

RISK MANAGEMENT AND CORPORATE GOVERNANCE ARE THEY THE SAME?

PART 2 – ISSUES OF RESPONSIBILITY, ACCOUNTABILITY AND ASSURANCE

In the second of a two part series examining how risk management can be leveraged in a cost effective way to underpin sound governance **Ted Dahms** examines the concepts of responsibility, accountability and assurance, and how they interact to promote effective governance.

Recent collapses and partial failures of major listed companies serve to keep the topic of corporate governance in the public spotlight. Accompanying this phenomenon has been a call for greater regulation with the view that by creating a set of new rules greater compliance will result. The more regulatory position adopted by the United States in comparison to Australia and Europe's less onerous approach was discussed in *Tuning in for the Results* by Shaun Drummond in issue 46 of *riskmanagement magazine*.

The danger with increasing statutory and regulatory compliance is increased resistance and a greater internal focus on compliance to the detriment of innovation and performance. There is another way, and this is outlined in Standards Australia's Handbook entitled *Governance, Risk Management and Control Assurance* (HB 254-2005).

The following article outlines the Control Assurance Plan from HB 254-2005, and defines the Plan's Control Elements, Control Criteria and Control Activities. The Plan relies on the concepts of risk and control outlined in the previous article and to recap the main points were —

- Risk is part of each objective both strategic and operational.
- Risk treatments for each objective are also controls and strategies.
- Controls provide governance.
- 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.
- Governance practices are in essence standard management practices, which are in turn Control Activities. 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 system (performance, compliance, changes to internal and external operating environments); and
- designing a system for effective and timely information flow throughout the organisation.

Under the Plan assurance is achieved through a balance of two aspects of control –

- inherent control, based upon soft controls that occur continuously and consistently throughout the organisation, is embedded in normal business practice, and is to a large extent self sustaining; and
- formal control processes of assigning, monitoring, reviewing and reporting (command-control style based upon a hierarchy, e.g. statutory and regulatory compliance systems).

In addition to linking risk management with objectives, the Plan acknowledges that the establishment of a governance framework without an underlying system of inherent controls encourages compliance rather than commitment. Accordingly, it sets out a methodology for establishing an effective, underlying system of inherent controls through the development of capable and committed Directors, chief executive officers, managers and employees who have a clear understanding of organisational, divisional and personal purpose.

Inherent controls are proactive and centred around standard management practices (Control Activities). The Control Activities address the Control Criteria of purpose, capability, commitment, monitoring and learning, and information throughout an organisation and are reliant on sound HR practices, ethics and communication.

The aim of the Control Assurance Plan is to increase the focus on inherent control and reduce the reliance on formal control. In so doing, the Plan provides a framework for moving the organisation towards self-management at the operational level. This leaves the Board free to concentrate on its key tasks of policy formulation, strategic thinking, supervising management and accountability.

The foundation of the plan is five Control Elements, defined by their control responsibilities, linked by an information system (Fig 1). The Control Criteria operate in each Control Element and are addressed through the application of Control Activities according to the control responsibilities of each Element. The Control Elements in a public company and a summary of their control responsibilities are as follows —

- **Planning** (the core control element setting the purpose for the organisation and its divisions in the form of linked corporate plans and operational plans underpinned by sound risk management practices – provides organisational, divisional and personal purpose).
- **Board** (shareholder representatives accountable for organisational performance to key stakeholders – sets organisational direction, develops broad policy and supervises management).

- **Organisation** (CEO, senior managers and employees – responsible and accountable for the delivery of organisational outputs in line with the Board's corporate objectives).
- **Independent Assurance** (includes elements such as internal and external audit, and Board committees e.g. audit, risk and compliance committees - provides risk management and control assurance to the Board independent of management and supports the Board's accountability).
- **Management Assurance** (management's performance/compliance reporting, including the associated risk and control assurance to the Board – supports management's accountability).

The Control Elements are linked by an information system that promotes —

- effective decision-making;
- clarity of roles, responsibilities, authorities and accountabilities; and
- the performance/compliance processes of monitoring, reviewing and reporting.

Responsibility, accountability and assurance are many faceted concepts. Those assigned responsibilities are accountable to those assigning the responsibility for the achievement of an objective, use of resources, ethical conduct and the exercise of authority. Whilst responsibility can be delegated, accountability cannot i.e. a manager can delegate responsibility for achieving an objective and hold the persons delegated accountable, but the manager remains accountable for its achievement to those above.

The relationship between the Control Elements is defined by the concepts of responsibility, accountability and assurance outlined above. Assurance relates to the likelihood that planned objectives will be achieved within an acceptable degree of residual risk i.e. it seeks to ensure that an acceptable level of accountability will be realised by those assigned responsibility, authority and resources for the achievement of an objective. Assurance is sought by the person or body assigning the responsibility, authority and resources.

The quality of the assurance received relies on the effectiveness of the systems and culture put in place by those persons or bodies responsible and accountable for implementing and maintaining the control environment. It follows that the persons or bodies assigning responsibility, authority and resources, as well as seeking assurance, are responsible and accountable for the implementation of systems that provide and enhance that assurance. As these concepts are objectives related they are also multilayered in line with the organisational structure.

To understand the operation of the Plan, consider the position of a manager of an organisational division. The manager is responsible for, and accountable to those above for, addressing the Control Criteria as follows —

Purpose

Ensuring that —

- the objectives at division level (divisional purpose) are translated to the next level down (personal purpose) and clearly linked to divisional and organisational objectives (divisional and organisational purpose); and
- responsibility and accountabilities are clearly assigned through position descriptions aided by organisational and workplace inductions, mentoring, and up-to-date policies

and procedures.

Capability and Commitment

Ensuring that —

- the division is structured to allow the effective assignment of responsibilities and accountabilities;
- skills and experience match responsibilities through effective recruitment and selection processes;
- skills and experience are maintained or enhanced through succession planning and professional development programs;
- policies and procedures are clear, accurate, up-to-date and readily available (intranet);
- appropriate levels of resources are provided;
- authority is delegated to match assigned responsibilities.
- expectations of professional and personal conduct are clearly defined and communicated; and
- reward systems are appropriately developed.

Monitoring and Learning

Ensuring that —

- reporting systems are aligned to objectives and the management of risk;
- any deviation from expected results is addressed in a timely manner and linked with other mechanisms such as post event analysis in the organisation's learning program;
- the performance management system monitors personal performance and professional development needs; and
- an ethical environment is established that promotes open communication (essential for continuous improvement and innovation).

Information

Ensuring that —

- critical information is accurate and flows throughout the division in a timely manner; and
- the information needs of the division and its members are regularly reviewed for quality, quantity and timeliness.

The good news is that the Control Assurance Plan promotes sound governance by refining and aligning current management practices (Control Activities). This means that its implementation can be achieved within existing resources and without additional infrastructure, and is self sustaining.

The Control Assurance Plan is outlined in more detail in Standards Australia's Handbook HB254-2005. This is the first Handbook to link management of risk and corporate governance in a proactive manner. For this reason it is an essential supporting Handbook for the AS 8000-8004 Corporate Governance Standards and a companion for the Risk Management Standard AS/NZS-4360. In addition, its simplicity and common sense approach make it an indispensable reference for organisations seeking to achieve cost effective, better practice corporate governance.

Ted Dahms Principal Consultant, Plum Concepts & Solutions
<http://www.Plumcon.com.au>



Fig 1

Control Assurance Plan

© 2008 Plum concepts & Solutions