

Speed through common language

Critical factors in risk management today



When the same risk language is spoken throughout a company, its managers and employees know they are on the same wavelength when they talk about risks and opportunities. As a result, the company will detect and react to new risks faster; it will better protect and create value.



Introduction

The credit crunch and the subsequent sharp economic downturn have suddenly confronted businesses worldwide with a dramatic increase in risk-related challenges. This recent experience has confirmed that many companies are slow to detect and react to new risks, a delay that threatens their competitiveness.

In this paper, we explain how to shorten your risk detection and reaction time. Companies should eliminate the barriers to timely and efficient risk management efforts by ensuring that the same risk “language” is spoken throughout the organization: company-wide definitions, priorities, procedures and communication channels should be clearly defined. As a result, your company will be better able to create and protect value and gain a competitive advantage.

The faster a company detects and reacts to new events, the more time it has to reduce risks and seize opportunities.

Detecting and reacting

How sharply will the demand for our products fall in our most important markets? Should we supply customers whose liquidity is in doubt? Can we rely on the strength of our suppliers? Will we be able to obtain funding under acceptable conditions?

Overwhelmed by the sudden, radical deterioration of the economic climate in 2008 and 2009, businesses are wrestling with these and many other risk-related dilemmas. Companies all over the world feel pressed for time when redefining their business priorities or even strategies. They now rue the fact that they failed to pick up on early warning signs that the economic tide was turning: “If only we had known earlier what was coming, we would have had more time to prepare ourselves.” In other words, companies have learned the hard way that they have to reduce the **detection** time of new risk-related events and trends. The flexibility of each organization is limited; a company cannot instantly adapt its practices and processes once it spots a new risk/opportunity event. Early detection is, therefore, essential: it provides an organization with precious extra time to react.

Companies know equally well that a short **reaction** time is also necessary if they are to deal swiftly and adequately with new events and trends. The structure and communication channels of an organization should facilitate such a speedy reaction. The faster a company detects and reacts to new events, the more time it has to turn risks into opportunities – a true competitive advantage. In the pursuit of effective risk and opportunity management, time is indeed of the essence.



Time is of the essence

"...our supervisory group identified actions and decisions that have tended to differentiate firms' performance during the period of market turbulence through year-end 2007. Some firms recognized the emerging additional risks and took deliberate actions to limit or mitigate them. Others recognized the additional risks but accepted them. *Still other firms did not fully recognize the risks in time to mitigate them adequately.*"

Observations on Risk Management Practices during the Recent Market Turbulence, 6 March 2008. Report by the Senior Supervisors Group; this group was formed by financial sector supervisors of countries including the US, the UK, Germany and France.

Rapid responses to new risk-events are relevant beyond the current crisis in the financial sector. In our global, fast-changing, competitive world, speedy detection and reaction are essential whatever the economic climate. Companies are constantly faced with new trends and events, with new risks that they must turn into opportunities; a short response time is an essential condition for dealing with this challenge successfully.

In our global, fast-changing, competitive world, speedy detection and reaction are essential whatever the economic climate.



Language confusion reigns in risk-Babylon

A fast response to new, risk-related events requires that the same risk management language is spoken throughout a company. Unfortunately, with respect to risk management, many organizations resemble a modern-day Babylon of language confusion. As a result, they are slow to detect and react adequately to new, risk-related events and trends.

A common risk management language is much more than an agreed set of symbols for communication. A common risk language in an organization means shared definitions, company-wide priorities, a common culture of risk awareness and accountability and clear procedures for measuring, monitoring, communicating and dealing with risks. Companies hampered by a lack of common risk management language and related procedures are incapable of defining and prioritizing different risks, let alone measuring, communicating and monitoring them.

All too often, the different “risk dialects” spoken in an organization are so diverse that a conscious effort is necessary to create a common understanding of the organization’s risk profile.

Some well-known risk management dialects:

Hazard analysis and critical control points (HACCP) deals with physical, chemical and biological threats to food and drugs safety.

Sox 404 top down risk assessment (TDRA) is a financial reporting risk management tool to comply with section 404 of the Sarbanes-Oxley Act of 2002.

Failure modes and effects analysis (FMEA) is a procedure for analysis and classification of the possible effects of failures on a system. Very popular in manufacturing, it is now also used in the service industry.

Benchmark assessment tool (BEATO) is both a tool and a methodology originally designed to check compliance in security assessments.

Probabilistic risk assessment (PRA) is a methodology for comprehensive assessment of risks associated with complex engineered constructions such as airplanes or nuclear power plants.

An essential part of risk management consists of the development of a language that everybody in the organization understands.

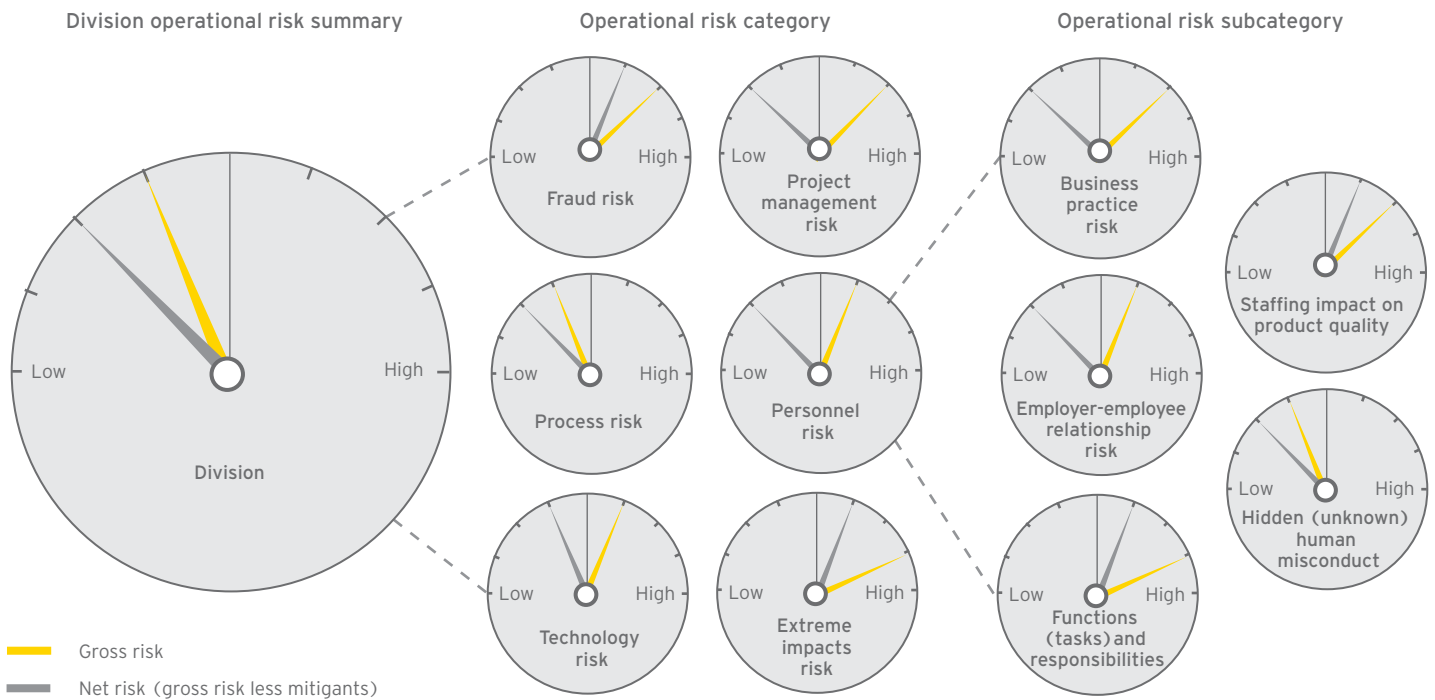


Different units and sections in an organization will view risks from a varied perspective. An essential part of risk management consists of the development and translation of a language that everybody in the organization understands. Only this common language will allow an organization to define, measure and prioritize different risks and to compare them on a common risk dashboard.

Of course risks change. The definition of the most important risks is, therefore, an on-going task for an organization. Like all languages, a risk management language is constantly evolving and its speakers should adapt. However, this acceptance of constant change must never become an excuse for inaction. Not developing a common risk management language because risks change is like not installing anti-virus software on your computer because new viruses constantly appear. As with anti-virus software, the correct answer is not to dispense with a common risk management language, but to update it periodically.

Risk-specific scorecards are used to assess division-level operational risks

Cascading division-level operational risk dashboard



Source: Ada Financial; Operations Council research



Gaining consensus on the main risks

In order to detect and react to new events quickly, an organization should know what it is looking for. This may seem obvious but, in fact, many companies have not clearly defined what their main risks are. Even board members more often than not disagree among themselves about the most relevant risks their company faces.

At Ernst & Young, we have measured to what extent managers of a company agree on the main risks through a risk consensus index (RCI). The RCI is based on the answers of different managers to a simple question: "What do you consider to be the three most important risks for your organization?" The RCI score for board members rarely reaches 50% or higher, a telling sign of a lack of consensus at the highest level of a company. What is more, the risk consensus between board members and lower levels of management is also normally quite limited.

Calculating risk consensus

Members of the sample group are asked individually to name the three most important risks for their organization.

Imagine the sample group consists of five board members and they all name three identical or very similar risks. Once the answers are in, the RCI is calculated as follows:

The risk consensus index (RCI)

$$\text{RCI} = \frac{(\# \text{ respondents} \times 3) - \# \text{ different risks mentioned}}{(\# \text{ respondents} \times 3) - 3} \times 100\%$$

In this case, the numerator of the fraction would be 12, since $(5 \times 3) - 3$ equals 12. The denominator would be 12, too. Their score would be 100% – the perfect consensus!

Now imagine the other extreme: none of the five board members identifies any risk mentioned by any of the others, i.e., among the five of them, they would mention 15 risks. In that case, the numerator of the fraction would be 0, since $(5 \times 3) - 15$ equals 0. The score would be 0%: an absolute lack of consensus. The RCI shows us to what extent a sample group has the same view on what the most important risks for an organization are. It is expressed as a percentage: a higher percentage means more consensus.



No risk consensus: vertical silos

There are multiple reasons for this lack of risk consensus. First of all, where there are vertical separations between functions, resulting in silos within an organization, managers' risk perspectives tend to diverge. Different units and divisions within a company may have very different views on the gravity of a risk if no common risk management language exists. In consequence, everybody within the organization will act according to their own particular assessment of what constitutes an important risk and what doesn't.

Managers in the human resource or marketing function may well have very different risk perceptions from managers in the legal or internal audit function. A similar lack of consensus may obviously exist between managers in different business lines. To the extent that board members identify with certain functions or product lines, this silo-determined approach to risk assessment is often reproduced at the board level.

Silo thinking can have very grave consequences. In the absence of company-wide definitions, priorities and procedures, different business units will always press for more attention for "their" risks once detected. As a result, the discussion about the importance of newly detected risks may produce internal rivalries – or exacerbate existing ones. With the lack of a common risk language, critical resources may be allocated to those best able to articulate their perspective instead of to the area most directly affected by a key risk. Clearly, the resulting internal conflicts will further delay an efficient response to the most important risks, just at the moment when a speedy response is essential. Therefore, a company should make a conscious effort at the senior management and board level to define its main company-wide risks – definitions that transcend the limited perspective of individual business lines and functions. These clearly defined and prioritized risks should be communicated throughout the organization and procedures should be put in place to measure and monitor these risks adequately.

In this effort, special attention should be paid to systemic, cumulative risks. These are present in multiple silos and may represent a very significant risk to the company as a whole, although from the perspective of each individual silo, they may not seem that significant.



Loss of relevant information means extra risk-detection time

Within most organizations, there is no scarcity of “raw information” relevant to risk management. Unfortunately, most of this information never reaches the managers who could interpret and act upon it. Obviously, this loss of information increases the risk detection and reaction time of a company.

There are many ways information gets lost on the way to its final destination:

- ▶ An individual within the company may obtain relevant risk-related information (possible fraud by a colleague; financial problems at a client firm; safety problems with a machine; merger discussions between suppliers) but does not share it with anybody else in the company.
- ▶ The individual shares the information with a colleague or superior but it never leaves the business unit.
- ▶ Risk-relevant data never leave a silo within the company, i.e., they are not shared with managers from other divisions or functions nor with managers who have a more comprehensive, company-wide risk management responsibility.
- ▶ Managers present their data and analysis to the board in a way that is too complex for the board to understand and act upon.
- ▶ “Inconvenient” information gets ignored, possibly because acting upon this information could imply changes to apparently profitable business practices.

Examples:

In the run-up to the subprime crisis, many retail banks in the US picked up signs that the mortgage default rate of private home owners was rising. At some universal banks, this information in the retail operation was actively shared with the investment banking operation of the same bank and as a result, the exposure of the investment bank to securities backed by home mortgages was reduced. At other banks, this information was either not shared in any meaningful way or not acted upon.

At some banks, highly placed risk managers who warned about the risks involved in certain business strategies were urged not to press their case. At other banks, in the words of the report by the Senior Supervisors Group, *Observations on Risk Management Practices during the Recent Market Turbulence*, 6 March 2008 “hierarchical structures tended to serve as filters when information was sent up the management chain, leading to delays or distortions in sharing important data with senior management.”

According to a recent research project by the Corporate Executive Board, approximately half of all business misconduct is never reported by employees; 60% of information reported by employees to managers is likely never to leave the business; 21% of reported information relevant to top risks stays within silos.

Source: Corporate Executive Board, Compliance and Ethics Leadership Council, *Managing through volatility in 2009*, page 10



No risk consensus: horizontal layers

All too often, managers in different horizontal, hierarchical layers in an organization have very different perceptions and time frames when thinking and talking about performance and risk. Strategic risk analysis and its related scenario analysis tend to be the domain of executive management and the board.

Lower down in the organization, managers stress tactical SWOT analysis, operational risks and related scorecards, or very short-term budget-to-actual considerations. Where the Board asks itself, "Are we in the right markets going forward?" further down in the organization an operational manager may ask, "Do I continue selling to company X now that it has been denied credit insurance?"

In other words, managers from different hierarchical layers speak different risk languages. As a result, detection and reaction times are far longer than necessary. Again, as in the case of silo thinking, layer thinking too should be actively tackled by management to communicate the company-wide definitions, priorities, procedures and communication channels regarding risk management. Due importance should be given to the main strategic, tactical and operational risks and their interaction. Whatever the horizontal layer managers belong to, they should share the same view regarding the most important short-term, medium-term and long-term risks facing their organization and how to manage them.

Such an exercise can also help to avoid short-termism. Even in difficult circumstances, an exclusive focus on short-term risks to the detriment of attention to longer-term risks should be avoided. All too often, companies are so absorbed by short-term operational and financial issues that they dedicate all their means and management time to these questions. "How can we make the numbers for this quarter?" is, for better or for worse, a very common question in business.

Layer thinking should be actively tackled by management to communicate the company-wide definitions, priorities, procedures and communication channels regarding risk management.



Solid organizational procedures versus individual instincts

When it comes to the detection of a new risk-related event, it is not enough that some individuals within the company are personally aware of a potential new risk. As long as the company as an organization is not aware of the new threat, the risk has not really been “detected” in any meaningful way.

What use is it for a company if many of its employees saw the current economic downturn coming, if the organization as a whole failed to process this information systematically, let alone act on it. A risk is only detected in an organizational sense when it is put on the agenda of those managers that “own” this risk area and are in a position to decide how the organization should react to it.

If a marketer becomes aware of financial difficulties at one of the company’s major clients, the organization as such hasn’t detected the risk of discontinued payments by this client, unless and until the marketer informs the people in the organization who deal with the operational risk of client non-payment. In the same way, if a manager somewhere in the organization becomes aware of a possible regulatory change that may have a significant impact on the company’s business model, the company as such hasn’t detected the risk until this information has been communicated to and understood by the appropriate management.

Even if a person or business unit is ideally placed to spot a risky new development or event, they will not detect it in any meaningful way unless they know what they should be looking for and are aware of the importance of these trends or events for the broader company. Even if they realize the significance of a new risk they have spotted, they must know how to communicate this risk swiftly to those managers best placed to deal with it and prepare a response. Only with such a common risk language in place can a company act quickly to turn potential threats into opportunities.

Solid collective procedures based on a rationally designed risk language have proven that they are a much better basis for efficacy and efficiency in risk management than individual gut feelings. Managers as human beings, process of analysis and decision-making are not 100% rational. Far more often than we think, our decisions are informed by irrational emotions, deficient logic and biased thinking, as Max Bazerman rightly argued in his 2005 book *Judgment in Managerial Decision Making*. Obviously, this is especially dangerous when it comes to risk management. If no solid collective procedures are in place, chances are that instincts, group thinking and the inertia that comes from an intrinsic state of denial, significantly delay detection of and reaction to “inconvenient” new risks.

Given the importance of risk management, it is quite remarkable that there are many more proven procedures and tools to design and implement performance management than for risk management. As we explained in our recent Ernst & Young paper *A new balanced scorecard; measuring performance and risk*, an effective way to bring procedures in risk management up to the desired level is to integrate risk management in performance management tools such as the balanced scorecard.

Solid collective procedures based on a rationally designed risk language are a much better basis for efficacy and efficiency in risk management than individual instincts.



The best is the enemy of the good

Nokia and Ericsson, a classic example of different reaction times

In March 2000, a Philips microchip plant in Albuquerque, NM (USA) was hit by lightning which resulted in a fire. Production had to be halted for weeks due to the contamination of the chips and the facilities with water and smoke. The plant supplied essential parts to both Nokia and Ericsson, two major competitors in the global market for mobile phones.

When informed of the incident, Nokia and Ericsson reacted very differently. Ericsson basically waited for weeks before taking action and limited itself to monitoring Philips' updates on the gravity of the situation. Nokia immediately started to contract capacity at other Philips and non-Philips plants to make up for the possible prolonged loss of capacity at the Albuquerque plant. When Ericsson recognized the need to do the same, it was too late. All free capacity had been taken by Nokia. In that fateful year, Nokia increased its market share from 27% to 30%. Ericsson saw its market share fall from 12% to 9%.

Source: *A Comprehensive Approach to Assess Operational Resilience*: Stolker, Karydas, Rouvroye, Eindhoven University of Technology

Pick up early warning signs to shorten your risk detection and reaction time

From The Economist, *Confessions of a risk manager*, 7 August 2008:

"In January 2007 the world looked almost riskless. At the beginning of that year I gathered my team for an off-site meeting to identify our top five risks for the coming 12 months. ... The possibility that liquidity could suddenly dry up was always a topic high on our list but we could only see more liquidity coming into the market – not going out of it. ... "Where is the liquidity crisis supposed to come from?" somebody asked in the meeting. No one could give a good answer.

Looking back on it now we should of course have paid more attention to the first signs of trouble. *No crisis comes completely out of the blue; there are always clues and advance warnings if you can only interpret them correctly.* It was the hiccup in the structured-credit market in May 2005 which gave the strongest indication of what was to come."

Risk management is not an easy task. Risks are the ultimate moving target. New risks appear, old ones disappear, the relative importance of different risks changes constantly. The definition, prioritization and monitoring of its most important risks is an on-going task for an organization. Some risks are easier to detect and measure than others. Like all languages, risk management language is constantly evolving; users need to keep up to date with risks and the impacts of these risks on the business.

While it may be impossible for a company to introduce a 100% foolproof risk management system, this should not be an excuse

for inaction and confusion. "The Best" is the enemy of "The Good." In our fast-changing world, inaction is simply not an option; the faster business circumstances change, the more important it becomes to detect and react to new risks quickly. Companies can reduce this detection and reaction time by designing and implementing a comprehensive risk management system that is based on a common risk language spoken throughout the organization: common definitions, priorities, communication channels and procedures. As a result, they will be much better positioned to transform risks into opportunities and to increase their competitiveness, even in challenging circumstances.



Contacts

For enquiries about our Advisory services in the following countries and regions, please do not hesitate to contact our global team

Norman Lonergan	Global Vice Chair	+ 44 (0)20 7980 0596
Robert Patton	Americas	+ 1 404 817 5579
Andrew Embury	EMEIA	+ 44 (0)20 7951 1802
Nigel Knight	Far East	+ 86 21 2228 2189
Isao Onda	Japan	+ 81 3 3503 1100
Doug Simpson	Oceania	+ 61 2 9248 4923

Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multi-disciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.





About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 135,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

www.ey.com

© 2009 EYGM Limited.
All Rights Reserved.

EYG no. AU0314



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.