Article 02

ERNST & YOUNG
Quality In Everything We Do

EFFECTIVE RISK MANAGEMENT

BACK TO THE BASICS OF BUSINESS

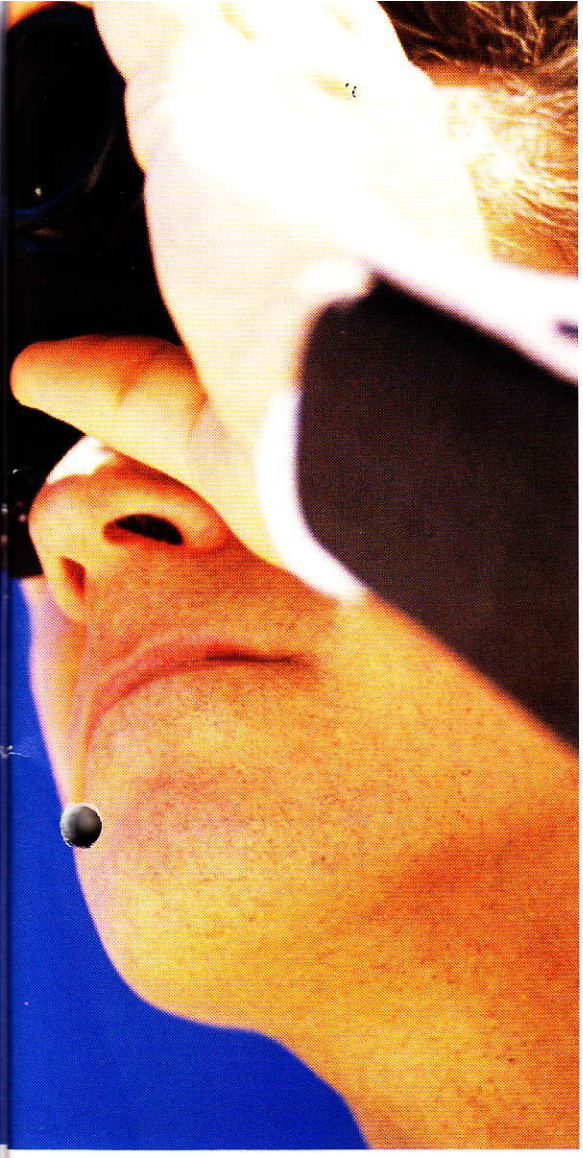
Drs. M. de Pooter RA CMA CFM CIA,
Ernst & Young – Director, ERM Solution Leader, The Netherlands

Introduction

The credit crunch has brought the financial sector to the center of media attention. This sector that spends many millions of Euros on risk management had to report write-offs and losses amounting to many billions. How much more disturbing can things become?

Many scholars and journalists have written analyses about the things that went wrong and which parties in this big game should be blamed and how much. Commonly heard accusations include: legislators introducing fair value accounting, investors demanding too high returns, credit rating agencies incorrectly valuing financial products, regulators misjudging risk profiles, executive management failing to grasp the complexity of their own financial products, supervisory boards granting inappropriate remuneration packages, risk managers using incorrect assumptions and data in their risk quantification models, risk management functions without sufficient influence, status or power, auditors failing to ask the right questions, etc.

In this article I want to briefly explain the basics of risk management and the application thereof in practice. The approach outlined below can be applied to any level (e.g. group, division, subsidiary, department, and project) within an organization.



Risk management – not just an academic hobby horse

Companies and their shareholders earn money by undertaking business activities. Company management is exposed to risks as a result of that. In order to maximize profits, to ensure continuity, to avoid accidents, etc. the executive management has to manage a large variety of risks. That makes risk management part and parcel of their daily jobs.

Risk management is the ability of management to successfully deal with uncertainty. In daily practice each of us deals with managing risks. Imagine you have to deliver a presentation at a conference. You want to give an online demo of a new application, requiring broadband internet access. It probably won't take you long to imagine what could go wrong, resulting into you not achieving your objective of impressing your audience. Maybe the wireless signal is too weak, the bandwidth is insufficient, access is only feasible by using a credit card, etc. As you are responsible for delivering the presentation, you are going to analyze which controls are required to give you reasonable confidence and assurance that you will be able to deliver. Controls are management actions to achieve certain objectives. In this case you may opt for a cable connection instead of wireless, a second laptop or USB-stick as back-up, timely availability of technical support staff, etc. That is to say 'realistic' controls, as some might be too expensive or require too much effort. Obviously, you'll make sure that you arrive on time, e.g. by staying the night before. And you will consider a suitable 'Plan B', in case the internet connection doesn't work at all, such as showing off-line screen shots, etc.

Risk management – what it is all about

'Risks' are future events that could hamper the realization of your objectives. Likewise, 'opportunities' are future events that could help the realization of those objectives. Without proper clarification of the scope and the objectives in question, effective risk management becomes hard to achieve. The risks and controls in question need to be identified and prioritized. Responsible management also needs to assess if those risks are at acceptable levels and if the organization is sufficiently equipped to seize opportunities. This is the design effectiveness assessment. In other words, asking: "Are we doing the right things?" To the extent that is not the case, management needs to implement additional or improved controls. Last but not least, management needs to establish that the controls work as intended. In other words they should ask: "Are we doing (the agreed) things right?" This is the operational effectiveness assessment. The evaluation of the design and operational effectiveness forms the basis for the conclusion whether the organization is 'in control' or not. It is also the basis for risk management reporting to the supervisory board, regulators, etc.

'Value management' – a better term

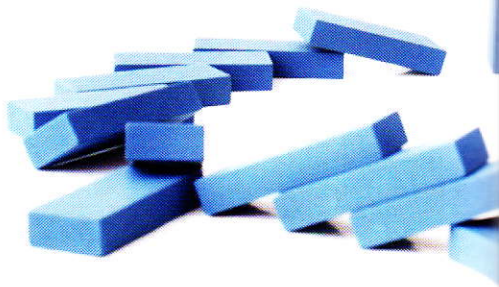
Enterprise Risk Management ('ERM') is an organization-wide process to identify potential events that might impact the realization of business objectives. In order to ensure that the risks remain within the desired risk profile(s), measures are required to ensure that the organizational objectives are achieved. Traditional risk management approaches the future from a negative angle: a variety of unpleasant things may happen that should be avoided. Consequently, risk management and performance management were considered to be separate worlds until recently. However, both profit and non-profit organizations can benefit from a more integrated approach. The latter could be labelled "value management", i.e. creating and preserving value within the organization.

Making value management more tangible

By focusing on 'value' the emphasis shifts to the 'assets' of the organization – in the broadest sense of the word. So, not only tangible and financial fixed assets (such as equipment, stocks, receivables and cash), but particularly also the intangibles (such as patents, employees, brands and reputation). Assets contain value or can be used to generate (additional) value. For example, a good account manager can ensure profitable contracts. A very practical approach for effectively applying risk management in a specific situation is by focusing on the key assets in question.

Article 02

ERNST & YOUNG
Quality In Everything We Do



Internal control - unique for every organization

Internal control is inextricably linked with risk management. At the heart of internal control is the aggregate of measures ('controls') that management takes in order to ensure that certain objectives are realized. As every organization has its own culture and every situation is unique, risk management and internal control vary by entity. Differences relate to: the expectations of the stakeholders, the business model, the maturity of the organization, the risk appetite of the owners and management, etc. In practice, risk management often takes place in more implicit ways, e.g. when making investment decisions, when selecting suppliers, when hiring employees, etc. Usually, the analyses are performed by separate functions or departments familiar with specific risk categories, e.g. IT, Treasury, Health & Safety, Environmental, Finance & Controlling, etc. Therefore, it is quite common that a variety of separate, mostly independent, risk management systems exists, implemented for historical reasons and usually driven by regulators.

The benefits of good internal controls

Many reasons can be mentioned why management can benefit from effective internal control. The main benefit is that it allows management to achieve the organizational objectives in a structured way. Good internal control requires an overview of the risk categories that matter, so that they can be managed and prioritized better. If management succeeds at that, it becomes much easier to convince bankers and other financiers that their money is in safe hands. That will result into lower risk premiums, i.e. lower interest charges.

Implementing value management in practice

Good value management can help management at all levels to achieve their business objectives. Those objectives are aimed at creating and preserving value for their stakeholders, such as: clients, employees, shareholders, the government, regulators, neighbours, etc. In order to achieve those objectives, managers need take measures for their areas of responsibility. Those measures are known within the organization as the 'rules of the house', such as: charters, policies, procedures, instructions, manuals, etc.

Internal control in practice

Basically, internal control comes down to ensuring that there are adequate 'rules of the house' and that they work as intended. Those rules (both in writing and verbal) are intended to steer the behavior of the employees in the direction chosen by management. Those rules have been implemented in the course of time and sometimes maintained poorly due to cutbacks in expenditure, the departure of employees, reorganizations, changes in processes, etc. Factors like these make it hard for management in question to keep an overview of their own rules. This in turn can lead to situations that conflicting rules are issued, causing confusion for the employees in question. That is why the 'governance' of the rules is so important and essential to avoid an excessive 'control burden' by balancing costs and efforts of controls versus the reduction of risk exposure.

The level of formalization

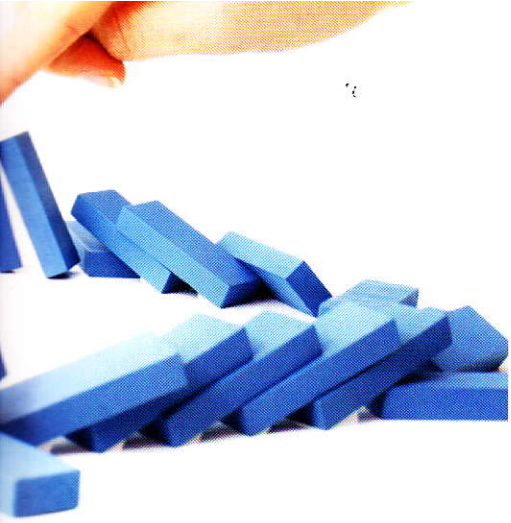
In practice many important internal control activities are carried out implicitly, i.e. management and other employees often aren't even aware of their risk considerations. Typically, the larger, older and more complex the organization is, the more formalized is the internal control structure. For larger organizations, particularly those that are monitored by external parties like regulators, it is crucial that management can substantiate that it is 'in control' over the realization of their objectives. Consequently, more information needs to be documented, analyzed, reported, etc. The extent to which this needs to take place obviously depends on the laws and regulations in a particular situation.

Achieving effective internal control

The following steps are important to get and stay 'in control'. They can be applied to every level within an organization.

1. Determine the objectives, aimed at creating and preserving value for the stakeholders. In addition, determine the extent of acceptable deviation.
2. Analyze which future events could hamper (risks) or help (opportunities) the achievement of the organizational objectives. This step is about the identification and weighing of potential events that could impact the realization of those objectives.

ERNST & YOUNG
Quality In Everything We Do



3. Inventory and document the current controls, aimed at ensuring the realization of the business objectives.
4. Determine whether the current controls are sufficient to ensure that the deviations of the desired results are within acceptable limits. In addition, decide which controls need to be implemented or improved and which ones are redundant.
5. Properly document the 'rules of the house', so that those responsible know what is expected from them and implement the necessary modifications.
6. Monitor whether the 'rules of the house' are being followed through daily management supervision, business reviews, control self-assessments, (internal and external) audits, inspections, etc.
7. Evaluate to which extent the business objectives are realized and which internal control improvements are required. This is also the basis for the risk management reporting to the oversight functions.

Finding the right balance

Value management is rather art than science. It is about management's competences to deal with the uncertain future. It requires a lot of judgement, e.g. about what the stakeholders really want, what the likelihood and effects of the risks and opportunities are, what the adequacy and effectiveness are of the measures taken by management, balancing costs and benefits. And particularly, judgement regarding balancing the perceived and the desired (i.e. based on the risk appetite) risk profiles.

Determining risk tolerance in practice

Risk appetite is about the likelihood and impact deemed acceptable for specific (undesirable) events, e.g.:

- How much money is management allowed (e.g. by regulators), willing (e.g. by the supervisory board) or able (e.g. in view of the financial position) to loose, if a large new product development project turns out to be not successful?
- How long is management willing to accept (start-up) losses caused by a new branch or outlet?
- How many and how serious complaints from customers does company management consider 'reasonable', 'normal', etc.?

Risk appetite can be determined in practice simply by asking responsible management about:

- Specific future situations deemed unacceptable;
- Incidents, accidents, write-offs, losses, etc. that stakeholders view as (totally) unacceptable;
- Circumstances that require immediate management action and escalation.

Who should be responsible for what?

It is the role of top management to define the areas of responsibility for each of the functions within the organization. Effective risk management requires clear setting, cascading and communication of the business objectives. Business processes and initiatives exist to realize these objectives in practice. It must be clear to the process owner, usually line management of an organizational entity, what the requirements are, stipulated by third parties (e.g. governmental and regulatory agencies) versus the matters that are left at their discretion. Each process owner then needs to determine which controls are suitable, in view of the perceived risks, cost-benefit considerations, etc. Last but not least (s)he also needs to monitor if the quality of the business process or initiative is within acceptable tolerances. Based on that (s)he can then report on the status of 'in control'.

Explicitly deciding about the 'rules of the house'

Deliberately deciding not to stipulate 'rules of the house' implies that directing and controlling of the situation is left to the own judgement of line management in question. The benefits of the freedom to make decisions locally can outweigh the benefits of centralization and standardization. Examples include: selection of suppliers, background checks, flexible office hours, teleworking, salary ranges, internet usage, etc.

Many organizations struggle with making their internal rules specific, transparent, accessible, etc. This includes questions such as:

a. Who can issue which 'rules of the house' and how often?
b. Are our rules clear for the intended audience and mutually consistent?
c. Have our rules been documented in ways that facilitate maintenance in the future?
d. Are our rules updated on a timely basis?

ERNST & YOUNG
Quality In Everything We Do

e. Do we have too many rules?
f. Can we leave more at the discretion of our managers and employees?
g. Are our internal rules sufficiently transparent for our regulators?

It is recommended to use the organization's intranet as the one stop repository for all the 'rules of the house'. That infrastructure will also facilitate accessibility and regular updates of all relevant rules.

What is needed in practice

Several key aspects of the organization's culture and management reporting appear to be powerful enablers of successful Enterprise Risk Management in practice. They include:

1. The univocal support of top management and their attitude (underscoring the importance of internal control, making people feel responsible for it, walking their own talk, dealing with resistance where needed, punishing those who violate the 'rules of the house', etc.).

2. The allocation of responsibilities for the realization of objectives, hence also for managing the related risks and opportunities. Clearly linking risk categories to responsibilities within the organization avoids gaps, overlaps and inconsistencies in risk coverage. Gaps can arise, when e.g. everyone assumes that somebody else takes care of managing a given risk.

3. Aligning the incentives and rewards systems with effectively managing the risk exposures within the organization's risk appetite. Excessive short-terminism, coupled with a lack of accountability can have disastrous economic effects.

4. Including key indicators (e.g. performance or risk indicators) in the existing management reporting appears to be a very effective way to inform those responsible for achieving the objectives about the quality of the business processes. Defining bandwidths to business objectives ('risk tolerances') can be used to apply the concept of 'risk appetite' in practice. However, carefully selecting a suitable number of key indicators turns out to be a challenge for many organizations.

A key lesson learned from the credit crunch

Risk management is all about human behaviour and capabilities. Behaviour is only predictable to a certain extent. It is also influenced by factors such as: greed, herd reflexes, short term focus, incomplete information, limited judgement, etc. Nevertheless, applying the integrated risk management approach outlined in this article can help boards to create and preserve value for their organizations in practice. Provided it is always based on sound integrity principles.