RISK MANAGEMENT AND CORPORATE GOVERNANCE ARE THEY THE SAME?

In the first of a two part series examining how risk management can be leveraged in a cost effective way to underpin sound governance **Ted Dahms** outlines the close relationship between risk and objectives.

This two part article was prompted by recent contributions to Risk Management entitled *We Need a Common Definition of Risk* (Michael Rasmussen) and *Tuning in for the Results* (Shaun Drummond). It is not intended to directly address or critique issues raised in the previous papers but as a further conceptual contribution to the understanding of risk management, control, corporate governance and compliance. The core conceptual view in this article is that corporate governance is an organisation's strategic response to risk[1], i.e. the short answer to the question posed in the title of this article is yes.

The current enterprise-wide concept on risk management has the process undertaken across all areas of an organisation. In application however, risk management continues to exist as a discrete activity without clear integration as part of normal business practice. The definition of risk in AS/NZS 4360: 2004 stating that risk is "*the chance of something happening that will have an impact on objectives*" indicates that risk should be treated as part of each objective. When applied in this way risk treatments for the mitigation of risks are at the same time controls providing reasonable assurance that objectives will be reached, and strategies for achieving those objectives. This has a number of significant advantages —

1. The management of risk is no longer a separate exercise but part of the planning process and is truly integrated throughout the organisation as an element of normal business practice.
2. Risk registers arranged by objectives are transformed from information to knowledge with the added advantage of stimulating universal buy-in.
3. Any variance from expected performance measured through KPIs indicates either that the risk treatments-controls-strategies for that objective are not as effective as planned or that the risks associated with the objective have changed. Risk reporting then becomes linked to standard performance reporting rather than a separate exercise.
4. Everyone who has responsibility for achieving an objective also has the responsibility for managing the risks associated with that objective and the controls to manage those risks. This means that responsibilities and accountabilities for the management of risks are clearly and appropriately established.

The many definitions of corporate governance may be condensed into one concise statement: corporate governance is the way in which an organisation is controlled and governed to achieve objectives. The common factor linking risk management, control and corporate governance is the focus on achieving objectives.

[1] David McNamee and Georges Selim 2000. *Changing the Paradigm.* www.mc2consulting.com/riskart8.htm

© 2008 Plum Concepts & Solutions
ted.dahms@plumcon.com.au
http://www.Plumcon.com.au

Mention has been made above that risk treatments are in effect also controls for achieving objectives. Risk management therefore develops the control environment and the control environment provides reasonable assurance to boards and senior managers that the organisational objectives will be achieved within an acceptable degree of residual risk. Effective risk management is therefore the cornerstone of sound corporate governance.

The complex relationship between risk, control and governance is further revealed by examining the rigid nature of governance implied in its many definitions. These definitions dwell heavily on control and oversight, but there is a paradox in that an organisation also needs to be flexible to respond to changes in its internal and external environments.

Risk management not only provides a mechanism for treating risks that might prevent an organisation from achieving its objectives, but also provides the flexibility for the organisation to respond to unexpected threats and take advantage of opportunities. Risk management therefore provides the resilience.

In short, corporate governance is the glue that holds an organisation together in pursuit of its objectives, and risk management provides the resilience. With this resilience comes competitive advantage.

The next step in this conceptual journey is to regard risk management and corporate governance as one and the same process. The key to understanding this relationship is an examination of what activities are undertaken in corporate governance and the environment in which they occur.

Essentially corporate governance is a guidance system composed of standard management practices operating within a governance framework designed to suit the organisation. The practices are essentially common management tools drawn together into a logical, inter-related system focused on achieving results. They can be universally applied to any organisation irrespective of their size, or statutory and regulatory environments. Once an organisation‘s strategic direction is set, the management practices involve —

- setting an appropriate organisational structure;
- developing linked strategic and operational planning;
- matching competencies to objectives (strategic HR and Board recruitment practices);
- clearly defining roles, responsibilities and accountabilities (Board operating manuals, terms of reference, charters, job descriptions, policies and procedures, inductions, ongoing training/information sessions; electronic document handling systems);
- matching assigned responsibilities and accountabilities with authority (delegations);
- allocating appropriate levels of resources to support assigned responsibilities and accountabilities;
- establishing high standards of ethical behaviour (codes of conduct, leading by example);
- developing an effective monitoring and reporting systems (performance, compliance, changes to inertial and external operating environments); and

- designing a system for effective and timely information flow throughout the organisation.

Management practices that provide governance are at the same time control activities to address risks. Looking at it another way, control activities establish the control environment which provides governance, i.e. the management of risks is also governance.

Governance frameworks provide the structure within which the control activities operate. Parts of this structure are mandatory and set by legislation, regulation or listing rules in different jurisdictions, or by policy directives for public-sector organisations. Others are discretionary and set by Boards and senior management to address the control activities according to the organisation's operating environment. Discretionary frameworks can vary from organisation to organisation even within the same statutory environment e.g. the risk/control environment for a port authority would have a high workplace health and safety component and for this reason the Board may assign oversight of these matters to a committee. In comparison, a legal company's risk/control environment would focus more on the risks associated with providing professional advice and the oversight of workplace health and safety matters could be assigned to a single person in management. For this reason there is no one governance framework that suits all organisations, *i.e*. one size does not fit all.

In the next article I will discuss how the above concepts of control activities and compliance can be leveraged to promote performance and competitive advantage. Because the methodology is founded on refining and aligning standard management practices, its implementation is both uncomplicated and cost effective.

SUMMARY

Governance is essentially a guidance system aimed at achieving objectives *i.e*. it is objectives-focused. Risk management is an essential element and the following statements outline the relationship between risk, control, strategies and governance —

- An organisation is a group of people working together to achieve objectives and is multi-layered.
- Objectives are the results or goals set by the organisation and are also multilayered with alignment of objectives and organisational layers.
- Risk management develops risk treatment plans that are at the same time the controls and strategies associated with each objective. Risk management is therefore part of each objective at all levels of the organisation and is also multilayered by this alignment to objectives.
- By associating the management of risk with objectives at all levels of the organisation it becomes fully integrated as an enterprise-wide system.
- Risk management develops the control environment and provides reasonable assurance that objectives will be reached within an acceptable degree of residual risk. This is governance.

In essence —

- The purpose or focus of the organisation is defined by its corporate objectives and by their translation into operational objectives throughout the organisation. Strategies are developed by applying the AS/NZS 4360:2004 risk management process to the

defined corporate and operational objectives. In short, strategies and controls = objectives + risk management.

- Reporting against performance measures for each objective is also a report on the effectiveness of strategies, controls and the risk management process for that objective. Performance reporting therefore provides a continuous risk management reporting platform.
- Risk management not only provides a strategy for treating risks that might prevent an organisation from achieving its objectives, but also provides the flexibility for the organisation to respond to unexpected threats and take advantage of opportunities. Risk management therefore is dynamic in that it provides organisational resilience as well as control and provides competitive advantage.

Ted Dahms is the Principal Consultant with Plum Concepts & Solutions (http://www.Plumcon.com.au).