IBM Global Services
Thought Leadership White Paper

September 2010

Lucky fools, villainous scoundrels and unsung heroes in enterprise risk management

Clearing the clouding factors of risk to optimize ERM

IBM

Contents

Executive summary

Panic. Chaos. Pain. You are terrified. Your stomach is sick. Maybe the enterprise has lost millions. Perhaps employees or customers have been injured or killed. Maybe you or even hundreds will lose their jobs. Maybe it wasn't even your fault. But so what? Something terrible has happened, and you are dealing with it now.

Enter the risk event: something big and bad that struck your enterprise. Perhaps it was a catastrophic event caused by nature or unforeseen problems. Maybe your organization suffered through its own version of an underwater oil well explosion. Or maybe your business is just plain old tanking. It doesn't matter. It's here now. And the reasons for why you didn't see it coming are completely clouded over.

Worse yet, when there is no mechanism to plan for risk, there can be no preparedness. There are only the lucky and the unlucky. When organizations decide or opt to not prepare, the risk event can come at any time with the same devastating effect.

Here lies the challenge for almost all enterprises: How do you instill a risk management program that is prepared to deal with risk events and that ultimately learns from mistakes? Managing enterprise risk is a critical and growing discipline within leading organizations. Doing it right is difficult and there are many "clouding factors" that could sabotage good enterprise risk management (ERM) at every step. But doing it well may ultimately determine if your organization—and especially you—will be seen by the world as a hero (unsung or recognized), a lucky fool, or the worst of villains.

Understanding and correcting common misfires in ERM

The practice of enterprise risk management is too often misunderstood, pigeon-holed, underinvested in, or mystified at many organizations, yet it is the very practice that can prevent the large-scale damages that risk events can deliver. Perhaps the term's heritage in financial management, investing, or actuarial practices has minimized understanding to be limited to compliance, controls, and audits. We believe the scope of ERM is much bigger, more systemic and structural, and merely misunderstanding its definition is but the smallest challenge.

In recent memory, we've seen major risk events severely cripple or wipe out companies:

Risk Event	Outcome
2001: Energy giant fraud The company went through a financial scandal and suffered one of the largest corporate bankruptcies in U.S. history, causing shareholders to lose $11 billion.	
2002: Big 6 accounting firm brought down The firm was found guilty of criminal charges, consequently sentenced to five years' probation, was fined $500,000 and ultimately destroyed by the event.	
2004: Major retailer has employee trouble In one of several class action suits against the company, the retailer paid millions of dollars to thousands of employees in a single state for forcing them to work through breaks and work extra hours without pay.	
2006: Food company suffers outbreak The company issued a massive recall on bagged spinach after an E. coli outbreak in over 27 states, leading to consumer deaths and financial losses for California farmers of up to $74 million.	
2007: Toy company recall The company recalled nearly two million toys due to high levels of lead content in paint, ultimately paying $2.3 million in fines, and writing off millions of dollars of inventory.	
2008: Banking industry on the edge of systemic failure Large financial institutions collapsed during the peak of the financial crisis as a result of write-offs of bad debts and poor investments, forcing a multibillion-dollar-government bailout.	
2008: Electronics retailer bankrupt The company did not recognize fundamental changes in shoppers' buying patterns and migration to other formats and filed for bankruptcy, liquidating its stores in 2009.	
2009: Major auto manufacturer fined for product defect The manufacturer was fined $16.4 million after waiting months to recall 2.3 million vehicles because of "sticky pedal" defects. In addition, lives were lost prior to the recall and the recall itself cost millions along with substantial erosion of consumer confidence in the brand.	
2010: Mining company suffers explosion Despite a history of safety violations and fines of over $382,000, practices did not change substantially and a large explosion killed 25 miners.	
2010: Oil company well disaster The company was unprepared for the 2010 Gulf of Mexico well disaster that continued to threaten the company's survival. The explosion resulted in loss of life, environmental destruction, and damage to private property.	
Key: Significant financial loss; Loss of life; Environmental or societal damage; Reputation severely damaged; Destroyed company	

There are three major ERM misfires at most enterprises:

1. **"Doesn't get it, doesn't do it":** not understanding the true scope of risk management and ignoring important aspects because the costs aren't explicit until the worst happens.

2. **Clouding factors inhibit organizations from achieving successful ERM:** not being able to see and/or assess the risks facing the enterprise.

3. **Organizations fail to effectively shine light on the clouding factors and bring the ERM program to life:** inability to undertake key steps that "scatter the clouds."

Is risk management everything?

When discussing enterprise risk management as a primary function of business decision making, we can easily expand the definition to include all outcomes of decisions, both good and bad. In this sense, we could explore expansive terms such as "opportunity management," "decision management," or even "chance management." In some situations, the utility of this expansion may be desirable (it is certainly provocative), but in our immediate imperative to minimize the effects of negative risk events, and for the focus of this paper, we will tighten the scope of ERM to include only the negative outcomes of business decisions or the absence of such decision making.

"Doesn't get it, doesn't do it"

Risk events are the terrible things that happen to businesses that cause the destruction of value, competitiveness, capital, or even cause harm or loss of life. They can be large and externally driven, such as an unexpected natural disaster or the malicious sabotage of a product. They can be internally driven through mistakes, misinformation, poor design, inadequate safety systems, lack of skills, bad purchasing decisions, bad operational actions, bad financial or infrastructure/asset decisions, poorly received or delivered communications, failed product launches, or deliberate misbehavior. There are few business functions that escape exposure to risk.

Much of what constitutes a risk event and its poor management when it occurs is a product of misguided or misinformed business decision making (i.e., *mistakes*). The business of avoiding mistakes and making good decisions is the realm of ERM.

Here lies the first misfire of organizations when it comes to risk management. Organizations don't understand ERM's scope; they *don't get it*. They fail to see its sheer influence and pervasiveness to the core of nearly every business function, at every moment the business is operating.

Most organizations spend little time thinking about risk during periods when the organization (or a competitor) is not immediately struggling through a particular catastrophe. When things are sailing smoothly, the specter of a risk event is

a non-thought. When the organization should be planning, predicting, and preparing, it is often asleep at the wheel. The organization *doesn't do it*.

It is during these times that organizations typically have their fate in their own hands. Some prepare, some don't. Some get lucky and others get slammed. The question to the decision maker is this: "What position do you want to be in when the risk event happens?"

For those that prepare, they can avoid, prevent, or minimize the impact of the risk event whether it happens or not. The one who prepared and managed the risk successfully wins, hands down, and is the hero. The "unsung hero," the one who prepared but didn't experience a risk event, may be accused of wasting resources, but at least they were expended within a plan the organization could live with. His or her ERM actions may have also prevented an internally occurring risk from happening, either by squelching a chain of mistakes or putting in the right safety, mitigation, or prevention measures.

Let's say you have bad luck and didn't prepare. You might have cost the organization millions or lost hundreds of jobs. Being unlucky and unprepared makes you a villainous scoundrel. Like in our opening scenario, it doesn't matter if it was on purpose or your fault: you take the blame and suffer through the consequences.

Is it desirable to be lucky and unprepared? Maybe. You didn't have to work on preparedness and you escaped. In the recent Gulf of Mexico oil well explosion, it is seldom asked whether other oil companies were more careful, better prepared, or just plain lucky an explosion didn't happen on their watch. Luck is arbitrary, and, over time almost everybody will be unlucky at least once.

Many organizations don't know whether preparation is worth it or not. But in the plainest terms, failed ERM—through the occurrence and the poor management of a major risk event—can ruin an organization.

Heroes and villains

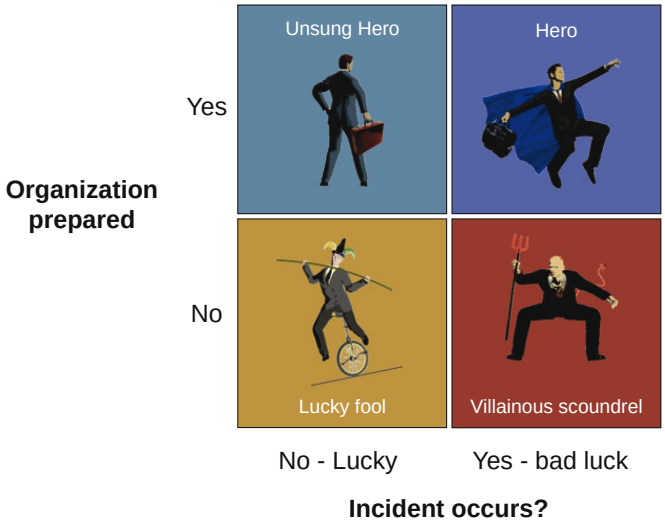

Image inspired by "Integrating Cost and Performance Management with Risk Management" by Robert Torok and Frank Wood, Cost Management, September/October 2006, pp. 36-40.

Anecdotes and hearsay: Have you seen these characters?

We can think of these recent stories in terms of our fools, heroes and villains:

Villainous scoundrel: Who was in charge of making sure the levees could withstand a category 4 or 5 hurricane in Louisiana prior to Hurricane Katrina? Experts sounded the warning for years, yet preparations were never made.

Unsung hero: Two-thirds of one of the most densely populated areas on earth is extremely vulnerable to flooding, but we hear few disasters coming from the Dutch. Their dikes failed in a storm, too—in the year 1421.

Hero: GAP Adventures, an eco-tourism company operating in Antarctic waters, had a ship with 154 passengers hit ice in 2007, tearing a hole in the hull. GAP was prepared with their Critical Incident Management team that maintains mission critical operations, mobilizes incident response teams, keeps customers safe, and gets the business back on track. The incident was a panic, but they were prepared and persevered. Not only did they rescue 100 percent of the passengers and crew, their crack PR team and the transparency of their safety operations averted bad publicity.

Lucky fool: Is it you? Stories about who didn't prepare and had nothing happen don't make for frequent news headlines. It's only when lightning strikes that the comedies and tragedies of business finally come to light.

As ERM program costs are typically miniscule in comparison to the massive losses from large risk events—barely described as rounding errors compared to the survival of an enterprise—we wonder why it is so hard to figure out the value of ERM. The cost of preparing for an event is usually both small in relative terms and readily incorporated into period budgets and business plans, while the cost of non-preparation is virtually infinite.

Perhaps people don't like to talk about bad things. Perhaps they lack imagination. Perhaps it's seen as too pessimistic or anti-progress or counter to team spirit. Whatever the case, knowing the scope and value of ERM, and ultimately doing it at the right time may make the difference between prosperity and survival versus emergency and disaster.

Seven factors inhibit organizations from achieving successful ERM

Characterizing risk events and bad decision making may be one of the most important steps in raising a new meaning and significance to ERM. The less we understand about risk-event creation, the less we are prepared to act. There are seven *clouding* factors typically experienced by organizations that inhibit the detection, mitigation, and management of risks.

The Seven Clouding Factors of Enterprise Risk

The unpredictable

Many of the highest profile risk events have been characterized as "black swan" events: sudden, random acts of unknowable disaster that were perceived to be beyond our control or general predictive abilities. Examples include major weather events such as Hurricane Katrina or the tsunami of 2004. Events of this order may seem too big and impractical to try to tackle for any one organization or enterprise, but as we will discuss, the black swan event's damage to an organization is primarily driven by its handling of the crisis. And yet, we believe that most so-called "black swan" events were indeed known about ahead of time, or could have been known with reasonable forethought and planning.

In addition, many risk analyses calculate the cost of risk in a way that may be detrimental. They simply calculate the cost of the risk event and multiply that by the likelihood of it happening. For example, if a risk event is estimated to have an impact of $10,000,000 but is only one percent likely to occur, most risk analysts would record an expected loss of only $100,000, an amount that may be very manageable and acceptable without further action. But in reality, the impact of the risk event will be *either* $0 or $10,000,000; therefore the organization must decide if a loss of that magnitude is acceptable, a very different question from assessing an expected loss of only $100,000.

Chains of mistakes

Many catastrophic risk events are generated within the organization by business decision makers. They are often chains of little mistakes that people either miss, ignore, or compound by letting them persist and then make other mistakes on top of them. The recent oil well explosion, the Ford Pinto, Three Mile Island, and the auto "sticky pedal" recall are all cases where it took a great many smaller mistakes before the large strategic crisis was recognized and action taken.

Organizations let mistake chains happen for many reasons. Sometimes it is a lack of oversight or coordination on the part of different stakeholders or actors within a process. Sometimes there are perfectly good processes in place to prevent mistakes, but they are overridden all the same. In other cases, an organization's culture may interfere where authority isn't questioned or critique is not freely heard.

Quantification and subjectivity

Success in risk detection often depends on how quantitative vs. subjective its detection is, and how frequent or routine the occurrence of the risk event. Some risks can be measured in hard numbers, especially ones that are frequent (e.g., every week, every quarter), and therefore can have very formal risk management programs assigned to them. In areas where risk is relatively routine, such as consumer defaults on payments or credit card fraud, the risk programs become business-as-usual functions and likely not thought of as ERM.

But consider an example where the specific risk is not known. A large, international shipping company must deal with the known risk of airplanes in its fleet breaking down. It is known with near statistical certainty that there will be a breakdown every night. But since decision makers do not know *which plane or which location* will be in need of an emergency replacement aircraft, they cannot plan by location. It is too expensive to retain substitute aircraft or outsource shipping to other carriers. They solved this risk challenge by having two aircraft do nothing every night but circle the continent empty, waiting to be deployed to the location of the grounded aircraft. This ensures that local relief will only be a couple of hours away, thereby managing a quantifiable risk that occurs more like a subjective event.

Long time frames

The role of time, especially long time frames, may be the most confounding and elusive dimension of risk management. Organizations are typically much better at managing risks that are recent and/or frequent. Risk events that occur over long time frames, such as five, ten or

twenty years seem to slip from institutional memory quickly after they happen and those that take decades to manifest are equally difficult to detect and manage.

Consider the procurement of longer-term assets or infrastructure. When a facility location is being assessed for suitability, the evaluators typically can only take a relatively short-term view of the possibilities for the location. They may look at current employment rates, how safe or secure the location is, or real estate prices. But the reality is that the decision is typically made with the lessons from the last decision forgotten or not measured, and without a thorough analysis of the possible long-term changes that might happen. Will the city deteriorate? Will the population mix change? This long-term view of risk is rarely measured for past decisions nor is a process established to measure the decision going forward.

Gradual shifts

Many risks, such as those due to market shifts or changes in competitive structures, materialize slowly and thus catch organizations off guard. For example, slow declines in market share are often ignored as being minor, temporary, or reversible with the *next big thing*. But these are as dangerous as sudden risk events, and often are only addressed once the organization is in crisis mode. Many of the seemingly inevitable bankruptcies or loss of business we see are quickly blamed on shifting markets and tastes. But the real issue is that they were ignored for years. They should have been dealt with, within the scope of decision making, and hence, ERM.

Mistake chains, subjectivity, long time frames, and slow shifts can all be inadvertently exacerbated by an enterprise's incentive structure and culture. These forces are the human actions that help manifest failure.

Incentives

Performance reviews and incentives, be they commission or bonuses are typically based on short-term performance. As a result, most managers and executives are looking towards the period's performance to gauge their prospects for advancement and reward, a situation amplified by seniority (in title) as the proportion of total compensation delivered through incentives becomes ever greater. This structure can create cultural environments conducive to seeking super-sized rewards. During the recent mortgage subprime crisis, one banker remarked, *"What's the worst that can happen? We make $200 million and then we get fired."*[1]

Another implication for short-term incentives is the drive to meet monthly, quarterly, or annual targets that have been communicated to stakeholders. Consider the "hockey stick" progression in forecasts by sales units that have to hit quarter- or year-end goals. The likelihood of them overpromising results or underpricing to their clients in order to get the sale raises the risk of, in effect, meeting the current period target at the expense of the next one and/or having an unprofitable sale simply to be able to record that sale.

There are also strategic or operational incentives that have less to do with personal or unit performance than in meeting enterprise goals. Despite having the necessary or right-minded goal to reduce costs or streamline operations, an enterprise may neglect to see how these changes could affect the organization's risk profile. For example, it is not unusual to try to minimize training expenses to improve profitability. But the unintended consequence may be increased risk when the trainee is sent to work without proper skills. At best, the skills shortfall may just drive inefficiency as the employee learns on the job, but at worst it may increase the number or magnitude of mistakes made, perhaps leading to property damage or loss of life.

Culture

An organization's culture may also reduce its ability to successfully detect, mitigate, and respond to risk. The tracking of mistakes or measurement of past decisions may seem to be a waste. Many leaders prefer *not* to spend large amounts of time reviewing their past failures and do not want a continual spotlight on them. Others may find risk planning to be hypothetical or theoretical. Some may not like the sense of negativity or the focus on failure, instead preferring optimism. With past mistakes out of mind, and future mistakes not thought of, it is all too easy to rely on the optimistic or statistically driven position that "such and such has not happened before or will not happen to us."

One executive of a Fortune top 20 company said "In a culture of 'got to look good', there are no risks."

In most cases, risk events are typically not the result of a single clouding factor, but rather a complex mix of many, making risk management a more complicated enterprise challenge. The good news about understanding the "clouding" factors of ERM is that their antidotes become easier to identify and obtain.

Shining some light on ERM

Organizations that take specific actions to build or improve their ERM programs are better positioned to survive and manage risk events, perhaps even prosper from them. Ultimately, ERM must take the form of a combination of capability, process, and discipline, each with its own set of techniques, experts, programs, and practices that are supported and invested in across the enterprise. It must be formally recognized as a distinct responsibility, having a pervasive influence across the enterprise, virtually embedded in every decision-making moment.

No enterprise can be perfect, and any that doesn't experience risk events is likely not taking enough risk to innovate and compete in the marketplace. With the inevitability of risk events, an enterprise risk management program cannot solely be founded on risk avoidance, but also on preparation for and management of events when they happen. Even if you are able to clear the clouds, you still must be prepared for lightning to strike.

If the clouding factors of enterprise risk handicap one's organizational ability to deal with risk, then a smart, proactive approach seeks their antidotes. These are the drivers of clarity, a clearing of the clouds to shed some light on the subject:

Antidotes

Managing risk events (MRE) and scenario planning

Typically, too much effort is expended on risk prevention and not enough focus is spent on managing risk events and building response, resiliency, learning, and feedback mechanisms. In a reversal of our ERM acronym, we introduce the term MRE or "managing risk events." Most risk management programs only focus on activities that seek to mitigate or prevent risk. Since risk events will happen despite the best efforts to prevent them, MRE is necessary to be able to react and recover, and then learn for the future when they

do occur. The costs of unused MRE processes and actions are known, measurable, and able to be planned for: i.e., the expense of preparation is part of the period budget, whereas the cost of needed but nonexistent MRE processes and actions can be catastrophic.

For example, in 2008 oil prices spiked, prompting a major airline to hedge a substantial portion of its 2009 fuel purchases by locking in a large quantity at a fixed price. Within a fiscal quarter, as oil and fuel prices plummeted, this hedge, which was lauded by the media at the time of the purchase, turned into a disaster and required a multimillion dollar write-off. Despite this decision having substantial negative results, the MRE in this example (the hedging program) was planned for with known, manageable financial implications—in a sense, it didn't cost anything that the company had not already planned for. If the opposite occurred—if the company had not hedged and oil prices continued on their 2008 trend—the costs would have been unknown, unplanned, and possibly catastrophic to the business.

Predictive analytics for risk

The use of data analytics to analyze, measure, model, and predict risk is a growing capability among leading enterprises. These new tools can add a sophisticated advantage in avoiding, detecting, and responding to risk in many categories.

Decision controls

A risk monitoring program should be put into place, using a comprehensive set of key performance indicators (KPIs) or key risk indicators (KRIs) to measure both the impact of risk events and any associated mitigation efforts. These are the *decision controls* used by management and employees alike to understand risk events.

In managing the enterprise "at rest", i.e., during noncrisis times, the steps of monitoring, reporting, and reviewing should be to assess whether chains of mistakes may be occurring, and/or whether the likelihood of risk events is changing, with the objective of preventing them from ballooning into full-blown crises. Positive efforts towards breaking mistake chains should be perpetual and persistent such as through a rigorous analysis of causal factors that may influence future risk events.

When a crisis does occur, the MRE "function" should be able to snap to attention like a prepared emergency organization (think of firemen waiting for an alarm). While managing the crisis, getting the business back on track and recovering from the event will be the top priority, it is critical to later use the event as a learning point for future planning.

Comprehensive analysis

The ERM process starts with "identify," a listing and categorization of possible risks that could happen under any reasonable set of circumstances. It is important during this step to be expansive and exhaustive in considering different risks. Risk analysis should extend beyond what happened or what is planned to happen to include what *could* happen. Virtually no risk should be ignored as being too unlikely, too preposterous, or too devastating. Arguments of authority and emotional critiques should be ignored. The value in this step is in understanding what can or might happen and performing the proper analysis of how to avoid or prevent the potential risk event and, failing that, how to prepare for it, including its financial or emotional justification (e.g., "Failure is not an option").

A risk assessment should take the form of a report or written analysis that is used to assess and plan for the risk. Risks can be assessed for their likelihood, impact, and the relative costs to either absorb the risk and/or the costs of investing in MRE tactics (be they assets, safety systems, redundancies, relationships, etc.). In this analysis, risk events that have massive impact should be prioritized highly. All risks should be measured on three key dimensions: likeliness of occurrence, impact if the event occurs including response and recovery efforts, and cost of preparation/prevention. This becomes a method of prioritization for planning, and the basis for a risk scorecard.

The risk scorecard may have information such as basic risk information, expected risk, different types of controls, potential impact, opportunity to mitigate, cost of mitigation, and recovery requirements.

The output of this analysis should result in a risk "playbook." Just as a sports team develops a playbook to deal with different contingencies and challenges posed by a defense or offense, the organization should have one to follow in case the risk event seems to be approaching or occurs. The playbook will have both specific actions that need to be taken, as well as governing instructions to guide flexible decision making to respond to and mitigate the impacts of the crisis if it occurs in a manner different from what was expected.

Institutional memory

Upon dealing with a risk event (successfully or not), risk managers must be able to look all the way back in the process to the "identify" stage to see how accurately they identified and planned for the particular event, including what the real impact and costs were. The knowledge around the risk event must be stored in a formalized record of institutional memory, and act as an input to review and revise other related risk analyses, playbooks, and deployments.

In risk planning, managers should develop long-term views of the business forward and backward, i.e., extending the time horizon of risk management substantially beyond the immediate future. The intent should be to reverse the instinct to only examine recent history and only look into the next period or two.

Risk events are either anticipated or unanticipated (sometimes called the "known unknowns" and "unknown unknowns"). When risk events that are wholly unanticipated occur, this should prompt the organization to evaluate why they didn't see it coming and to widen their view of risk to be more expansive. When anticipated risk events occur, the questions are two-fold: First, did we foresee the event reasonably accurately, and second, did we reasonably estimate its impact? If the answer to either question is negative, the organization needs to treat the event as if it had been an unanticipated event.

When examining the past, it is more important to examine the validity of the assumptions that were used rather than the decision itself. Even the most carefully made decisions can be wrong if their underlying assumptions or facts were incorrect. Achieving this will likely require a different approach than merely relying on memories and personal experience.

An institutional memory must be codified in a formal way in a system, complete with its own formats, procedures, update processes, and incentives for use. The institutional memory must also forgo bias, flattery, and revisionist history. The bad stuff that happens—despite being painful to examine and remember—is extremely valuable.

Trend evaluation

Making decisions about slow-moving trends must be included in any risk analysis. Like the proverbial frog in water that is slowly brought to a boil, decision makers can't sit idle while their environment changes. They must scrutinize long-term business trends such as customer taste, competitors, rising technology, new products, or channel innovation, just like any other potential risk event.

Risk-adjusted incentives

Incentives—be they in the form of personal compensation or in stated corporate goals—should also be subject to scrutiny for risk. When creating incentives, the objective is usually to drive certain action or behavior. A sales incentive is to drive more sales, an enterprise performance goal is to drive better results, and a cost-reduction goal is to reduce expenses. When any of these types

of incentives are designed, managers must look not only to the first degree of expected outcome—i.e., the target itself—but to the chain of possible secondary and tertiary impacts, i.e., the ripple effects. In this analysis, they must look objectively at the possible negative outcomes, often analyzing a much larger set of possibilities than merely the planned good outcomes.

Collaboration culture

Successful ERM and MRE programs, as described here, need to become formal responsibilities within the enterprise. The ERM function will require authority to establish risk tolerance, implement prevention, mitigation, and recovery practices, perform reviews, provide guidance, and issue corporate policy. It will rarely be a complete clearinghouse or authority on all business decision making, but instead provide guidance, tools, and practices on how decisions should be made. In this respect, it should be seen as more a *center of excellence* than a ruling body or service bureau for vetting business decisions.

As an organization shifts its culture to one better suited for managing risk, the ERM team can provide guidance on how this should occur. Actions such as reversing authoritarian arguments, openness to far-flung possibilities, and honest review of failures may take some significant reconditioning of behavior that will require investments in communication, training and executive advocacy.

Conclusion

So who are you? A lucky fool waiting to be vilified? An unsung hero waiting to be justified? Risk events happen, and most of them are substantially within the control of the decision makers in the enterprise. Risk is constantly "clouded," abstracted by time; snuck through chains of mistakes; ignored by the best and brightest; and even ignited through well-intended actions and incentives. The difference between those who fall to catastrophe and those who recover from them should not be determined by luck. Instead, a new view of ERM needs to be taken so that companies can clear the clouds, see risk in a new light, see the oncoming horizon better, and ultimately be ready to act when lightning does strike.

About the author

Robert Torok is an Executive Consultant with IBM Canada's Strategy & Transformation consulting practice. He is responsible for leading the development and delivery of enterprise risk management services for clients around the world, specializing in risk identification, management and mitigation, and the integration of risk and performance management. Mr. Torok holds an MBA from the Schulich School of Business at York University and is a Chartered Accountant in Canada. He is an author and frequent speaker on the subject of ERM in both Canada and the United States.

For more information

To learn more about enterprise risk management please contact your IBM marketing representative or IBM Business Partner, or visit the following website:
ibm.com/services/c-suite/insights

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
September 2010

[1] C. Gasparino, *The Sellout* (New York: HarperCollins, 2009), page 195.

Please Recycle

CIW03073-USEN-00