

EFFECTIVE RISK MANAGEMENT —

THE FOUNDATION FOR EFFECTIVE RESILIENCE

DR TED DAHMS

(15 March 2009)

Much public analysis and finger pointing has occurred in an attempt to identify the triggers for the current global financial crisis. Two related but incorrect assertions have emerged from this process. One is that conventional risk management has failed. The second is that organisational resilience, supported by corporate governance and risk management, is the new assurance process for promoting business success.

It is clear from a majority of the public analysis that the causes are complex involving failures in legislation, regulation and governance practices. Running through all of the identified causes is the failure to understand and apply sound risk management principles by legislators, regulators and those elected or paid handsomely to know better. Distillation of the public analysis provides a number of examples to support this view.

The traditional linkage between risk and return was ignored and the focus was on funding risks rather than managing them. There was an increased reliance on computer modelling without sufficient attention to past events, the value of human judgement or allowance for outsized events. In some cases those charged with making critical decisions unquestioningly relied on the judgement of rating agencies, thus abrogating their fiduciary obligations.

Underpinning these issues is the reliance, at least in the US, on guidance from the COSO ERM Standard which falls far short of best practice and is regarded by some commentators as being more of a hindrance to the implementation of effective risk management than a help. Criticisms of COSO include its: size and lack of clarity; focus on negative impacts, internal control and compliance, mostly financial; focus on reporting risks rather than managing them; and lack of practical guidance for implementation of an effective system of risk management.

The management of risk is an uncomplicated process used daily by people to achieve objectives. Examples include getting to work on time and safely, meeting appointments and deadlines, driving, crossing the road. The process of setting the objective, identifying and assessing the level of risk and developing strategies (risk treatments) to achieve the objective is intuitive. We don't notice it because it is part of normal life. In contrast, organisations are required to develop a separate, resource-hungry risk management framework that duplicates the processes intuitive in normal business practice.

The new international Risk Management Standard ISO 31000, due for release in the last quarter of 2009, is an evolution of Australian/New Zealand Risk Management Standard (AS/NZS 4360-2004). It retains the proven simplicity of the AS/NZS 4360 process, but includes a number of conceptual changes that serve to absorb the management of risk as part of an organisation's overall managerial framework rather than as a separate process.

ISO 31000 at around 25 pages in draft form is clear and concise (COSO over 100 pages not including attachments). In defining risk as the effect of uncertainty on objectives it clearly places risk as part of each objective, embraces external as well as internal risks, and includes risks from all sources not just financial. The risk management process is more appropriately placed with the processes of planning and performance reporting.

A number of significant outcomes arise from this definition: the risk management process is integrated throughout the organisation with objectives; responsibility and resources for the management of risk can be clearly assigned facilitating the assurance processes for accountability; capability and commitment for the management of risks are enhanced throughout the organisation; risk registers arranged by objectives transform risk information into knowledge; and resources used in duplicating the process as a separate compliance exercise can be redirected to more effective uses. The ISO 31000 process is uncomplicated, cost effective and performance focused.

Resilience is an objectives focused concept as are corporate governance and risk management. Corporate governance is an organisation's strategic response risk where risk is defined as the effect of uncertainty on objectives. Resilience is the response to unexpected events and part of an organisation's uncertainty profile.

Various elements of uncertainty are predictable and identified when developing risk registers against objectives. There remains uncertainty in the form of unexpected events that are either threats or opportunities, both having an upside and a down side. Resilience fits into this risk management space.

The resilience discussion in the current literature is focused on low probability, high consequence events such as extreme weather events and terrorism. However, resilience exists in a continuum from mild to extreme as unexpected events resulting from the complex and dynamic nature of an organisation's operating environments, both external and internal.

The study of resilience is useful in identifying a suite of strategies (risk treatments) to address the strategic objective of resilience. However, the underlying methodology is risk management and the ultimate aim is sound corporate governance.

Corporate governance is therefore the overarching concept through its focus on corporate objectives and risk management is the methodology. All of the processes that help achieve these objectives are under the direction and control of the governing body. Resilience cannot exist by itself outside of this framework because it is the governing body that is responsible and accountable for it as an objective and a strategy, the latter the result of application of the risk management process.

Resilience would be enhanced by governing bodies issuing a discrete resilience policy, placing resilience as a strategic objective and translating this objective down through the organisation. To elevate resilience above corporate governance and risk management serves not only to confuse the issues, creating turbulence and fad fatigue, but more importantly to devalue the findings from its study.

RMIA is strongly of the view that any organisation with an effective risk management framework will achieve sound corporate governance, a feature of which will be organisational resilience.

Ted Dahms

P: 07 3273 2396

M: 0408 756 272

E: ted.dahms@plumcon.com.au