Extending Enterprise Risk Management (ERM) to address emerging risks

~~Managing known risks~~

Exploring emerging risks

PricewaterhouseCoopers

Table of contents

Foreword by Samuel A. DiPiazza Jr

In the past several years, many large-scale events that were once thought unlikely, distant, or isolated – climate change, food insecurity, energy supply volatility, overhaul of technology, and a global liquidity crisis, to name a few – have manifested and changed the course of business for many organisations.

Venerable financial services companies have succumbed to the biggest financial crisis in decades; the evolution of the automotive industry has been accelerated by the need to reduce reliance on finite natural resources; food and product safety issues have had major business and reputational impacts; and ongoing concerns such as volatile energy prices and geopolitical instability have made an interconnected global economy both unpredictable and uncertain.

Such global or "emerging" risks are systemic in nature and span beyond the capacity of a single enterprise to contain. While their likelihood may have once been deemed low, their impact is so significant – potentially franchise destroying or opportunity generating – that it cannot be ignored. Not surprisingly, understanding unknowns has become a boardroom issue.

The aftermath of these events has brought to the surface in many instances a lack of preparedness or effective response. Processes may have been in place to identify, assess, and manage risk, but shortcomings became evident where these processes did not systematically refresh based on changing conditions. Identifying the risk after it has already manifested can be too late.

The agility to detect and adapt to changes in the environment and appreciate the interrelations between events when they occur emerges as the key not only to endurance but also new opportunities. Findings of PricewaterhouseCoopers' 2008 *Annual Global CEO Survey* indicate that 95% of respondents believe change agility is an important or critical source of competitive advantage in sustaining growth over the long term. Indeed, hailed as success stories in the global financial crisis are those organisations that were able to identify signals of increased exposure early on, such as increased mortgage lending, ease of lending requirements, reports of borrowers not understanding the mortgage arrangements they entered into, emergence of new financial instruments that were mortgage related, or a possible balloon in home prices. While some financial institutions folded as a result of their bets and the difficulty they faced in adjusting these as the signals became more evident, others were able to adjust their positions, make acquisitions, and grow.

Understanding such potentially game-changing events requires heightened awareness of changing conditions and an assessment of the risk's impact, its interconnectedness with other risks, and implications for the organisation's strategy and objectives. The risk-resilient organisation continuously scans the environment for changes that could impact its strategy and objectives, convenes as necessary to adjust its course, and recognises that certain risks may be too large for it to manage alone. Collaborative risk mitigation can occur with supply chain partners or with peers (at an industry, geographic, or other level) that may be confronted with the same challenge. Such collaboration is equally valuable among the independent business units of a single organisation.

Organisations need to take a new look at their risk management processes and allocation of resources to ensure that emerging risks are effectively identified, assessed, and managed from strategic planning to day-to-day processes at all levels of the organisation. Risk management practices and resulting risk radars must evolve from an enterprise-level programme, designed to manage the impact of risks on a single organisation, to a collaborative process, one in which many organisations and stakeholders work together to assess and mitigate their shared risks. Successfully engaging in such partnerships provides the rewards of improved preparedness and response to risks that could challenge organisations' business strategy and survival, and unveil opportunities hitherto unknown.

Samuel A. DiPiazza Jr
Chief Executive Officer

~~Avoiding unknown risks~~

Capitalising on emerging opportunities

Section 1

The heart of the matter

Many organisations have deployed risk management programmes to identify, assess, and manage risks, using techniques such as risk assessment, scenario analysis, and stress testing as a basis for determining response strategies that align with the entity's objectives and risk appetite and tolerance.

However, major events occur that reveal shortcomings in risk management programmes and limits to organisations' resilience in the face of risk. Questions arise: Where was the breakdown? Why did the risk management process not work? How could we have known?

ERM is only as effective as it is able to produce a risk radar that is meaningful and forward-looking.

Enterprise Risk Management (ERM) is indeed only effective insofar as the risk management process produces a risk radar for the organisation that is meaningful and forward-looking. Think of how, over the past two years, climate change went from decades of scientific debate to a fundamental driver of business strategies. Or think of how, after 9/11, terrorism went from a speculative thought exercise to the top of the boardroom agenda. Such "emerging risks," which are beyond any particular party's capacity to control individually, have transformed the world in which we operate. Some organisations have disappeared as a result, while others have come out stronger. What has made some succeed and others fail?

As the confluence of trends in recent decades has led to greater interdependence in the global economy, it has also increased the interconnectedness between risks, which today often transcend enterprises, industries, and national borders. In pursuit of opportunities, businesses are increasingly collaborating with a wide range of communities, investors, regulators, and other stakeholders – but in the process, they also expose themselves to an increasing range of risks, not least of which is risk to reputation. While technology has enabled new forms of intra- and inter-enterprise collaboration, its risks are also borderless – as, for instance, would be the impact of a blackout of the Internet. The interactions that comprise the connected world have increased the complexities in managing risk.

The heightened focus on risk management is also expressed by credit rating agencies such as Standard & Poor's, whose guidance for ERM states that "a solid risk-management program must consider risks that do not currently exist or are not currently recognized, but that might emerge following changes in the environment. For these risks, normal risk identification and monitoring will not work because the frequency and impact is usually completely unknown. Nevertheless, experience shows that when they materialize, they have a significant impact and therefore cannot be excluded."[1]

Moreover, the provisions of the United States' "Implementing Recommendations of the 9/11 Commission Act of 2007" – a voluntary but formal set of certification processes, standards, and protocols for business continuity and resilience management – reinforce the expectation that, across the board, stakeholders, investors, and regulators expect organisations to manage risks holistically and mitigate those risks that were once perceived as extreme scenarios, and perhaps still are.

1 Standard & Poor's, "Criteria: Summary of Standard & Poor's Enterprise Risk Management Evaluation Process for Insurers," *RatingsDirect* (2007)

To address risks that may seem unknown or unknowable, organisations must adopt a systematic approach to emerging risk identification, assessment, and management. Effectively applying ERM principles can help business leaders think through informed, rational, and value-creating decisions where risks may be emerging. Organisations can better protect themselves and even further their strategies and objectives by embedding this discipline into their risk management culture. Key steps include:

Identify emerging risks relevant to the organisation

Relative to the strategy and objectives of the organisation, risks should be identified by thoroughly scanning and analysing all relevant risk factors, as remote as they may seem. These risks, together with the other known risks, form the basis for the organisation's risk radar and must be refreshed in real time as changes in the environment occur.

Assess the risk's significance, interconnectedness with other risks, and implications to the business

Effectively assessing emerging risks requires consideration of the significance of the risk to the entity and its stakeholders (both internal and external), considering impact, probability, and correlations (interconnectedness with other risks) in relation to the organisation's strategy and objectives.

> By applying ERM to emerging risks, organisations demonstrate the agility to detect and respond to large-scale risks.

Determine risk response strategies, considering collaboration with external parties

To address emerging risks, the organisation may need to accept the risk as it is or respond to it through preparedness and mitigation strategies. In determining its approach, based on the expected impact and likelihood of occurrence in relation to its appetite for risk and its tolerance for deviation from its objectives, the organisation may seek to explore partners with whom to collaborate to mitigate the risk or prepare for its possible realisation. Collaboration is best accomplished with partners (such as value chain partners and peers within the industry or geography) that share both the cost of failure to mitigate the risk and the benefit of effective risk mitigation.

Routinely monitor emerging risks through effective use of indicators

Resources should be allocated (or reallocated) to identify and monitor indicators of emerging risks and develop the organisational agility to address these should they arise. Considering the nature, scale, and interconnectedness of such risks and also inter-organisational risk mitigation alternatives, such resources must enable dynamic risk management in support of the achievement of organisational strategy and objectives. Emerging risks can be monitored through both qualitative and quantitative indicators. Understanding the circumstances around possible emerging risk events provides a starting point from which to monitor the symptoms of developing issues, which should be refined as further data becomes available to monitor and determine the need for alternative risk responses.

Applying ERM principles to emerging risks represents an opportunity to fully capture the rewards of effective risk management as manifested in the agility to detect and respond to large-scale risks. Such discipline should be embedded in the processes and tools used for planning, executing, and evaluating business performance. With the use of innovative approaches such as scenario analysis and event simulations, supported by a strong risk management culture, organisations will be better able to identify and prioritise emerging risks in order to protect value and further the organisation's strategy and objectives.

~~Register of known risks~~

Radar of emerging risks

Section 2

An in-depth discussion

2.1 Understanding emerging risks

Emerging risks, also sometimes called global risks, are large-scale events or circumstances that arise from global trends; are beyond any particular party's capacity to control; and may have impacts not only on the organisation but also on multiple parties across geographic borders, industries, and/or sectors, in ways difficult to imagine today. Emerging risks are those large-impact, hard-to-predict, and rare events beyond the realm of normal expectations – what philosopher-epistemologist Nassim Nicholas Taleb calls "black swans" in reference to the fact that Europeans once *knew* that all swans were white – until explorers in Australia discovered black ones.

As these risks present high impact but low probability and fall beyond the organisation's direct control to mitigate, they are often found to be under-resourced. When competing for budgets, those risks with greater probability of occurrence tend to win. When competing for management attention, those risks deemed more likely to impact performance targets and rewards win again. However, failure to understand and track these risks can lead to a situation in which today's afterthought becomes tomorrow's global headline issue. As a result, these risks are often referred to as the unexpected or the unknown. One can argue, however, that "almost all consequential events in history come from the unexpected."[2] In fact, with adequate information and analysis, the unexpected can often be predicted by extrapolating from variations in statistics based on past observations.

> Emerging risks are those large-scale events or circumstances beyond one's direct capacity to control, that impact in ways difficult to imagine today.

The speed and impact of these risks are further exacerbated by their interdependence with other risks, which requires a profound understanding not only of the underlying risk factors but also of other events that may be triggered. In a global economy, where opportunities are sought across borders and industries, risks spread equally vastly.

The sub-prime mortgage crisis occurred when, over a very short span of time,, firms found their holdings of mortgage-backed securities and collateralised debt obligations (backed by sub-prime mortgages) turn into positions that could not be sold in an orderly manner. The crisis affected seemingly unrelated firms, with the credit markets freezing up and liquidity crises ensuing around the world, forcing global central banks to inject billions of dollars into capital markets and slowing economic growth in virtually every country around the globe.

Some companies did a better job than others at proactively monitoring their portfolios through this crisis, identifying trends, performing portfolio analysis, and examining their market risk exposures. They were able to recognise when the organisation's risk tolerances were exceeded and alter their course of action. For example, some companies chose to reduce their stockpiles of mortgage and mortgage-related securities and buy expensive insurance to protect against further losses. Such proactive monitoring of risk that embeds analysis of trends and understanding of interdependencies in the interconnected business markets can help avoid losses and seize opportunities.

Through its Global Risk Network, the World Economic Forum has identified a number of global risks and plotted them in terms of likelihood and severity. (See Figure 2.1.1.)

2 Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House (2007))

2.1.1

Global risks landscape 2009: Likelihood with severity by economic loss

Based on the assessment of risks over a 10-year time horizon by the Global Risk Network
Key: Boxes indicate change since last year's assessment

Increased

Decreased

Stable

New risk for 2009

Likelihood Severity

ECONOMIC

1 Food price volatility
2 Oil and gas price spike
3 Major fall in US$
4 Slowing Chinese economy (6%)
5 Fiscal crises
6 Asset price collapse
7 Retrenchment from globalisation (developed)
8 Retrenchment from globalisation (emerging)
9 Regulation cost
10 Underinvestment in infrastructure

GEOPOLITICAL

11 International terrorism
12 Collapse of NPT
13 US/Iran conflict
14 US/DPRK conflict
15 Afghanistan instability
16 Transnational crime and corruption
17 Israel-Palestine conflict
18 Violence in Iraq
19 Global governance gaps

ENVIRONMENTAL

20 Extreme climate change related weather
21 Droughts and desertification
22 Loss of freshwater
23 NatCat: Cyclone
24 NatCat: Earthquake
25 NatCat: Inland flooding
26 NatCat: Coastal flooding
27 Air pollution
28 Biodiversity loss

SOCIETAL

29 Pandemic
30 Infectious disease
31 Chronic disease
32 Liability regimes
33 Migration

TECHNOLOGICAL

34 CII breakdown
35 Emergence of nanotechnology risks
36 Data fraud/loss

Source: World Economic Forum, *Global Risks 2009: A Global Risk Network Report*

Further examples of emerging risks can be derived from various studies. A starting point for organisations to consider may include the illustrative, non-exhaustive list in Figure 2.1.2.

2.1.2

Illustrative examples of emerging risks

- **Increasing natural resource constraints**
  (e.g., loss of freshwater reserves, depletion of oil reserves, loss of biodiversity) that could raise the cost of raw materials and increase food prices, human suffering, and the pressure to identify alternate energy sources.
- **Natural or man-made disasters**
  (e.g., floods, terrorism, cyber-terrorism, viruses, spyware) that could cause business disruption and human catastrophes.
- **Increased industrial pollution and rising global carbon emissions**
  leading to climate change that could cause a decrease in biodiversity, a shift in locations of production and consumption, and regional resource shortages.
- **Rapidly shifting demographic patterns**
  (e.g., ageing population) that could cause talent shortages in certain labour markets or within certain capabilities, lack of adequate skills, or shifts in customer demands and/or loyalties.
- **Rising labour costs driven, in part, by expanding benefits**
  (pension, workers' compensation, and other non-salary expenses), which could result in lower profitability and loss of competitive advantage.
- **Increased volatility in asset prices and commodity markets**
  (e.g., oil price shock, asset price collapse) that could cause fluctuations in cost structures that cannot readily be passed on to the consumer or otherwise absorbed.
- **A global liquidity crunch**
  (e.g., resulting from sub-prime mortgage lending practices) that could raise the cost of capital for financing transactions.
- **Emergence of new technologies**
  (e.g., nanotechnology) that could evolve in unforeseen ways in an emerging market – for example, leapfrogging existing technologies as new applications arise.
- **Technology and communication disruptions**
  (e.g., Internet blackout) or system failures, which could lead to business disruptions and economic loss.
- **Changes in laws and regulations**
  (e.g., spread of liability regimes impacting foreign investment, or industry-specific laws such as prohibition impacting the alcohol beverage industry) that could cause an overhaul in the manner by which businesses are run, or affect the sources of their profits.
- **A realignment of power in the capital markets of a country**
  (e.g., increased governmental control of companies, foreign investment) that could lead to classes of activist investors who could pressure for different industry approaches to capital structure, profit allocation, or strategic goals.
- **Decline in global economic growth**
  (e.g., caused by slowed Chinese economic growth, global recession, unsustainable deficit levels) that could negatively impact demand and put downward pressure on prices.
- **Political crises**
  (e.g., failed and failing states, war, Middle East instability, failure of democratic institutions, regime change), which could result in nationalisation of assets, increased regulation, protectionist tendencies, or other loss of control.
- **Pandemics and other health crises**
  (e.g., fast-traveling pathogens such as avian flu, developing world disease such as HIV/AIDS, tuberculosis, malaria), which could jeopardise supply chain, consumers, employees, and others.
- **Economic inequality**
  which could exacerbate poverty and suffering and increase pressure on business to engage in humanitarian efforts.
- **Rise in nuclear capabilities**
  which could endanger global political stability and physical security.
- **Terrorist threats**
  which could reduce economic confidence or cause direct economic losses as well as loss of life, property, and security.
- **Increased competition from emerging markets and/or within the home market**
  which could cause downward pressure on prices.
- **Rise in anti-globalisation sentiment and protectionism**
  (e.g., fiscal policies, trade embargoes, heightened tariffs, or other anti-competitive practices), which could cause retrenchment from global trade and investment.
- **Increase in corruption**
  (e.g., bribery in procurement or sales), which could create anti-competitive business practices and lead to regulatory fines and sanctions and reputational damage for perpetrators.
- **Decline in recognition or enforcement of intellectual property rights**
  (e.g., patents, licenses), which could cause unlicensed commercial activity or loss of proprietary information.

Source: PricewaterhouseCoopers

Organising relevant emerging risks can follow different categorisation schemes. These should be integrated with an organisation's ERM framework to facilitate ownership and accountability as well as due processes for identifying, assessing, and managing these risks. Examples of such categorisation include:

By source of the risk or theme	e.g., per categories of the World Economic Forum Global Risk Network:[3] • Technological • Geopolitical • Societal • Environmental • Economic
In relation to objective types	e.g., per the Committee of Sponsoring Organizations (COSO):[4] • Strategic • Operational • Reporting • Compliance
By characteristic of the risk	e.g.: • Exogenous/endogenous • Predictability • Degree of control • Duration
By the manner in which the risk manifests	e.g.: • Long-term changes • Sudden, unexpected events • Gradually deteriorating operating conditions • Local events with systemic impacts • Resulting from catastrophic events

The PricewaterhouseCoopers 2008 *Annual Global CEO* Survey reveals several findings in relation to risks spanning beyond the enterprise itself:

- The risks deemed most likely to occur include political and religious tension; the emergence of a new set of countries that will challenge the economic, political, and cultural power of the G8; and pressures on natural resources.
- Top threats to business growth are deemed to be the downturn in major economies, disruption of capital markets, over-regulation, energy costs, inflation, low-cost competition, and availability of key skills.
- Top opportunities for business growth are deemed to be better penetration of existing markets, new product development, new geographic markets, mergers and acquisitions, and new joint ventures and/or strategic alliances.

It is important to recognise that emerging risks can be opportunities rather than threats if they're identified, assessed, and managed for competitive advantage, as illustrated by the successes emerging from times of turbulence and change.

Emerging risks can be opportunities rather than threats if they're identified, assessed, and managed for competitive advantage.

3 World Economic Forum, *Global Risks 2009: A Global Risk Network Report* (2009)
4 Committee of Sponsoring Organizations (COSO), *Enterprise Risk Management – Integrated Framework* (2004)

2.2 Allocation of resources to preparedness

Successes and failures in responding to emerging risks are often the result of organisations' rigor in applying risk management principles and their agility in adjusting to a changing environment and new challenges. To be able to effectively uncover such risks, resources need to be sensitised and focused on identifying the broad realm of potential risks, including emerging risks.

In most organisations, there is a fundamental mismatch between risk exposures and risk management resource allocation. According to some estimates, the risks that led to 60% of "rapid losses" (drops in shareholder value by one-half within one year) experienced by Fortune 500 and FTSE 100 companies are strategic in nature.[5] Yet, the majority of risk management resources tend to be focused on operational, financial, and compliance risks. Strategic risks and "black swan" types of low-probability risks are often under-resourced.

The resource allocation conundrum can be understood by considering the continuum of risk, from known (K) through unknown (u) to unknowable (U). Some risks, particularly natural disasters, can be said to be "known." Their causes, probability of occurrence, and likely impacts are understood and well defined, although there is still some uncertainty surrounding these estimates. Known risks have occurred previously – and, therefore, can be measured and managed.

Other risks are "unknown." The risk events are well defined, but it is not possible to assign probabilities as to the occurrence of specific events (for example, terrorism and systemic financial instability). Another way of looking at unknown risks is to think of them as risks where there are several competing plausible models of how reality might unfold, but no accepted paradigm. Unknown risks require governments or businesses to build resilience into their risk models – through continuity planning, stockpiling, slack in the system, or diversification of sources of vital goods.

> Risk management resources tend to be focused on operational, financial, and compliance risks. Strategic risks and "black swan" types of low-probability risks are often under-resourced.

The last class of risks is those that are "unknowable." Unknowable risks have not yet emerged, and our understanding of the systemic linkages of unknowable risks is speculative. "Unknowability" is a key consideration in the context of risk conflation, where a large number of possible combinations of risks and vulnerabilities can lead to a vast array of possible outcomes, some of which are "perfect storms."

Resources are typically allocated more heavily to known risks, for several reasons:

- First, existing incentives tend not to be aligned with long-term corporate performance. In the case of sub-prime mortgages, for example, many players, such as mortgage brokers and investment banks that assembled collateralised debt obligations (CDOs), were compensated for deal flow with too little consideration for the longer-term risks they introduced into the financial system. They had little incentive to tighten standards because the risks were, in theory, borne by other parties. In practice, of course, these players were selling long-term shareholder value and financial system stability for year-end bonuses.
- A second reason is a general lack of perceived relevance – a failure to recognise the significance of global phenomena until events result in local impact. Hindsight, as the saying goes, is clear – a cliché that seems to be repeated any time an emerging risk manifests. Yet, the potential impact of those risks can most certainly be cushioned through more proactive, prudent, and collaborative approaches. In other words, relevance need not be an afterthought.
- The third constraint to expanding ERM to emerging risks is both the most pertinent and the oldest: limited resources. Resources need to be allocated (or reallocated) to help anticipate risks that are currently being ignored.

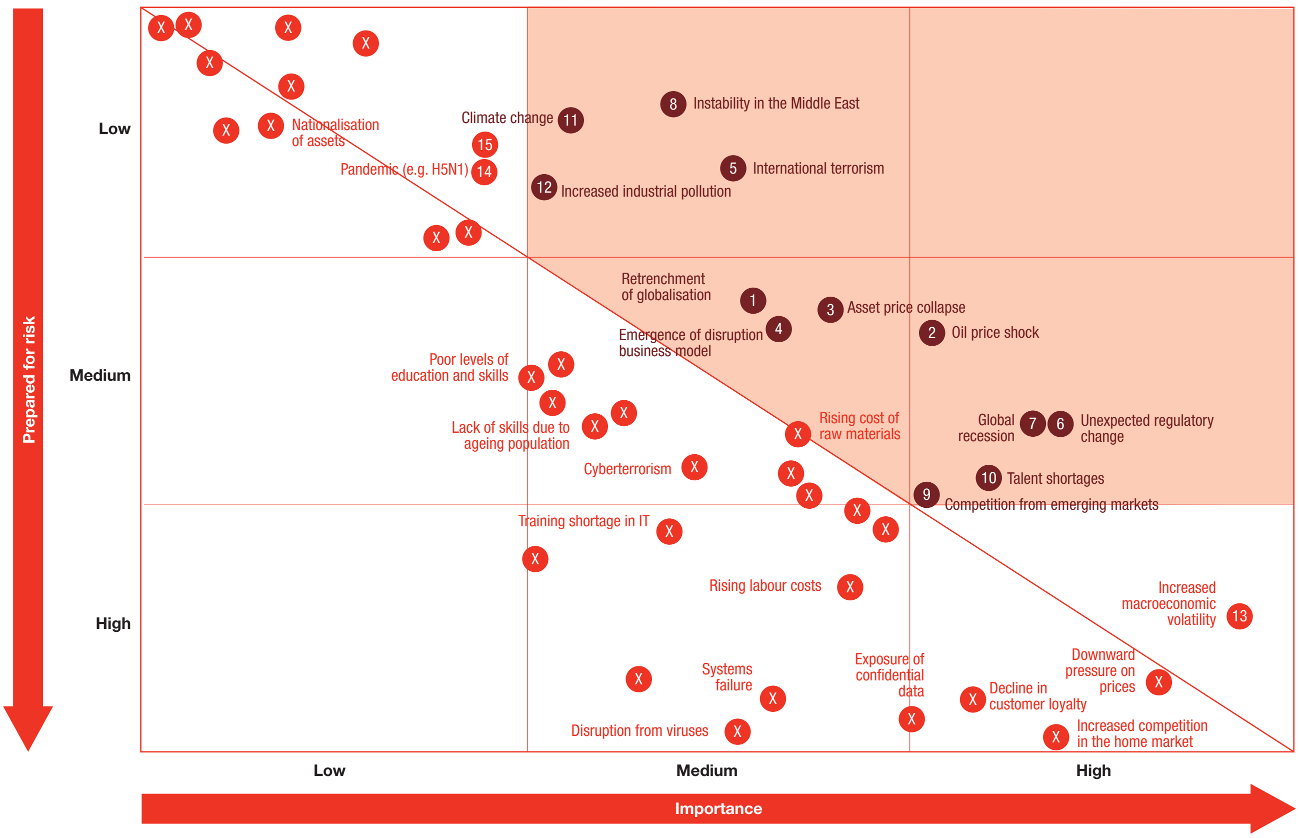
5 PricewaterhouseCoopers, *State of the Internal Audit Profession Study: Targeting Key Threats and Changing Expectations to Deliver Greater Value* (2008)

Figure 2.2.1 illustrates current levels of preparedness to respond to emerging risks, as identified by leading executives.

Applying ERM to address emerging risks will help improve preparedness against the most uncertain events, through a reallocation of existing resources. Of course, different types of emerging risks require different levels of resource allocation, along with different approaches. A risk-resilient organisation seeks to minimise unknown risks by actively identifying and assessing such risks, devising strategies for mitigation, and monitoring changes in exposures routinely. As a result, unknown risks transform into known risks and an organisation is left with a more manageable set of constraints.

2.2.1

Long-range risk grid



Source: Economist Intelligence Unit, *Risk 2018: Planning for an Unpredictable Decade* (March 2008)

2.3 Embedding the discipline of addressing emerging risks into ERM

The discipline for addressing emerging risks should become part of the organisation's strategic planning, business execution, and performance evaluation and reward structure. How does this differ from traditional risk management activities? Applying ERM principles to emerging risks is an opportunity to share the effort and rewards of preparedness and mitigation with partners. Companies with the vision to connect global trends and risks with their own strengths and market knowledge, and to participate in collaborative efforts to manage those risks accordingly, will be better prepared for global growth.[6] Therefore, building on an established framework for thinking about ERM (such as COSO's Enterprise Risk Management – Integrated Framework), several activities should be expanded to effectively address emerging risks and embed these practices into the organisation's business planning, execution, and evaluation processes.

As an organisation designs or evaluates its internal environment, it should ensure it has the requisite capabilities and skills within the organisation to ensure adequate oversight and management of emerging risks to support the organisation's strategy, mission, and values. (See Figure 2.3.1.)

To ensure that each of these components is effectively in place throughout the various parts of an organisation, and to engage the relevant external parties as necessary, organisations should assess their risk management culture periodically.

As a result of an effective risk management culture and extending ERM to emerging risks, the organisation follows a structured approach to define, assess, and manage all relevant risks, including those that may be just emerging. This discipline becomes part of managing the business.

2.3.1

ERM applied to emerging risks

ERM components per COSO	Applied to emerging risks
Objective setting	The objectives that the organisation sets for itself at various levels – enterprise-wide, business-unit-specific, or otherwise – and the amount of risk it is willing to accept in pursuit of these objectives should serve as the basis for identifying, assessing, and managing relevant emerging risks. These risks may impact one or several of the organisation's objectives, which may range from strategic to operational, compliance, and reporting.
Event identification	Event identification involves not only capturing known emerging risks but also performing historic and forward-looking analysis to uncover potential exposures relative to the organisation's objectives. Embedding this capability into day-to-day processes requires awareness, training, and dedicated focus on such risks across the organisation, to the extent that unknown risks are reduced and the organisation can focus its efforts on managing currently known risks and preparing for those that are unknowable.
Risk assessment	This step requires consideration of the impact of emerging risks not only on the organisation or business unit itself but also on other organisations or business units. It also requires an understanding of the ways in which interconnections between emerging risks and other risks could increase the emerging risk's impact or likelihood of occurrence. The organisation should have a clear definition of how much variance from the achievement of objectives it is willing to tolerate.
Risk response	An organisation should determine the appropriate risk response based on its defined corporate risk appetite and tolerance levels and the results of its assessment of the emerging risk. While the typical risk response options of accepting, avoiding, sharing, or reducing remain, the most effective response may be one that is achieved through collaboration with partners, a response that can help mitigate the impact or likelihood of occurrence, minimise negative impact on the achievement of objectives, and possibly even capture opportunities.
Control activities	Checks and balances deemed appropriate to control the risk should be in place to manage known risks and prepare for the occurrence of unknowable risks.
Information and communication	Information and communication are essential to engaging the requisite parties, raising awareness, and provoking analysis of emerging risks in relation to the organisation's objectives, particularly in light of the interconnectedness of emerging risks with other risks.
Monitoring	Monitoring the effectiveness of emerging risk mitigation efforts requires evaluation of past events and analysis of future trends. A look-back analysis considers how emerging risks were or could have been mitigated, thus providing lessons on how to further enhance the ability to manage such risks in the future. Forward-looking analysis requires the definition and use of relevant leading indicators to alert management to changes in the organisation's exposure to emerging risks.

Source: PricewaterhouseCoopers

6 World Economic Forum, *Global Growth@Risk 2008: A Report of the Global Risk Network* (2008)

~~Established risk tools~~

Optimised approaches to risk

Section 3

What this means for your business

While many organisations have processes and structures in place for managing risks day-to-day, practices reveal that these often fail to fully address emerging risks, largely due to many of the inherent characteristics of these risks described above: hard to quantify, seemingly remote, with low probability but high impact.

The seemingly more immediate obligation to focus on the short or medium term often impedes the attention of many organisations to such risks. An organisation's stakeholders, however, focus not only on short-term results but also on long-term success.

The culture of the organisation must reinforce the fact that ERM can be optimised by expanding the traditional application of its principles to emerging risks and further risk resilience. ERM, as defined by leading standards such as COSO, provides key principles that can be leveraged for managing emerging risks. Consider four essential steps:

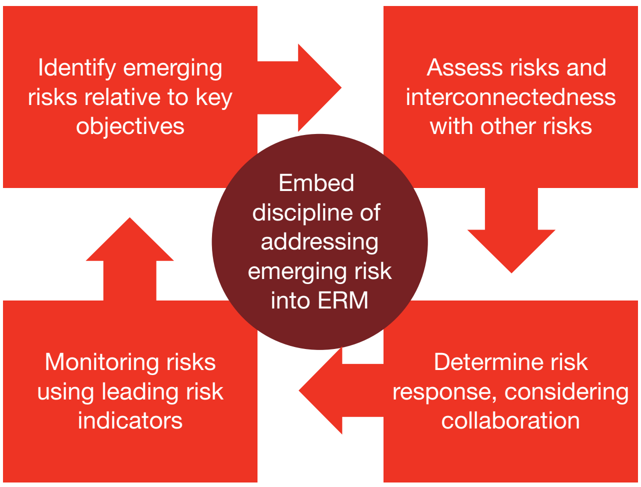
1. Identify emerging risks that are relevant to the organisation
2. Assess their significance, interconnectedness with other risks, and implications
3. Determine how to respond to such risks, considering options to collaborate with partners
4. Monitor routinely emerging risks through effective use of leading indicators

Each of these steps benefits from the broadest possible perspectives and contributions, not only internal but also external, managed through an integrated risk management process.

(See Appendix A for a graphical depiction of these steps and Appendix B for case study illustrations.)

3.0.1

Embedding the discipline of addressing emerging risks into ERM



Source: PricewaterhouseCoopers

3.1 Identify emerging risks relative to key objectives

Organisations are increasingly required to think of their risk profile not just as their own, but also as an integral component of their international partners' risk profiles. Success in a connected world is only possible through a paradigmatic shift from *ignoring* risks that do not readily appear related to one's enterprise, to *embracing* and managing emerging risks throughout an organisation's value chain. For example, a local manufacturer may today serve as customer to a supplier on one continent, vendor to a retailer on a second continent, client to a merchant bank from a third continent, and financial intermediary to a fraternity of investors from every continent. Each of these relationships implies new opportunities but also new risks. A failure of *any single relationship* entails consequences for *all* relationship partners. Thus, an understanding of the risks faced by each partner has become an important input in identifying and evaluating risk.

Based on the organisation's strategy and goals, management should identify all potentially relevant risks, both organisation-wide and at the various levels and units of the organisation. To go beyond known risks, organisations should explore what may seem unknown but could be uncovered through analysis of historical data and forward-looking analysis. Management should regularly perform a thorough scan of characteristics and changes in the environment to identify events that may have impacted the organisation's shareholder value in the past or may impact it in the future. Drivers to consider include economic, social, political, technological, and natural environmental events, all of which can be identified through external sources such as media articles, analyst and rating agency reports, and publications by not-for-profit foundations.

To identify all relevant risks, organisations should capture perspectives from industry, academic thought leaders, economists, non-conformists, and contrarians in general – anyone who can help take the thinking of internal executives and experts to new places. History shows that many risk events have resulted as much from complacency, limited foresight, and a reluctance to challenge the status quo as from failures of controls, judgment, and governance.

Risks can be classified in different ways – for example, by source, related objective, implication, or other characteristics that help to analyse the risk and assign accountability for monitoring and response. This should be aligned with the organisation's existing risk classification framework (for example, as part of its ERM programme), considering a broad range of drivers such as economic, social, political, technological, and natural environmental.

The organisation should define tolerance levels for all key risks or risk categories identified. How much variation from the achievement of objectives is acceptable? This should be in sync with the overall level of risk the organisation is willing to take in pursuit of its objectives – in other words, its risk appetite. Certain emerging risks could put the organisation out of business, while others may present an opportunity to reshape the market.

Emerging risks may present a threat or an opportunity for the enterprise as a whole or for a certain business unit or geography. By definition, they may also affect other organisations, positively or negatively. The organisation's thinking, therefore, needs to extend beyond its own boundaries.

A meaningful risk radar is therefore the result of analysis not only of known risks but also of those larger, systemic risks that may have implications not yet known. In today's ever-changing business environment, organisations must continually update their identification techniques and mechanisms in order to refine their analyses of risks, increasing their ability to predict risk events such that they can create better and faster response mechanisms for dealing with major events.

3.2 Assess the risk's significance, interconnectedness with other risks, and implications to the business

Traditionally, risk assessment considers the significance to the entity and its stakeholders (both internal and external) as well as correlation between risks, often based on observed facts and trends. Assessing emerging risks requires a broader evaluation of such risks, considering the larger scale of impact and the interconnectedness of risks that typically have not yet manifested. As for any risk assessment, the assessment of emerging risks requires involvement of the requisite subject matter experts and use of a consistent risk rating methodology.

Scenario analysis can serve as an effective means for organisations to estimate their potential risk exposures and levels of preparedness should catastrophic risk events emerge. According to a 2008 Economist Intelligence Unit report, "by thinking through different futures, executives have the opportunity to stress test their strategy and challenge the assumptions they hold about what might be successful in the years ahead."[7]

To develop risk scenarios, leading organisations typically take a workshop-based approach, supported by requisite planning and review phases. Such an approach, conducted by an effective facilitator and involving the requisite subject matter experts, comprises the six key steps detailed in Figure 3.2.1.

Leading practices for conducting such scenario analysis workshops indicate that the impact and likelihood of emerging risks should be assessed using risk rating scales to generate heat maps or radars of the risks. This enables relative comparisons and determination of risk responses based on the organisation's risk appetite and tolerance levels, which should be defined in strategy setting and business planning.

Risk rating scales may be defined in quantitative and/or qualitative terms. Quantitative rating scales bring a greater degree of precision and measurability to the risk assessment process. However, qualitative terms need to be used when risks do not lend themselves to quantification, when credible data is not available, or when obtaining and analysing data is not cost-effective. Due to the strategic nature of emerging risks, rating scales tend to be qualitative. Risk rating scales are not one-size-fits-all, so should be defined as appropriate to enable a meaningful evaluation and prioritisation of the risks identified and facilitate dialogue to determine how to allocate resources within the organisation. Risk rating scales provide a common form of measurement to help organisations prioritise risks and determine required actions based on their defined risk tolerance.

For emerging risks, a key difference from traditional ERM approaches is that risk rating scales need to consider the cross-organisational impact and potential scale of the risks as well as interdependencies with other risks. Similarly, the time horizon used to assess the likelihood of risks should be consistent with the time horizons related to objectives. Some emerging risks, such as climate change, may challenge this notion with an understanding that long-term consideration may create value in the achievement of an organisation's objectives.

A risk map enables analysis over time as risk assessments are refreshed (e.g., noting upward or downward trend of threats and the extent of positive or negative correlations between

3.2.1

Scenario analysis approach

Source: PricewaterhouseCoopers

7 Economist Intelligence Unit, *Risk 2018: Planning for an Unpredictable Decade* (2008)

certain risks). In particular, the interconnectedness of emerging risks necessitates some assessment of their degree of correlation. This can be conducted through covariance analysis, where different variables are evaluated in relation to each other. The degree of correlation between various emerging risks (e.g., perfect positive correlation, perfect negative correlation, no correlation) enables the organisation to more effectively and efficiently mitigate risks. For example, similar mitigation strategies may be employed to manage risks that are correlated, whereas risks that have no correlation may require disparate mitigation techniques.

In addition to assessing threats to the organisation, leading organisations also assess how certain events or circumstances might call on their core activities to help other organisations manage exposures to catastrophic risks. The ability to capitalise on such opportunities requires adequate information flow, both internally and externally.

3.3 Determine risk response strategies, considering collaboration with external parties

Risk responses vary depending on the assessment of the risk, how much risk the organisation is willing to take on, and the organisation's tolerance for variation from its objectives. As the organisation selects its responses to emerging risks, it should do so on a risk-informed basis. It may choose to accept certain emerging risks by relying on natural offsets within a portfolio or considering the risks as a cost of doing business, in line with defined risk tolerances. For those risks where risk tolerances are exceeded and action needs to be taken, an organisation may find that the risks span beyond its individual control, and risk mitigation must explore collaborative approaches. PricewaterhouseCoopers' 2008 *Annual Global CEO Survey* revealed that collaboration in pursuit of long-term success is most developed with employees and trade unions (83% of survey respondents engage in such collaboration), customers (84%), supply chain partners (75%), providers of capital such as creditors and investors (67%), and government and regulators (61%).

Collaborative risk mitigation strategies are often the only means available for organisations to envision the unknown and adequately protect their assets – especially in cases without historical precedent. In a connected world, both the rewards and risks of doing business are, by definition, connected. Thus, effective responses to networked risks must themselves be networked in nature. However, collaborative efforts need not necessarily include multiple organisations and/or government and non-government agencies.

The same principles and processes are equally relevant when organising responses among an organisation's business units, each of which may have different exposures and resources relative to a particular emerging risk. It is important for corporate headquarters to understand different scenarios of how a risk may manifest differently for each business unit. Independent business units may also recognise the benefits of collaboration with other units. While one business unit may have more direct exposure to a particular emerging risk (for instance, rising energy prices and their effect on transport costs), another business unit may be able to help mitigate that risk and generate business opportunity through its production of alternate energy sources. Mitigating risks optimally for the organisation as a whole may require the units to work together closely. Collaboration can help decision makers rationalise the implications of emerging risks to their respective organisations or business units, and mitigate emerging risks through techniques that supplement existing approaches to risk management.

Collaborative risk mitigation strategies are often the only means available for organisations to envision the unknown and adequately protect their assets – especially in cases without historical precedent. In a connected world, both the rewards and risks of doing business are, by definition, connected.