

# ORGANISATIONAL RESILIENCE

## AN OUTCOME OF EFFECTIVE RISK MANAGEMENT

### INTRODUCTION

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. 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.

### RESILIENCE

The claim that organisational resilience, supported by corporate governance and risk management, is the new assurance process for promoting business success is incorrect on two counts.

In the first instance resilience is the capability of an organisation or its parts to respond quickly to uncertainty. The process for addressing uncertainty is risk management as outlined by AS/NZS/ISO 31000:2009. The key to understanding this proposition is the complex nature of uncertainty.

Uncertainty has a number of aspects. It is possible to anticipate some elements of uncertainty 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. However, even those elements of uncertainty that can be anticipated are in themselves subject to uncertainty due to the complexity of relationships within and without an organisation, i.e. organisations operate in complex adaptive systems.

The literature on resilience concentrates on disasters i.e. unpredictable, low likelihood, high consequence risks and is more akin to business continuity and disaster management. However, the definition of resilience has a much broader intent —

*The adaptive capacity of an organisation in a complex and changing environment<sup>1</sup>.*

---

<sup>1</sup> Organisational Resilience Standard. ASIS SPC.1 – 2009.

This definition remains incomplete and a more informative definition of resilience would be —

*Resilience is an organisation's state of being resulting from the management of uncertainty in a complex adaptive system. An indicator of this state of being is an organisation's adaptive capacity.*

In essence, resilience is the outcome of the risk management process, i.e. managing uncertainty.

In the second instance corporate governance is all about control assurance, which in turn is reliant on the ability of an organisation to anticipate and manage uncertainty. The conceptual foundation for this rests on an awareness of the organisation's operating environment and its connections within that environment. Awareness is facilitated by: the effective integration of risk management; adopting a broad view of control; and developing an understanding control assurance processes.

## **INTEGRATION 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, under existing ERM processes, organisations are required to develop a separate, resource-hungry risk management framework that duplicates the processes intuitive in normal business practice

The key to full integration of the risk management process is the realisation that the purpose of risk management is not risk management perse but the achievement of objectives. This reflects the intent of the definition of risk in AS/NZS/ISO 31000-2009 as "the effect of uncertainty on objectives". This simple change links risk and objectives throughout the organisation. A further significant outcome of this shift in thought is that risk treatments are also controls and strategies for achieving an objective, which in turn links the processes of risk management, planning and performance reporting.

A number of significant outcomes arise from this definition:

- the risk management process is effectively integrated throughout the organisation with objectives;
- responsibility and resources for the management of uncertainty can be clearly assigned thereby facilitating the assurance processes for accountability;
- risk registers arranged by objectives transform risk information into knowledge;
- resources used in duplicating the process as a separate compliance exercise can be redirected to more effective uses;
- the compilation and review of risk registers become part of the planning process;
- performance reviews against key performance indicators provide a real-time review of the effectiveness of the risk management system; and
- capability and commitment for the management of uncertainty are enhanced throughout the organisation (builds awareness and supports resilience).

The AS/NZS/ISO 31000-2009 process is uncomplicated, cost effective and performance focused.

## **CONTROL ASSURANCE**

A concise statement of corporate governance defines it as —

*The manner in which an organisation is directed and controlled to achieve its objectives<sup>2</sup>.*

Risk management develops the control environment and it is the control environment that provides reasonable assurance that an organisation's objectives will be reached within an acceptable level of residual risk. This statement provides the linkage between risk management, control and governance. It supports the view that the process of governance is risk management, i.e. it is the "manner" in the above definition.

The process of corporate governance therefore is risk management and resilience the outcome of governance, not the reverse.

There are two additional concepts that enhance the value of risk management. The first is that the concept of internal financial control ceased to be the overarching view of control more than a decade ago. The concept of control now covers all activities after the strategic direction has been set and it includes external as well as internal factors. Any system that restricts its view of control to internal financial control would be so woefully inadequate in addressing uncertainty as to be negligent.

The second is the importance of internal audit in providing governing bodies with independent, objective assurance over their company's control environment and therefore its risk management system. It is in a director's personal interest and in the interest of their company to ensure that its internal audit service has the skills to cover all of the company's activities, not just internal and financial, is adequately resourced and that its program focuses on the areas of key business risk for the company. Oversight of the internal audit function is a critical audit committee responsibility, neither the CFO nor the CEO.

RMIA is of the opinion that any organisation that effectively addresses uncertainty will have sound governance and also be resilient.

The attractive part of applying AS/NZS/ISO 3100-2009 is that governance and therefore resilience can be enhanced by the refinement and re-alignment of standard management practices. An uncomplicated methodology outlining how the management of uncertainty can be leveraged to provide control assurance and resilience is available in Standards Australia's HB 254-2005 entitled "Governance, Risk Management and Control Assurance".

The issues in this Position Paper are taken from an article by Ted Dahms<sup>3</sup>.

---

<sup>2</sup> *Corporate Governance, Beyond Compliance*. Audit Report N0. 7 1998-99. Queensland Audit Office, June 1999.

<sup>3</sup> Ted Dahms, 2009. *The Road to Resilience is Paved with Sound Risk Management*. New Paradigms for Risk Professionals. RMIA 2009 Conference.