern themselves with portfolio risk, credit and currency risk, market risk and other similar fields.

These are essentially twin disciplines running parallel to each other, both using the same term to define themselves, and neither really doing a whole lot to speak to the other side of the aisle. For operational risk managers especially, this is a problem.

In the last 12 months, as the global credit crisis has dominated business media coverage, the term "risk management" has been used time and time again by mainstream outlets in reference to financial risk management with no regard for the possible confusion between financial and operational differences. And while one can appreciate how the financial risk management discipline can use this crisis to address how systemic failures of risk management toppled the financial services industry to begin with, it becomes a reason for the operational risk manager to feel cast off. After all, with so much time and energy going into solving the epic problem of the credit

crisis, how much importance can senior leadership really give to problems such as terrorism, hurricanes and pandemics? Don't operational risk managers know that there is a real crisis going on here?

An easy way to address this would be to focus on the divisions between operational and financial risk management. One side could try to compete with the other to acquire the C-level recognition and resources needed to make their own mandates work. But that is no way to deal strategically with the kinds of risk that all organizations face in the 21st century. What is needed, really, is an extension of the ERM mode of thought.

ERM, of course, strives to break down the silos within an organization so that all departments, and all levels within those departments, have an equal understanding of- and stake in-the risk management process. When everyone from the night watchman to the CEO feels that they must be equally invested in the identification, analysis, appetite and management of the organization's risk, then risk is being handled in a way that is exponentially more effective and proactive than the traditional model of letting the risk manager buy insurance and attending periodic meetings with other department heads when questions arise.

But how can an organization create seamless and universal risk management within an organization when there are silos within the discipline itself? How can any organization truly say it understands its risks-let alone is able to manage them-when it speaks of risk management with two different voices? It cannot. And for anyone professionally charged with managing risk, this is the great problem that must be solved in order to drive the discipline further.

There must be a unification of these disparate fields. Those who practice risk management, regardless of which side of the historic classification they fall on, must find some common ground on which they can work together. They must understand each other's priorities, devise ways of lending one side's strengths to the other and, in time, create a fusion of skills and mindsets that leads to one important thing: risk management without qualifications, caveats or asterisks.

All of this is easier said than done, but it makes it no less necessary to accomplish. It will require rethinking how risk is managed within organizations, who owns it and who must champion its management. It requires an understanding of where operational risks and financial risks intersect-for there lies the first opportunity to blend together this divided discipline. It will require unquestioned and unqualified C-level command of all business risk. And it will require the various trade groups who serve risk

professionals of every kind to come together and find some way to unify their efforts for the improvement of every kind of enterprise in every industry.

This all could take quite a bit of effort, especially since it would require so many individuals with so many different interests to put a lot aside for the sake of a common goal. But it must be done or else the catastrophes of the past will continue to wreak havoc on the very enterprises that could withstand them if only they had the unified sense of mission to do so.

E a nova ISO 31000?
Como se enquadra em todo esse contexto discutido no artigo?