Risk management *drives* credibility and transparency

It helps to boost income, cut costs and manage intangibles such as reputation and brand

Risk management, from both a threat and opportunity point-of-view, should never be seen as a mere tag-on to other processes. It has to be fully integrated into any organisation's corporate management, favouring ethical behaviour, legal security and corporate social responsibility.

ÁNGEL ESCORIAL BONET
RISKIA

The introduction to the standard «UNE-ISO 31000-2010 Risk Management: Principles and Guidelines» states categorically that «all activities of an organisation involve risk». Later on it recommends that «organizations develop, implement and continuously improve a framework whose purpose is to integrate the risk management process into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture».

Moreover, according to Spain's Unified Good-Governance Code (*Código Unificado de Buen Gobierno*), also known as the Conthe Code, the board of director's powers include approval of «the risk management and control process and also the periodical monitoring of the internal information and control systems».

As regards the Audit Committee, the Unified Good-Governance Code recommends that its members, especially the president, «should be designated in light of their knowledge and experience in accountancy, auditing or risk management».

It also recommends that the risk management and control process should deal at least with all the following. Firstly, it has to identify the various types of risk (operational, technological, financial, legal, reputational) that the company has to cope with; financial or economic risks will include contingent liabilities and other off-balance risks. It should also establish the risk level deemed by the company to be acceptable as well as the planned measures to mitigate the impact of the identified risks and the internal control and information systems to be used for controlling and managing them, including contingent liabilities or off-balance risks.

As for the internal control and information systems, the Audit Committee, under the Unified Good-Governance Code, is considered to be responsible for «periodically reviewing the internal control and risk management systems to ensure that the main risks are pinpointed, managed and brought to wider notice».

Working from this reference framework, a Spanish school- and office-material production and distribution company hired the services of a specialist consultancy to ensure the former's compliance with the Conthe Code for listed companies and the standard UNE-ISO 31000. In this particular case the consultancy's remit was to audit the integral risk analysis that it had conducted in 2005 and whose conclusions were incorporated by the firm concerned into section D, Risk Management Control Systems, of its Annual Corporate Governance Report of this same year.

The purpose of the audit was to update the firm's risk map and bring it into line with its new business context, paying special attention to the purchase of a new company in 2009. The business of this purchased firm, with a turnover tripling the purchasing firm's, was the distribution of computer consumables; its production targeted the European market.

Phase-based approach

Working from the information and figures furnished by the firm, the consultancy's approach was phase based to fit the risk management stages: risk assessment (identification, analysis and evaluation), risk treatment (validation of the action plan by the organisation), monitoring and review (periodical auditing of the validated plan). This phase-based approach ensured optimisation of results and costs.

The study objective was to draw up a risk map and an updated draft of the action plan to optimise the organisation's risk situation and thus ensure compliance with the Unified Good-Governance Code for listed companies within the framework of the standard UNE-ISO 31000.

WORDS LIKE CONTROL, PREVENTION, LEARNING, EFFICIENCY, IMPROVEMENT OR EFFICACY ARE INEXTRINCABLY BOUND UP WITH THE CONCEPT OF RISK ANALYSIS

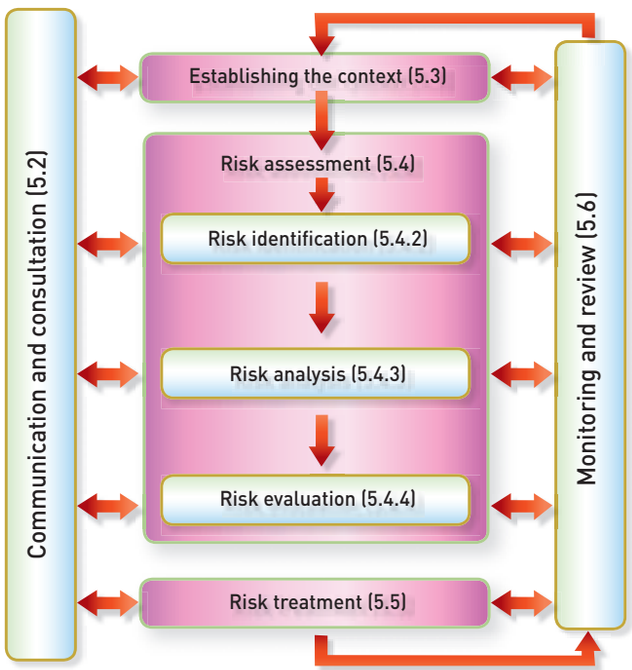
As already pointed out, it should be remembered here that the company concerned purchased a new subsidiary in 2009, whose volume and activity called for a review of the conclusions of the integral risk analysis conducted in 2005. Furthermore, while the project was underway, the company bought the continental business of a European competitor.

The consultancy's proposal for achieving the object in view involved the following steps: Audit the status of the improvement process proposed in the 2005 report. Identify and analyse the risks indicated in the Good-Governance Code, duly brought into line with the organisation's new situation, to build up an updated risk map in due accordance with the standard UNE-ISO 31000, on the basis of FERMA's risk classification. Validate the new risk improvement plan together with the firm.

Thus conceived, the project provided the company with all the following:

- An updated risk map with the desired scope.

Risk management process under UNE-ISO 31000



Source: UNE-ISO 31000

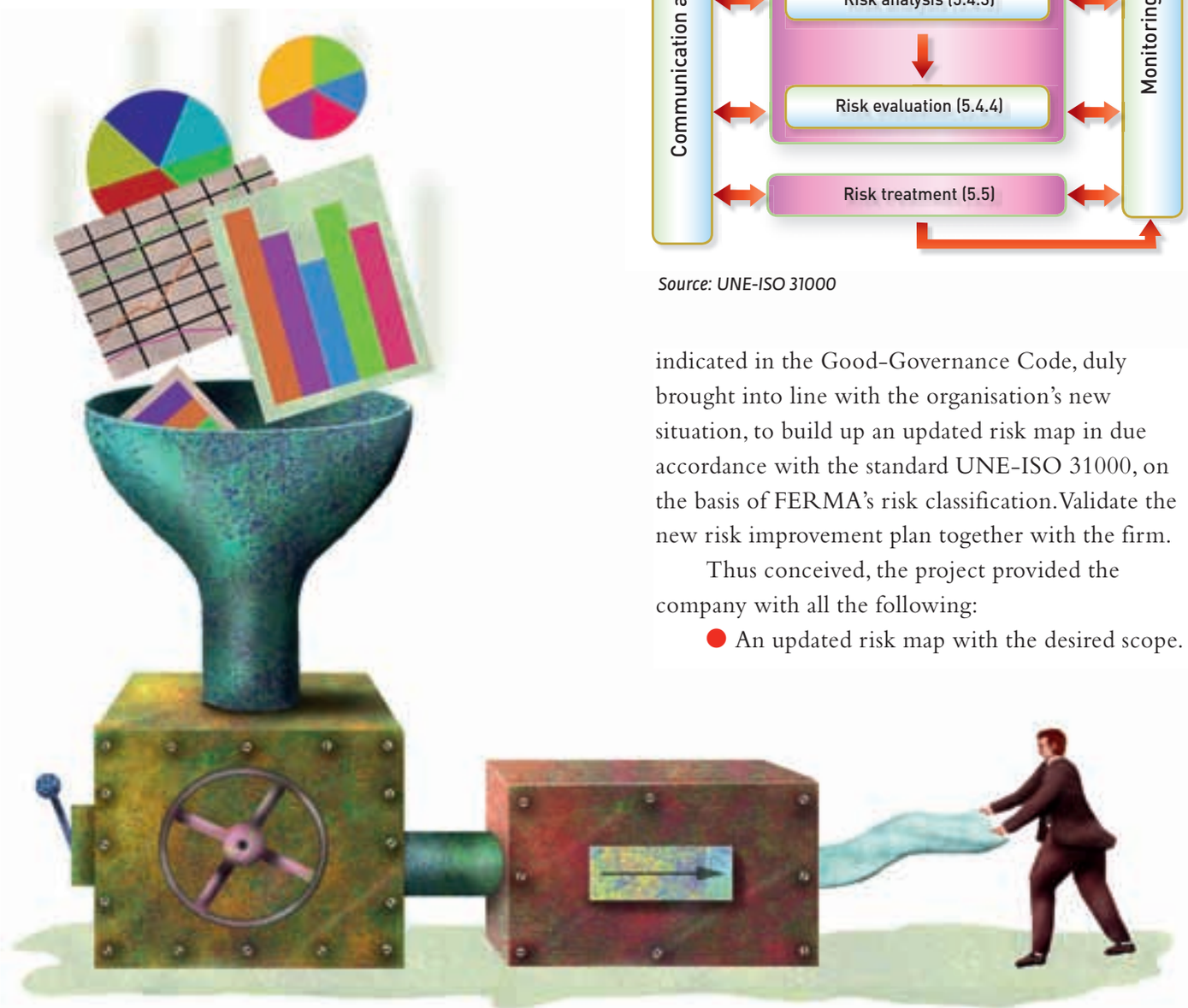
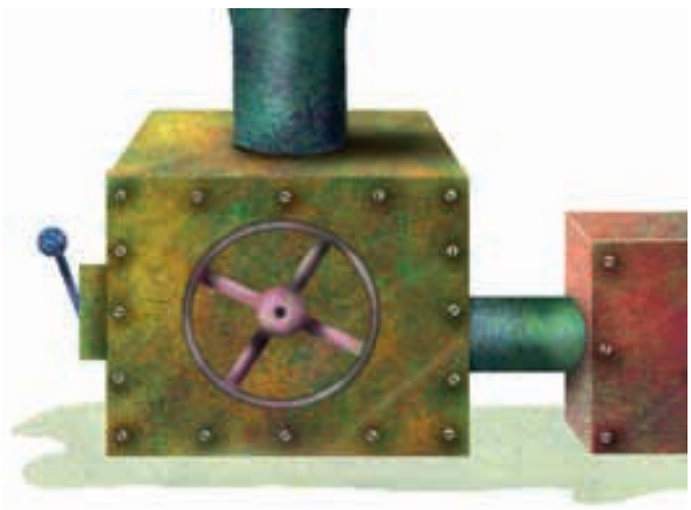


ILLUSTRATION STOCK



- A draft action plan to minimise the analysed and assessed risks.
- Validation of the plan by the audit committee.

Methodology

The audit, conducted by a multidisciplinary team of experts, pinpointed the different types of risks (operational, technological, financial, legal, reputational) faced by the company.

For the systematic management of the risks, the consultancy broke down its inventory and analysis into groups of risk in keeping with the company's structure and activities, according to the following classification:

I. Management (human resources policy, market regulation, business- and sector-culture, communication, including crisis readiness and board makeup).

II. Information systems (analysis of IT risks and physical security including cyber risks).

III. Supply chain (study of the contracts and suppliers of raw materials and supplies, including their logistics and transport, and of the products made by the organisation).

IV. Business processes (identifying bottlenecks with their back-up alternatives, taking maintenance into account).

V. Products and services (including the quality system).

VI. Environment (targeting environmental risks including those deriving from new legislation on the protection of natural sites and resources).

VII. Properties (taking in not only traditional internal risks like fire and explosion but also those deriving from public access and external natural events like floods and earthquakes).

VIII. Employees (focusing on health and safety aspects).

The eight abovementioned groups would take in operational risks and hazard risks as laid down in the scheme of the Federation of European Risk Management Associations (FERMA) and studied under the integral risk analysis conducted by the consultancy back in 2005.

The scope of the new analysis was broadened, incorporating Strategy and Finances into the abovementioned groups.

IX. Strategy (analyses the organisation's market situation, studying such aspects as competition, customer demand, customer- and industry-changes, the life cycle of products and services, potential mergers and acquisitions and the organisation's intellectual capital).

X. Finances (analyses the organisation's liquidity, cash flow, interest- and exchange-rates and credit).

The scope of the work carried out would thus cover the whole spectrum of the FERMA risk classification, with the 2005 risk analysis being updated to the current situation taking into account the purchase of the new company and the new strategic and financial risk groups. This meant that an opinion in keeping with the Unified Good-Governance Code could then be issued.

Risk evaluation involved the same semi-quantitative method of potential scenarios and their effects, as used back in 2005. This meant that past results could be harnessed, cheapening the cost of the project.

The semi-quantitative method of potential scenarios combines several of the techniques laid down in the new UNE-ISO 31010 standard, assigning to each identified risk a value from 1 to 16, the result of multiplying their intensity / severity by their probability / frequency, each one scored from 1 to 4.

Three risk-valuation thermometers were used:

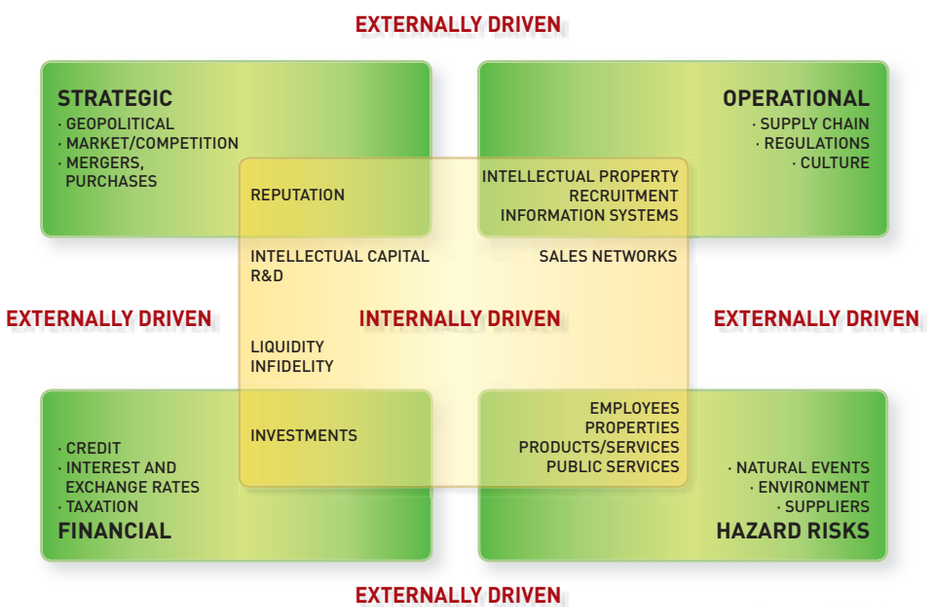
- **ERL:** Estimated risk level in 2005.
- **ARL:** Audit risk level in 2011.
- **TRL:** Target risk level.

The intensity / severity and probability / frequency for each risk scenario were rated from 1 to 4 according to the following criteria for each one of the variables considered:

Intensity, severity:

1. Moderate: If the consequences call for the modification of some resources or processes, causing economic disturbances that can be assumed in the results for that year.

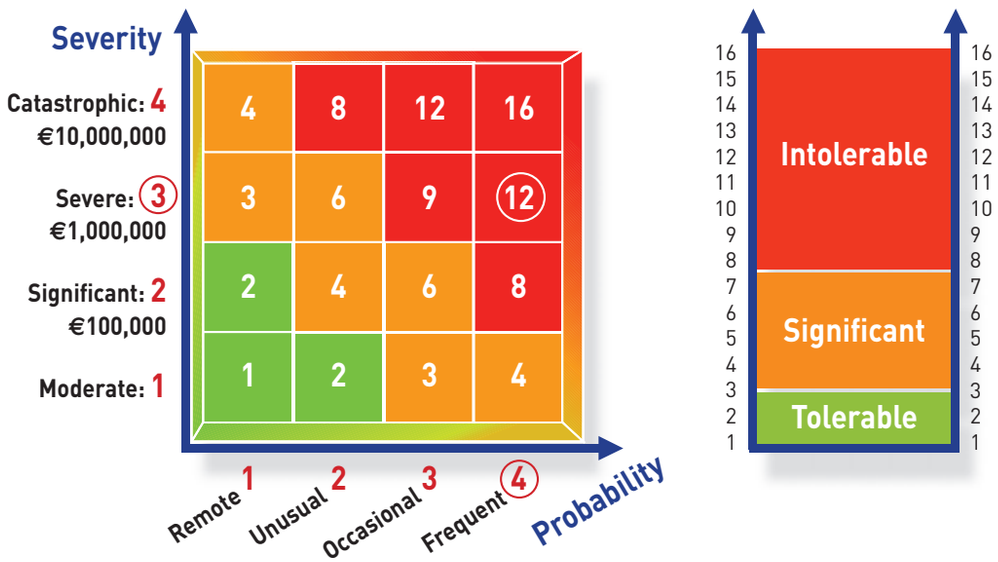
EXAMPLE OF EXTERNALLY AND INTERNALLY DRIVEN FACTORS



Source: FERMA.

RISK MANAGEMENT SHOULD BE FULLY INTEGRATED INTO ANY ORGANISATION'S CORPORATE MANAGEMENT, FAVOURING ETHICAL BEHAVIOUR, LEGAL SECURITY AND CORPORATE SOCIAL RESPONSIBILITY

RISK TRAFFIC LIGHT



Source: Riskia.

2. Significant: If the losses cause considerable short-term difficulties calling for the modification of some objectives and a knock-on effect on results for the year.

3. Severe: If their impact on results is such that the organisation not only has to tweak its short-term objectives but also rethink all its future plans.

4. Catastrophic: If they threaten the organisation's very survival.

Probability or frequency:

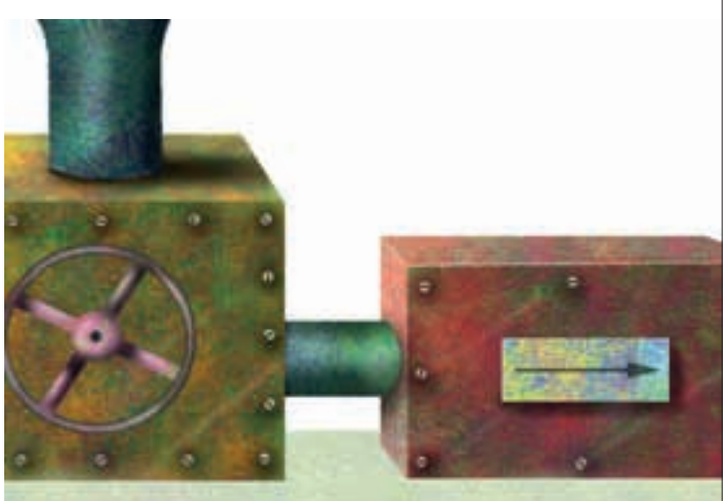
1. Remote: If the event concerned happens only extraordinarily (once a century or once in the organisation's existence).

2. Unusual: If it happens rarely (less than once a decade).

3. Occasional: If it happens once a decade.

4. Frequent: If it happens every year.

The estimated score obtained for each risk (on a scale from 1 to 16) gives a value that is classed in three zones of the thermometer under the ALARP



INTEGRAL RISK ANALYSIS ALSO FACILITATES COMPLIANCE WITH THE COMPANY'S LEGAL AND REGULATORY REQUIREMENTS

method (The ALARP method is defined in annex B27 of the standard UNE-EN 31010 and is put forward as ideal for risk management purposes):

- **Red**– intolerable risks.
- **Orange**– ALARP zone (As Low As Reasonably Practicable).
- **Green**– broadly acceptable risks according to the organisation's risk policy.

For each risk analysed and assessed (outside the acceptability zone), the consultancy proposed an improvement action to bring it down to a target risk level (TRL) in keeping wit the organization's risk policy, so that:

- As regards the risks of the 2005 report, the consultancy audited their current state. At the same time it checked for the appearance of new risks or the disappearance of old risks.
- For increases of scope (taking into account the company bought in 2009 and the strategy and finances groups) the indicated process was carried out from scratch.

The consultancy's report proposed minimisation measures for each risk analysed, such as the following:

1. Elimination technique from position A to D (tolerable).
2. Combination of risk minimisation measures to bring it down from A to D, passing through B (by applying probability-reducing prevention measures); to C (by applying severity-reducing protection measures) for a subsequent transfer (insurance or other contract) to position D.

A weighted measure can then be obtained of the risk levels of the risk groups analysed; this would represent the Overall Risk Level.

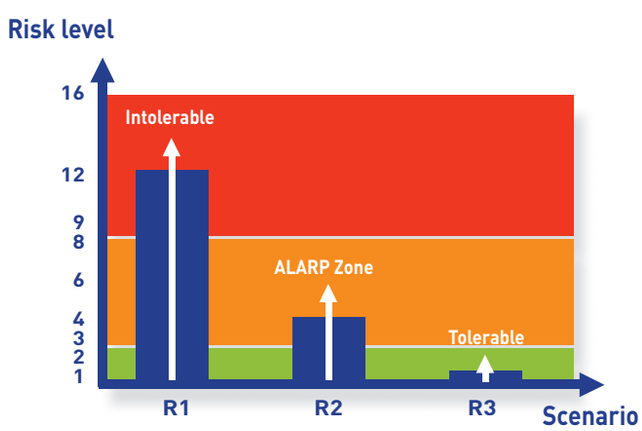
This Overall Risk Level is then broken down into an Estimated Overall Risk Level (estimated initially), an Audited Overall Risk Level (audited at each moment) and a Target Overall Risk Level, all of which then serve as global indicators of the improvement process. These indicators can be customised for each risk group or industrial establishment in the case of operational and hazard risks.

The consultancy used a colour system to facilitate monitoring of the risk inventory and of the improvement measures, as follows:

- Risks and actions of our 2005 report in black.
- Auditing and updating of the new 2011 risks in blue.

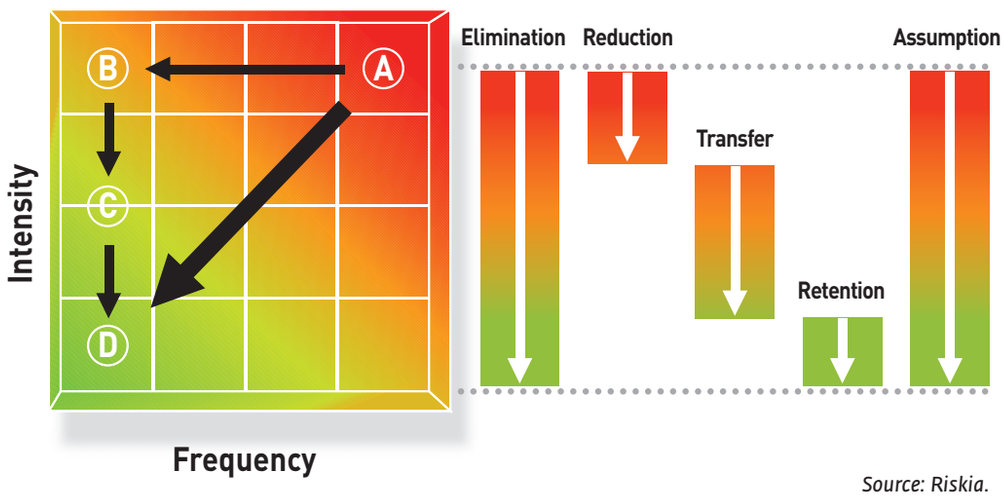
In June 2011 the consultancy company issued a preliminary report with the factfiles of the 10 groups

ALARP Method (*As Low As Reasonably Practicable*)



Source: Riskia.

Risk management safety cycle



Source: Riskia.

that had been sent to the company coordinator, who then sent them out to the various interlocutors for their comments. The company's resulting notes and comments were recorded in red, as were the activities to be taken by the organisation or even those planned as a result of the preliminary report.

The consultancy used the following ratings for its monitoring system:

- Pending, when no efficient measure has yet been taken.
- Underway, when measures have been planned but not yet enforced.
- Partially executed, if the measures partially reduce the risk.
- Eliminated, if the risk has disappeared when the audit is conducted.
- Assumed, if the risk is taken on by the organisation.
- Executed, if an effective minimisation measure has actually been carried out.

Threats and Opportunities

The consultancy established the 2011 risk map (both threats and opportunities) breaking down company risks into ten groups according to the FERMA risk classification, as already pointed out. The risk-identification and -assessment methodology used in a severity vs. probability map was in line with the standard UNE-ISO 31000.

Together with the 2011 risk maps, the consultancy's report included comments on the standout aspects of each one of the groups analysed and a comparative analysis of the target risk of the proposed indicator system for monitoring the level of each one of the ten risks from 2005 to 2011.

Likewise, the company was furnished with a set of indicators for periodical monitoring, internal and external, for controlling and managing identified risks.

INTEGRAL RISK ANALYSIS ALLOWS AN ORGANISATION TO IDENTIFY AND DEAL WITH ITS RISKS IN A PROACTIVE MANNER. THIS HELPS TO HEAD OFF THREATS AND PINPOINT IMPROVEMENT OPPORTUNITIES THAT INCREASE A COMPANY'S CHANCE OF ACHIEVING ITS STRATEGIC TARGETS

Risk card model

XXX Risk Audit

Group I. Management risks
Risk 1.1: Contingency plan

Action by XXX		
	RESPONSIBILITY PART:	**To be defined**
	IMPLEMENTATION DATE:	**To be defined**
	STATUS / SITUATION:	**Pending**

ERL	RISK DESCRIPTION	ARL	IMPROVEMENT ACTIVITY (2012)	TRL
L=3 P=3	XXX factories are complementary and neither could stand in for the other in the event of a significant accident in any of them. It would therefore be necessary to replace lost production by turning on the market. The firm does not have a contingency plan laying down action to be taken in the event of any accident or production shutdown, based on analysis of its response to a series of events such as fires, floods or other that might shut down one of the plants for a significant length of time.	L= P=	Drawing up a contingency plan defining all of the following: 1.- Appointing a coordinator and considering possible events (fire, flood, power fault, transport strikes, etc.). 2.- Definition of backup of key tasks and functions. 3.- Setting up teams and assigning responsibilities. 4.- Definition of plan-triggering conditions. 5.- Training and awareness raising.	L=1 P=1

16 15 14 13 12 11 10 09 08 07 06 05 04 03 02 01

Source: Riskia.

In its conclusions the consultancy proposed an action plan with a series of minimisation measures for each identified risk-threat, with the aim of reducing the likelihood of its occurrence and mitigating its impact if it should materialise.

The conclusion we can draw from this article is that integral risk analysis allows an organisation to identify and deal with its risks in a proactive manner. This helps to head off threats and pinpoint improvement opportunities that increase a company's chance of achieving its strategic targets, pursuant to UNE-ISO 31000.

Integral risk analysis also facilitates compliance with the company's legal and regulatory requirements. For example, the provisions of the Unified Good-Governance Code or Conthe Code for listed companies, or section D of the Annual Corporate Governance Report on risk management.

Words like control, prevention, learning, efficiency, improvement or efficacy are inextricably bound up with the concept of risk analysis, whose implementation provides the company with a trustworthy base for planning and decision making.