

**IBM Institute for Business Value**

# Clearing the clouds

*Shining a light on successful Enterprise Risk Management*



---

## IBM Institute for Business Value

IBM Global Business Services (GBS), through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive report is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM GBS to provide analysis and viewpoints that help companies realise business value.

You may contact the author or send an email to [iibv@us.ibm.com](mailto:iibv@us.ibm.com) for more information. Additional studies from the IBM Institute for Business Value can be found at [ibm.com/iibv](http://ibm.com/iibv)

---

By Robert Torok, Carl Nordman and Spencer Lin

**Risk is inherent** within every business ecosystem, adding to a multitude of existing challenges of operating in today's global business climate. The threat of catastrophic loss, from terrorism, natural disasters, financial mismanagement, IT security breaches, supply chain disruptions and more, demands preparedness to assure financial and business continuity. Yet recent studies suggest few companies fully understand or are properly prepared for the breadth of risks they encounter. Historically viewed as the domain of the Chief Financial Officer (CFO), less than 20 percent of enterprise risks are financial, legal or compliance in scope, yet all risks can ultimately have a financial consequence. Addressing the scope of Enterprise Risk Management (ERM) requires a level of organisational collaboration that culturally and practically can be very difficult to implement. The first step toward creating a robust ERM programme encompasses understanding the scope of risk management and nurturing collaboration and preparedness – making it a 'team sport' across the enterprise.<sup>1</sup>

### Executive summary

Risk events are occurrences – catastrophic incidents caused by nature, terrorism, financial fraud or other problems – that can dramatically impact your enterprise's ability to achieve its objectives. They can damage reputation, market capitalisation or other key aspects of your business. When no mechanism is in place to plan for risk, no preparedness is possible. While some companies have been moving toward implementing more formalised ERM programmes, establishing a Chief Risk Officer position, investing in systems, analytics and data management and hiring necessary talent to perform analysis, predict and quantify risk events, the vast majority are far behind where they need to be. What is hindering their ability

to make necessary progress? It comes down to a few simple things: properly defining the scope of ERM, establishing enterprise risk tolerance and driving a culture of sharing risk-related information.

The challenge for most enterprises is how to implement an ERM programme, instill a culture prepared to deal with risk events and learn from inevitable mistakes. Managing enterprise risk is a critical and growing discipline within leading organisations. Doing it right is difficult; many 'clouding factors' can sabotage an ERM programme at every step. But doing it well may ultimately determine whether your organisation can successfully avoid and/or mitigate risks.

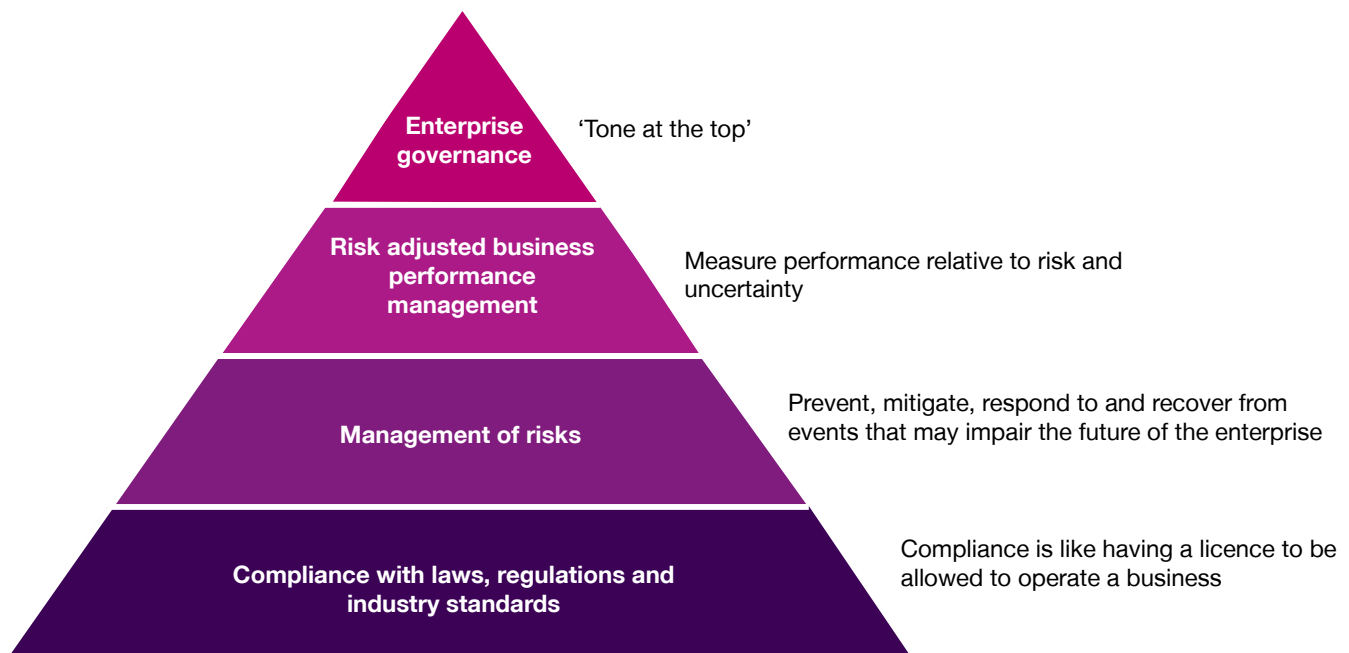
## Understanding and correcting common misfires in ERM

ERM is the practice that can prevent or mitigate the large-scale damages that catastrophic events can deliver (see Figure 1). ERM cannot be properly addressed by simply hiring a responsible executive and building a risk management department.

In most companies, this function historically has been largely the domain of the CFO and finance, based on the notion that most risk is financial and can be mitigated through controls. In certain industries, such as banking, financial markets and insurance, trading risk is the actual business, so the enterprise is focused on creating, selling, managing and servicing risk.




















But even in these companies, many lack a full appreciation for the broader scope of ERM that extends beyond their functional domain or the business they are in. Indeed, the empirical evidence suggests that less than 20 percent of risk that results in severe capitalisation declines is financial, legal or compliance that can be mitigated with traditional controls and monitoring.<sup>2</sup>

We believe the scope of ERM is much bigger, more systemic and structural. Merely misunderstanding its definition is but the smallest challenge (see Figure 1). In recent years, we have seen major risk events severely impact a number of companies in a wide range of industries, while other firms successfully avoided or mitigated the same risks (see Figure 2).



---

Figure 1: Scope of enterprise risk management.

Risk Event	Impact
<b>High tech companies – Earthquake</b> An earthquake causes power outages and damages equipment, thus creating a supply shortage of components for two high tech companies. One company changes its pricing strategy just in time to satisfy customers by influencing demand toward products with available components. The other company faces product backlogs due to component shortages and inability to alter product configurations.	 
<b>Food company - Outbreak</b> The company issues a massive recall on bagged spinach after an E. coli outbreak in over 27 U.S. states, leading to consumer deaths and financial losses for California farmers of up to £46.25 million.	   
<b>Investment bank - Mortgage risk</b> The company reviews the firm's full portfolio of mortgage risk. As a result, the enterprise reduces the bank's stockpile of mortgages and mortgage-related securities and buys expensive insurance to protect against further losses. While many of its competitors racked up huge losses with the onset of the credit turmoil in 2007, the company enjoys gains in share price during the year.	 
<b>Trading company – Currency crisis</b> When the Indonesia Rupiah devalues by more than 50 percent, many Indonesian suppliers are unable to deliver their orders to their U.S. customers because they are unable to pay for imported materials; however, this company adapts to the situation quickly by shifting some production to other suppliers in Asia and by providing financial assistance to those affected Indonesian suppliers to ensure business continuity.	 
<b>Mining company - Explosion</b> Despite a history of safety violations and fines of over £237,500, practices did not change substantially and a large explosion kills 25 miners.	   
<b>Electronics companies – Supplier plant fire</b> A small fire hits a microchip plant that supplies parts to two companies and the smoke and water damage from the fire contaminates millions of parts – almost the plant's entire stock. One company acts swiftly and moves to tie up spare capacity at other plants of the supplier and every other supplier they could find. It even re-engineers some of its products so it could take chips from other suppliers. The other company accepts assurances that the fire is unlikely to cause a big problem and waits it out. When it realises its mistake, it is too late. With no other source of supply, this company loses many months of production and, hence, many sales in a booming market.	  
<b>Shoe manufacturer – Intellectual property risk</b> When the relationship between this manufacturer and one of its suppliers goes sour, the supplier starts producing different types of shoes using a logo that resembles the manufacturer's design. The company files a lawsuit in the country without success.	 

 Financial risk
  Human risk
  Environmental/society risk
  Reputation risk
  Enterprise survival at risk

Figure 2: Examples of major risk events.

What is the common theme in these failures? A 2010 study commissioned jointly by IBM and American Productivity and Quality Center (APQC) found that more than two-thirds of the nearly 300 respondents had at least one significant risk event in the previous year and that only some 20 percent of organisations had both anticipated and reasonably estimated the impact of that event.<sup>3</sup> An earlier IBM study of senior financial executives also found the vast majority of major risk events had their roots in non-financial causes.

The Corporate Executive Board evaluated the root causes underlying market capitalisation declines for the top 20 percent of the Fortune 1000 from 1998–2009 (see Figure 3).<sup>4</sup> It found that strategic risks cause 68 percent of severe market capitalisation declines and pose a much more significant threat to companies than compliance and financial risks.



Note: Market capitalisation declines represent a drop in company share price of 30 percent or greater relative to peer group. N = 128  
 Source: Corporate Executive Board, with permission. From the Audit Director Roundtable of The Finance And Strategy Practice, www.adr.executiveboard.com. 2010.



Figure 3: Market capitalisation decline drivers (Top 20 percent of Fortune 1000 – 1998-2009).

Yet 56 percent of the IBM-APQC survey respondents identified strategic risks as being managed with the least mature risk management processes.<sup>5</sup>

ERM misfires at most enterprises are caused by three major factors:

1. **Organisations do not know what to do** – not understanding the true scope of risk management.
2. **Clouding factors inhibit successful ERM** – not being able to see and/or assess the risks facing the enterprise.
3. **Organisations fail to shine the light on the clouding factors and bring the ERM programme to life** – inability to undertake key steps that ‘scatter the clouds.’

### Organisations do not know what to do

Risk events are the terrible things that happen to organisations and cause the destruction of value, competitiveness, capital or even injury/loss of life. These events 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 or inadequate safety systems. Lack of skills, purchasing decisions, operational actions, financial or infrastructure/asset decisions, poorly received or delivered communications, failed product launches or deliberate misbehaviour can also lead to major risk events. Few business functions escape exposure to risk.

Much of what constitutes poor risk management occurs as a result of misguided or misinformed business decision making. Avoiding mistakes and making good decisions is certainly within the realm of ERM.

The first risk management misfire comes when organisations don't understand ERM's scope; they do not know what to do. They feel overwhelmed about risk management – its sheer influence and pervasiveness to the core of nearly every business function, at every moment the business is operating. In fact, more than half of the respondents to the IBM-APQC survey acknowledged having no enterprise-level process to identify risks.<sup>6</sup>

The question to the decision maker is this: 'What position do you want to be in when a risk event happens?' To determine this, organisations and risk managers must first accept that risk events will occur; an organisation may avoid them for a period of time, through luck or skill, but at some point negative events will happen.

Those that prepare may be able to avoid or prevent many risk events. Preparation can also limit the impact of unpredictable events and natural disasters. Being prepared also can help limit the potential for bad publicity and damage to reputation as news reports focus not only the impact of the risk event, but also the organisation's struggles to respond. For example, a ship owned by GAP Adventures, an eco-tourism company, hit ice in Antarctic waters in 2007, tearing a hole in the hull. GAP was prepared with a Critical Incident Management team that maintains mission critical operations, mobilises incident response, keeps customers safe and in touch with their families and gets the business back on track. The incident could have resulted in panic, but the company was prepared with a system in place for response. Not only did GAP rescue all 154 passengers and crew, but the company's PR team and the transparency of its safety operations averted bad publicity.<sup>7</sup>

The cost of an ERM programme pales in comparison to the potential massive losses from large risk events. The cost of preparing for an event is usually both small in relative terms and readily incorporated into period budgets and business plans. The cost of non-preparation can be so large as to cause organisational failure. 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.

### Clouding factors inhibit successful ERM

Five *clouding* factors typically experienced by organisations inhibit the detection, mitigation and management of risks (see Figure 4).

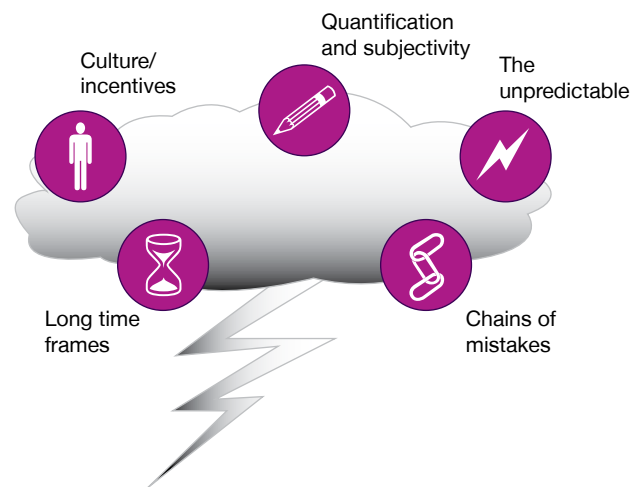


Figure 4: The five clouding factors of enterprise risk.

### Quantification and subjectivity

Success in risk detection often depends on how quantitative versus subjective its detection is and how frequent or routine the occurrence of the risk event. Some risks, especially frequent ones, can be measured in hard numbers (e.g., every week, every quarter) and can have formal risk management programmes assigned to them. In areas where risk is relatively routine, such as consumer defaults on payments or credit card fraud, the risk programmes 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 mechanical failure in its airplane fleet. It is known with near statistical certainty a breakdown will occur every night. But since decision makers do not know which plane or which location will be in need of emergency replacement aircraft, they cannot plan by location. It is too expensive to retain substitute aircraft or outsource shipping to other carriers. The risk challenge was solved by having two empty planes airborne through the night, available for deployment to any location. This ensures that local relief will only be a couple of hours away, enabling the management of a quantifiable risk more like a subjective event.

### The unpredictable

Many of the highest-profile risk events are characterised as ‘black swan’ events: sudden, random disasters beyond the ability to control or predict. Examples include major weather and natural events, such as hurricanes and tsunamis. Events on the scale of these may seem too big and impractical for an organisation or enterprise to manage. But, while the event itself may be beyond control, how the crisis is handled, often the biggest threat of organisational damage, is not. And except for completely unpredictable natural disasters, most so-called ‘black swan’ events can be anticipated ahead of time with reasonable foresight and planning.

In addition, many risk analyses calculate the impact of risk in a way that may drive organisations to deliberately not see such big or ‘black swan’ events. Many organisations simply calculate the cost (i.e., impact) 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 £6,250,000 but is only one percent likely to occur, many risk analysts would record an expected loss of £62,500, an amount that may be manageable and acceptable without further action. But, in reality, the impact of the risk event will be either £0 or £6,250,000; therefore the organisation must decide if a loss of £6,250,000 is acceptable, a vastly different question from assessing an expected loss of only £62,500.

### Chains of mistakes

Many catastrophic risk events are generated within the organisation by business decision makers. They are often chains of little mistakes that people either miss, ignore or compound by letting them persist. Then, on top of these, other mistakes are made.

Mistake chains happen for many reasons. Sometimes it is a lack of supervision or coordination on the part of different stakeholders or actors within a process. Sometimes perfectly good processes are in place to prevent mistakes, but, for some reason or another, are overridden or ignored. In other cases, an organisation’s culture may inhibit the questioning of authority or process critique.

---

*Many catastrophic events are precipitated by mistake chains, a series of small errors compounded and magnified over time.*

---



### Long time frames

Timing, especially long time frames, may be the most confounding and elusive dimension of risk management. Organisations are typically much better at managing recent or frequent risks. 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. 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 property 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.

### Culture/incentives

An organisation'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.'

Performance reviews and incentives, such as commission or bonuses, are typically based on short-term performance. As a result, most managers and executives are looking toward the period's performance to gauge their prospects for advancement and reward. This situation is 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. The tendency in such an environment is to focus on short-term results, not long-term risks. During the recent mortgage subprime crisis, one banker remarked: *'What's the worst that can happen? We make £125 million and then we get fired.'*<sup>8</sup> As one executive noted, 'In a culture of 'got to look good,' there are no risks.'<sup>9</sup>

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. However, understanding the 'clouding' factors of ERM makes their antidotes easier to identify and obtain.

### Shining some light on ERM

Organisations that take specific actions to build or improve their ERM programmes 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, programmes and practices supported and invested in across the enterprise. It must be formally recognised as a distinct responsibility, with pervasive influence across the enterprise and virtually embedded in every decision-making moment.

No enterprise can be perfect; innovating and competing in the marketplace creates inherent risk. With the inevitability of risk events, an ERM programme cannot be founded solely on risk avoidance, but also on preparation for and management of events when they happen.

If the clouding factors of enterprise risk handicap the organisation’s ability to deal with risk, then a smart, proactive approach seeks their antidotes (see Figure 5).

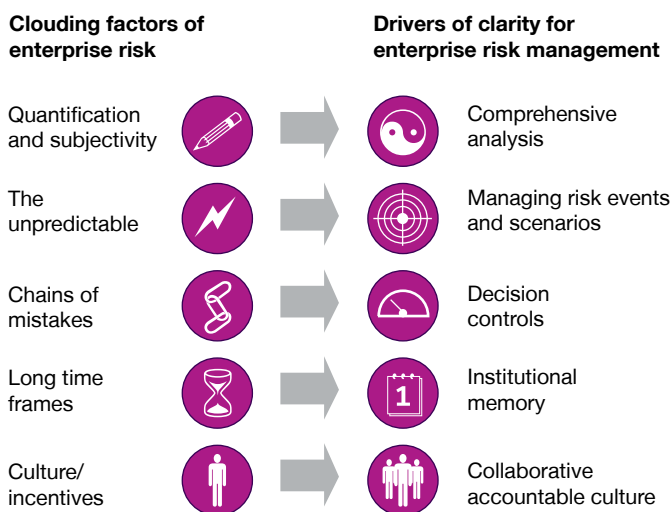


Figure 5: Antidotes to the clouding factors of risk management.

**Managing risk events (MRE) and scenario planning**

Much effort is expended on risk prevention activities and not enough on managing inevitable risk events, building response, resiliency, learning and feedback mechanisms. In a reversal of the ERM acronym, we introduce MRE, or ‘managing risk events.’ Most risk management programmes only focus on activities to mitigate or prevent risk. Since risk events will happen despite the best efforts to prevent them, MRE is necessary to react, recover and learn for the future. The costs of

unused MRE processes and actions are known, measurable and can be planned. For example, the expense of preparation is part of the period budget, whereas the cost of needed but non-existent MRE processes and actions can be catastrophic.

**Comprehensive analysis**

IBM GBS ERM practice has an ERM Solution in which it has incorporated a risk portfolio framework for inventorying ERM risk events to support comprehensive analysis, shown in Figure 6.

The process, usually triggered by the periodic setting of strategic and operational objectives, starts with ‘identify,’ a listing and categorisation 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: it must extend beyond what happened or what is planned to happen to include what *could* happen. Arguments of authority and emotional critiques should be ignored and virtually no risk should be ignored as being too unlikely, too preposterous or too devastating. 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. Even if risk events cannot be avoided or prevented, an organisation must understand, prepare for and evaluate the consequences of them, including financial or emotional justification (e.g., ‘failure is not an option’).

An organisation needs to take a very broad view of potential risks and build an ERM programme with the correct inventory and scope. One way to start defining that scope is to consider the example risk inventory presented in Figure 6.

IBM GBS has defined a framework for a risk portfolio within its ERM Transformation Methodology that organises risks into groups to facilitate appropriate and comprehensive analysis. First, external and internal risk factors are segregated between non-controllable and controllable. With each, risks are categorised for analysis. External risks, such as industry,

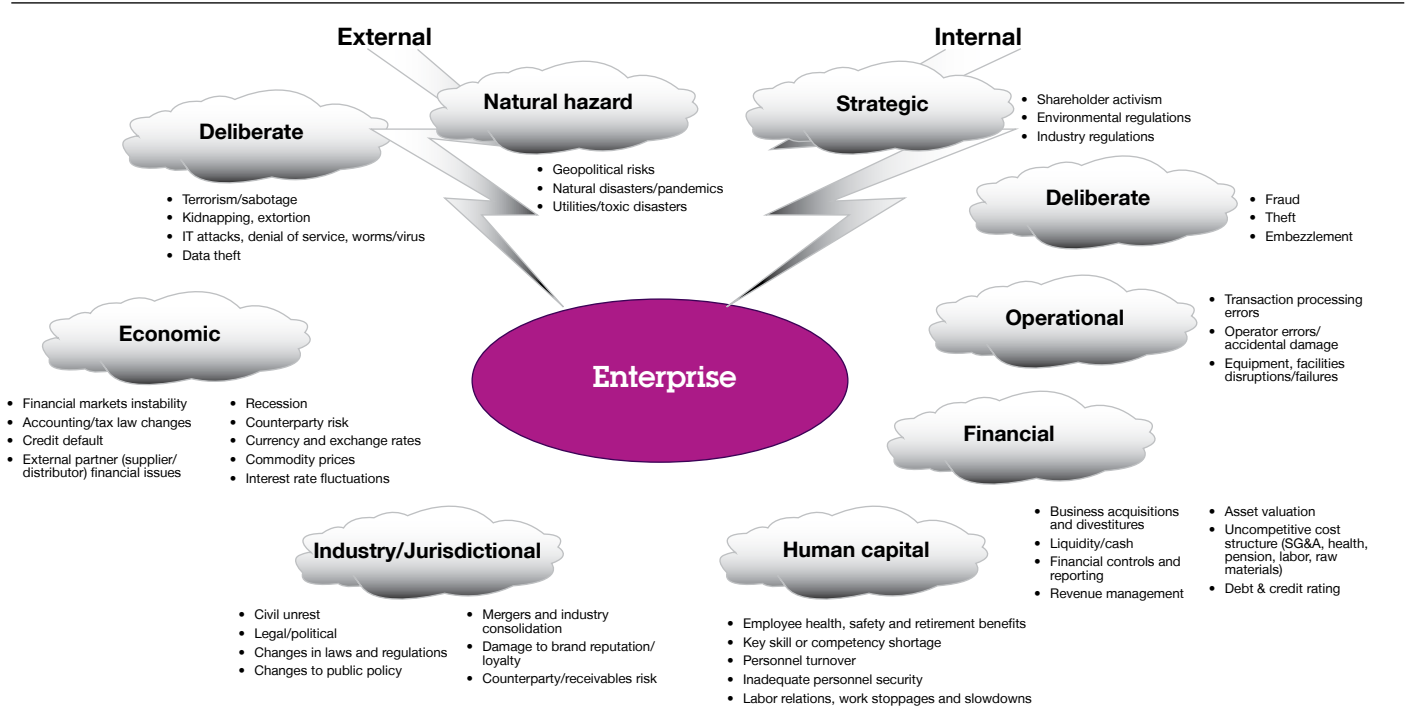


Figure 6: A framework to inventory enterprise risk events.

macroeconomic, deliberate and hazard, may drive different impacts to company performance and, hence, the MRE tactics. For instance, economic events that may impact revenue and supply chain costs may include interest rates, currency fluctuations and raw material costs. Proper modelling of the financial impacts of various scenarios can help plan for appropriate capital raising, hedging and inventory management. Internal risks, from strategic to operational, are similarly categorised to assess and develop mitigation approaches. For internal risks, fortunately, an enterprise can do much beyond preparation to actually mitigate those risks through controls, business execution and other efforts.

A risk assessment should take the form of a report or written analysis 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 (such as assets, safety systems, redundancies, relationships, etc.). In this analysis, risk events that have massive impact should be prioritised highly. All risks should be measured on several key dimensions, including likeliness of occurrence, impact if the event occurs (including response and recovery efforts), the cost of preparation/prevention and the speed at which the risk may emerge. This becomes a method of prioritisation for planning and the basis for a risk scorecard.

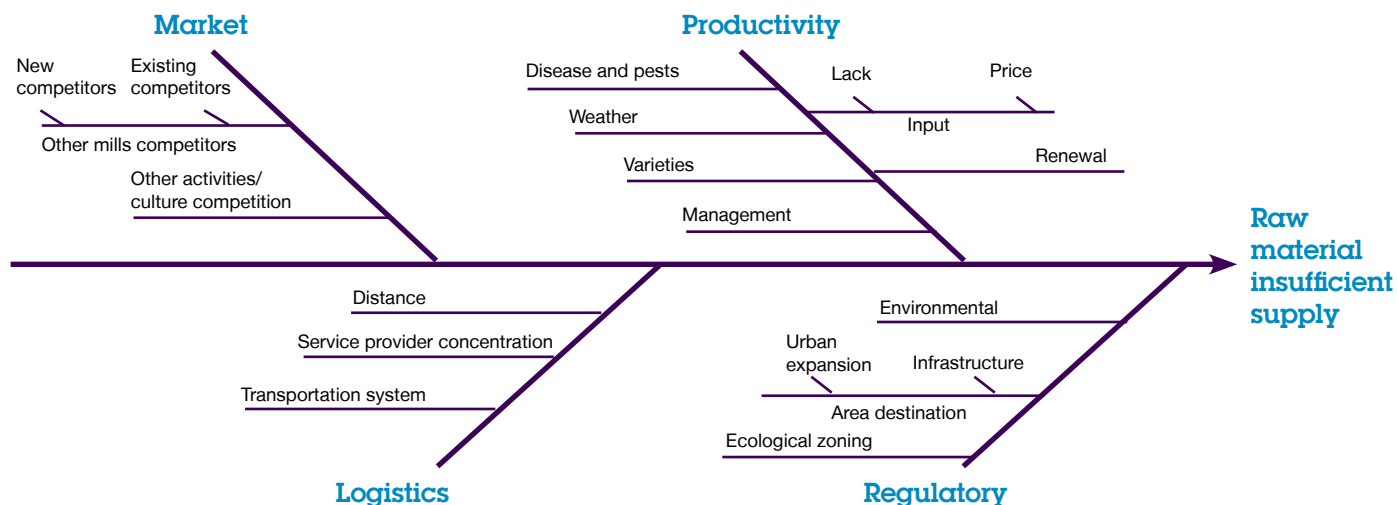


Figure 7: Example of risk cause and effect.

One approach to assessing risks and planning for their avoidance or mitigation is to undertake a root cause analysis. For example, a South American commodity producer undertook such a root cause analysis, as shown in Figure 7, relating to the insufficient supply of critical raw materials into its supply chain.

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 defence or attack, the organisation 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 differently than expected.

#### Expense preparation: Airline hedges fuel purchases

**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 had been 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 programme) 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.**

### Decision controls

A risk monitoring programme should be put into place that uses 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 both management and employees to understand risk events.

In managing the enterprise ‘at rest’, i.e., during non-crisis times, the steps of monitoring, reporting and reviewing should assess whether chains of mistakes are occurring and/or whether the likelihood of risk events is changing. The objective should be to prevent any events from ballooning into full-blown crises. Positive efforts towards breaking mistake chains should be perpetual and persistent, such as 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 organisation. 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.

The use of data analytics to analyse, 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.

For example, the South American commodity producer referenced earlier uses the following key risk indicators to measure the risk of insufficient supply of a critical raw material:

- Average duration of existing supply contracts
- Percentage of supply contracts maturing within a year
- Degree of supplier satisfaction
- Productivity loss related to pests and diseases.

### 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 spotted 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 formal 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 wholly unanticipated risk events occur, the organisation should evaluate why it didn’t see the event coming and widen its view of risk to be more expansive. When anticipated risk events occur, the questions are two-fold: first, did the organisation foresee the event with reasonable accuracy?; and second, did it reasonably estimate its impact? If the answer to either question is negative, the organisation 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 from merely relying on memories and personal experience.

As organisations perform this type of retrospective analysis, they must recognise that ERM programmes mature over several years; it is therefore extremely unlikely to get it 100 percent right the first time around. For example, a U.S. based software company reviewed its risk programme after one year of operation and found a number of risks that had been identified but were later seen as either very low impact or readily managed through day-to-day operations. The company also found it had experienced several totally unanticipated risk events. Being early in its programme, the company used this as a learning experience to improve its programme.

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 forego bias, flattery and revisionist history. The bad stuff that happens, despite being painful to examine and remember, is extremely valuable. Ultimately, this institutional memory helps create an ERM-enabled enterprise.

#### **Collaborative accountable culture**

Successful ERM and MRE programmes 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 will provide guidance, tools and practices on how decisions should be made. In this respect, it should be seen as more a *centre of excellence* than a ruling body or service bureau for vetting business decisions.

From several recent studies, it is clear that risk management has become a team sport, successful only when championed by the Board and C-suite of an organisation and supported by the entire executive team. While the senior risk executive of the organisation, whether or not titled as the Chief Risk Officer, may own and drive the process, the risks themselves are owned by the business units.

As an organisation 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.

To create success however, one final step is required and that is to align incentive compensation with the risks taken by the organisation. Specifically, the organisation must make sure that short-term results do not generate performance incentives until it is clear that those actions do not degrade its long-term success, in other words, accountability over a longer period of time.

---

*The ERM function should be viewed more as a 'centre of excellence' than an authority to review all business decisions.*

---

## Conclusion

What are your clouding factors of effective risk management? Is yours a culture of 'Got to Look Good'?  
What are the top three or four areas of risk exposure?  
Would any of these severely impair company financial performance or potentially lead to a severe market capitalisation decline?

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, emerging through chains of mistakes, ignored by the best and brightest and even ignited through well-intended actions and incentives. A new view of ERM is required to enable organisations to clear the clouds, see risk in a new light, have better long-term vision and, ultimately, be ready to act when lightning does strike.

To learn more about this IBM Institute for Business Value study, please contact us at [iibv@us.ibm.com](mailto:iibv@us.ibm.com). For a full catalogue of our research, visit:

[ibm.com/iibv](http://ibm.com/iibv)

Be among the first to receive the latest insights from the IBM Institute for Business Value. Subscribe to IdeaWatch, our monthly e-newsletter featuring executive reports that offer strategic insights and recommendations based on IBV research:

[ibm.com/gbs/ideawatch/subscribe](http://ibm.com/gbs/ideawatch/subscribe)

## About the authors

Robert Torok is an Executive Consultant with IBM Canada's Strategy & Transformation consulting practice. He is responsible for leading the development and delivery of ERM services for clients around the world, specialising in risk identification, management and mitigation and the integration of risk and performance management. Rob 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. He can be reached at [robert.torok@ca.ibm.com](mailto:robert.torok@ca.ibm.com).

Carl Nordman is an Associate Partner with IBM GBS Institute for Business Value. He is currently the Research Director of the Financial Management Research Team, responsible for developing and deploying research-based thought leadership for Finance and the office of the CFO. Carl has 24 years of experience in financial services, including 14 years delivering Finance and operations transformation consulting services to clients. The scope of Carl's experience includes all aspects of transformation from strategy and solution development through implementation. Carl holds a B.A. from the University of California, Berkeley and an MBA from the Yale School of Management. He can be reached at [carl.nordman@us.ibm.com](mailto:carl.nordman@us.ibm.com).

Spencer Lin is an Associate Partner in Financial Management in IBM Global Business Services. He currently serves as the Financial Management Global Business Advisor. In this capacity, Spencer is responsible for strategy development, planning, market development and solutions. He has a combination of financial management and strategy consulting experience over the past 16 years, with extensive experience in Finance transformation, strategy development and process improvement. He was a co-author of the 2005, 2008 and 2010 IBM Global CFO Studies. Spencer holds a B.S. from Princeton University and an MBA from Northwestern University's J.L. Kellogg School of Management. He can be reached at [spencer.lin@us.ibm.com](mailto:spencer.lin@us.ibm.com).



## For further information

For more information about this study, please contact one of our Financial & Risk Management leaders in your local geography:

### Global Business Services

#### Global ERM Center of Excellence

Robert Torok, [robert.torok@ca.ibm.com](mailto:robert.torok@ca.ibm.com)

#### Global and North America

William Fuessler, [william.fuessler@us.ibm.com](mailto:william.fuessler@us.ibm.com)

Spencer Lin, [spencer.lin@us.ibm.com](mailto:spencer.lin@us.ibm.com)

#### Northern Europe

Ian McMillan, [ian.mcmillan@uk.ibm.com](mailto:ian.mcmillan@uk.ibm.com)

#### Southern Europe

Philippe Bellavoine, [philippe.bellavoine@fr.ibm.com](mailto:philippe.bellavoine@fr.ibm.com)

#### Central and Eastern Europe, Middle East and Africa

Mark Ramsey, [mark.ramsey@cz.ibm.com](mailto:mark.ramsey@cz.ibm.com)

#### Asia Pacific and Latin America

Grace Chopard, [grace.chopard@au1.ibm.com](mailto:grace.chopard@au1.ibm.com)

#### Japan

Mie Matsuo, [miematsu@jp.ibm.com](mailto:miematsu@jp.ibm.com)

#### IBM Institute for Business Value

Carl Nordman, [carl.nordman@us.ibm.com](mailto:carl.nordman@us.ibm.com)

## The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment. Through our integrated approach to business design and execution, we help turn strategies into action. And with expertise in 17 industries and global capabilities that span 170 countries, we can help clients anticipate change and profit from new opportunities.

## References

- 1 'Balancing Risk and Performance with an Integrated Finance Organisation. The Global CFO Study' IBM Institute for Business Value. October, 2007. <http://www-935.ibm.com/services/us/gbs/bus/html/2008cfostudy.html>
- 2 Corporate Executive Board, with permission. From the Audit Director Roundtable of The Finance And Strategy Practice. 2010. [www.adr.executiveboard.com](http://www.adr.executiveboard.com)
- 3 'Improving Enterprise Risk Management Outcomes.' Joint ERM Study, IBM and APQC.
- 4 Corporate Executive Board, with permission. From the Audit Director Roundtable of The Finance And Strategy Practice. [www.adr.executiveboard.com](http://www.adr.executiveboard.com). 2010
- 5 'Improving Enterprise Risk Management Outcomes.' Joint ERM Study, IBM and APQC.
- 6 Ibid.
- 7 Thompson, Ben. 'Keeping Calm in a Crisis.' *Business Management*. May 11, 2011. <http://www.busmanagement.com/article/Keeping-Calm-in-a-Crisis/>
- 8 Gasparino, C. 'The Sellout.' HarperCollins. 2009.
- 9 Author interview with Fortune 20 executive.



---

© Copyright IBM Corporation 2011

IBM United Kingdom Limited  
PO Box 41, North Harbour  
Portsmouth, Hampshire PO6 3AU  
United Kingdom

IBM Ireland Limited  
Oldbrook House  
24-32 Pembroke Road  
Dublin 4

IBM Ireland registered in Ireland under company number 16226.

Produced in the United States of America  
June 2011  
All Rights Reserved

IBM, the IBM logo and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at 'Copyright and trademark information' at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.



Please Recycle

