THE EVOLVING ROLE OF RISK MANAGEMENT

IN FACILITATING

SOUND CORPORATE GOVERNANCE

Ted Dahms

INTRODUCTION

The conceptual views of risk, control and governance are currently undergoing rapid evolution. Most significantly, risk management and control have expanded from their original, narrower definitions of hazard risk and internal financial control to cover a wider sphere of influence. The result has been a closer relationship between the two and a greater understanding of their role in promoting sound corporate governance.

This paper explores the evolving nature of risk management, control and corporate governance to ultimately arrive at the view that corporate governance is an organisation's strategic response to risk[1]. In addition, the paper outlines a control assurance plan that demonstrates how these new conceptual linkages may be utilised to promote sound governance and introduces the concept of inherent control.

Recent changes to the conceptual view of control from internal financial control to a broader concept covering all activities has seen a change in the focus of internal audit methodology from transaction-based financial compliance to one of processes and controls. Similarly, the linking of risk management with objectives is heralding a boarder, more influential role for risk managers in relation to their organisation's planning and governance practices.

This paper is based upon conceptual views developed whilst working in governance and risk management since 1998 and incorporated into Standards Australia's HB 254, 2005 entitled *Governance, Risk Management and Control Assurance*. Readers are strongly urged to obtain a copy of this Handbook for a fuller explanation of its uncomplicated methodology. The great value of this methodology is that is offers a way to sound governance using existing resources and structures by refining and aligning current practices. The paper contains some short extracts from HB 254, 2005 interwoven with material from my other writings as well as incorporating contributions from my evolving view of governance and risk management.

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

ted.dahms@plumcon.com.au
www.Plumcon.com.au

CONTROL AND RISK

The concepts of internal control and risk management had very different origins, but they have now become inseparable. To understand the relationships between these two concepts it is necessary to examine their origins and the subsequent shifts in perceptions.

CONTROL

Internal control had its origin with the accounting profession and understandably its focus was financial controls and legal compliance. Risk management arose in gambling and was subsequently adopted up by the engineering and insurance industries as an essential methodology with a focus on hazard risk.

The definition of control has been expanded recently to cover the efficiency and effectiveness of all of an organisation's operations as well as the associated processes and risks that impact on the achievement of its objectives. In this view internal control is a process effected by an organisation's Board of Directors, Chief Executive Officer, senior management and other members of the organisation, designed to provide reasonable assurance regarding the achievement of the organisation's objectives[2].

Control is now seen to comprise those elements of an organisation (including resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives[3].

Previously control only involved bureaucratic processes such as second party authorisation and segregation of duties. This is typical of a command/control environment with second party authorisation and segregation of duties (formal control).

Modern control frameworks and models now recognise the essential contribution of what are referred to as 'soft controls' that include leadership, teamwork, culture, values, communication, accountability, anticipation, flexibility and capability[4]. These controls are crucial for developing capability and commitment throughout the organisation and are the foundation of the inherent control environment. Sound governance requires the striking of an appropriate balance between inherent and formal control. These two aspects of control are explained in more detail under Control Assurance Plan later in this paper.

---

[2] New South Wales Treasury, 1997. *Risk Management and Internal Control. A Step by Step Approach to Managing Risks More Effectively.* New South Wales Treasury, September 1997: 4 volumes.

[3] Canadian Institute of Chartered Accountants, 1995. Control and Governance No. 1. Guidance on Control*. Canadian Institute of Chartered Accountants, Ontario, Canada, November 1995: 32pp.*

[4] *Leithhead, B S, 1998. Control Self Assessment's Contribution to Corporate Governance. In Delivering Good Governance. Institute of Internal Auditors Conference, Gold Coast, Queensland, 1998: 14pp*.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

RISK MANAGEMENT

Risk is now defined as 'the chance of something happening that will have an impact upon objectives'[5].

Risk, control and governance have a complex relationship that is 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 the organisation also needs to be flexible to respond to changes in its internal and external environments.

Risk management not only provides a strategy for treating risks which might impede an organisation in pursuit of 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 with risk management providing the resilience for an organisation to respond to unexpected threats and opportunities.

SUMMARY

From these modern definitions of control and risk management it is clear that the coverage of both concepts has expanded to include all of an organisation's activities. The relationship between risk and control can be revealed by examining the risk management processes of identification, analysis, evaluation, monitoring and control. Cost effective internal controls are the treatment plans put in place to manage risks. Risk management is therefore the tool that assists in the development of the control environment and plays a key part in corporate governance.

The key issues that arise from the definitions of control and risk are that —

- the risk management process develops the control environment;
- control involves all aspects of an organisation's operations – its focus is no longer restricted to financial matters;
- the word "internal" has been dropped in front of control in recognition of external as well as internal environmental change;
- the focus of risk management, control and governance are one and the same - the achievement of organisational objectives and the exploitation of opportunities;
- although the responsibility for the organisation's control environment rests with the Board there is a delegated responsibility to everyone in relation to their assigned responsibilities, i.e. everyone who has responsibility for an objective has responsibility for the risks associated with that objective and the controls to manage those risks; and

[5] Australian/New Zealand Standard 4360 on Risk Management. Standards Australia, Sydney, 2005.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

RISK, CONTROL AND GOVERNANCE

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.

CONTROL ASSURANCE PLAN (HB254, 2005)

In addition to linking risk management with objectives, the Control Assurance Plan outlined in this paper acknowledges that the establishment of a governance framework without an underlying system of soft controls encourages compliance rather than commitment. Accordingly, it sets out a methodology for establishing an effective, underlying system of soft controls through the development of capable and committed Directors, chief executive officers, managers and employees.

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

The advantages provided by the Plan for those monitoring accountability are realised by separating control into formal and inherent control.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

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 monitoring, reviewing and reporting (command-control style based upon a hierarchy).

Inherent controls are proactive and centred around standard management practices. They promote purpose, capability and commitment throughout an organisation and are reliant on sound HR practices, ethics and communication. Elements that contribute to an effective inherent control system include systems thinking, developing a learning organisation, motivating trust and relationships, and matching competencies with objectives.

SYSTEMS THINKING

Organisations are complex systems. The traditional method of dealing with complexity is to break it down into component parts and examine each part in isolation. This process is followed in designing an organisational structure and assigning roles and responsibilities throughout the structure. The very act of assigning roles and responsibilities predisposes the organisation to fragmentary or silo behaviour where individual parts concentrate on their assigned tasks and function independently rather than as an integrated whole focussed on organisational goals. Where fragmentary behaviour develops, a compliance mentality follows and the worthy concepts of continuous improvement and innovation fall by the wayside. Performance is diminished and opportunities are lost.

Systems thinking takes a holistic view of an organisation based upon the observation that autonomy is never absolute and that we are all interdependent on each other. Decisions are never taken in isolation. An analogy would be an organisation as a still pool of water and the impact of one decision a rock thrown into the pool. The influence of that action can be seen in the ripples which radiate out from the impact to reach all parts of the pool. Now imagine a handful of stones thrown into the pool and you can appreciate the complexity of the interactions that occur – each action contributes to patterns of interrelated actions.

Additionally, organisations do not operate as closed, isolated systems, but in a world that is both dynamic and complex. The internal and external environments are constantly changing thus creating situations that lead to competition and collaboration both of which present threats and opportunities which must be managed. Organisations are therefore continuously under pressure to adapt to change and co-evolve with others in a complex, dynamic environment. Failure to do so threatens the organisation's viability. In short, adapt or fail.

In applying this concept to organisations, the leadership skill for Boards and senior managers is in promoting an understanding that all divisions of the organisation are part of an interconnected whole with the corporate objectives as the unifying force.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

LEARNING ORGANISATION

Peter Senge[6] in his book entitled The Fifth Discipline defines a learning organisation as —

> "*an organisation that is continually expanding its capacity to create its future. For such an organisation, it is not enough to merely survive. 'Survival learning' or what is more often termed 'adaptive learning' is important – indeed is necessary. But for a learning organisation, 'adaptive learning' must be joined by 'generative learning,' learning that enhances our ability to create*."

Here Senge means generative learning as the way of expanding an organisation's capacity to create rather than change by events of the moment (adaptive learning). The former is creative the latter reactive.

Learning organisations have cultures which predispose them to innovation and the early recognition of opportunities. The factors that facilitate the change from a controlling to a learning organisation include the development of a shared vision which in turn relies upon open communication in a climate of commitment and trust. New ideas are able to be shared allowing alignment of ideas to give a common direction and this facilitates team learning. In this environment risk taking is encouraged, learning is shared and the focus of all members is on organisational performance not conformance.

TRUST & RELATIONSHIPS

Where interdependent agents, internally and externally, wish to co-ordinate their behaviours they must invest in creating, building and maintaining trustful relationships. Without trust both parties descend into non-communicative and defensive behaviour. Innovation and synergy do not flourish and the opportunity is lost for two to achieve more than they could by operating separately.

The more effort invested on building trust and relationships within in an organisation the less will be the need to retain command/control structures founded on compliance.

Where members of an organisation, or co-operating organisations, are willing to accept accountability and perceive that they are operating in an environment of trust and synergy the reliance on conformance is reduced a greater focus on performance results. Complementing the aspect of trust is the development and maintaining a match of competencies with assigned responsibilities.

COMPETENCIES

An organisation must align the competencies of its employees with its objectives if it is to be successful. This alignment is facilitated by sound HR practices involving job design with matched position descriptions, recruitment and selection, professional development, performance planning, staff retention and succession planning.

Because of rapid external environmental changes currently occurring, these practices must be continually reviewed to ensure the organisation maintains its core competencies and builds new competencies to take advantage of opportunities. Senior managers must view the organisation as a portfolio of competencies, of underlying strengths and not just a portfolio of business units. In short strategic and operational HR planning are fundamental tools for success and should not be neglected.

---

1. [6] Senge, P M, 1992. The Fifth Discipline, the Art & Practice of the Learning Organisation. *Random House, Australia, 1992: 424pp*.

CONTROL ELEMENTS AND CONTROL CRITERIA

The Control Assurance Plan (definitions APPENDIX B) is based upon the following five assurance Control Elements (Figure 1) linked by an information system, each with their own control assurance focus as follows —

- **Planning** (the core Control Element setting the purpose for the organisation in the form of strategic and linked operational plans);
- **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 for the delivery of organisation outputs in line with the Board's strategic objectives);
- **Independent Assurance** (provides risk management and control assurance to the Board independent of management – supports the Board's accountability);
- **Management Assurance** (management's performance reporting, including the associated risk and control assurance to the Board – supports management's accountability).

The Plan operates by developing the control criteria of purpose, capability, commitment, monitoring and learning, and information in each Control Element according to the control assurance focus in each. The various aspects of the control criteria are developed by applying the standard management practices as Control Activities as follows —

- competencies matching objectives (strategic HR practices);
- clarity of roles and responsibilities (terms of reference, job descriptions, policies and procedures, inductions, ongoing training/information sessions);
- matching assigned responsibilities with authority (delegations);
- high standards of ethical behaviour (codes of conduct);
- effective monitoring and reporting systems; and
- effective and timely information flow throughout the organisation.

EXAMPLE OF APPLICATION

The assurance focus the Board Control Element is as follows —

- the on-going capability and commitment of Board members in relation to the discharge the Board's responsibility (Board member selection, induction, on-going professional development, Board Operating Handbook, Code of Conduct and Board performance review);
- the strategic direction of the oganisation is appropriate (integrated strategic and operational planning);
- the implementation and maintenance of a control environment that supports this strategic direction (integrated risk management system linked to objectives);
- the oganisation operates within its legal and regulatory obligations (compliance);
- the oganisation can continue to function in the face to major disruptions (disaster recovery and business continuity planning);

ted.dahms@plumcon.com.au
www.Plumcon.com.au

- the implementation of an information system that supports effective decision-making, open communication, monitoring and reporting;
- an effective linkage is developed between the Board and the organisation through the CEO; and
- development of a capable and committed workforce that has a clear understanding of the organisation's purpose.

The Control Criteria for the Board may be addressed by the following Control Activities —

- Development of a Board operating manual setting out its responsibilities, authority, operating procedures, and relationships to the CEO and management.
- A Board code of conduct setting out expected ethical behaviour and leading by example.
- An appropriate recruitment and selection policy and procedures for directors that includes provisions for succession planning.
- Induction procedures for new directors outlining the—
  - nature of the organisation's business and operating environment; and
  - Board responsibilities and accountabilities.
- On-going professional development to maintain and develop new competencies amongst directors.
- Meetings and well maintained meeting papers that—
  - are clearly laid out and circulated in advance of a meeting to allow directors time to examine the issues;
  - provide an indication of the outcome against each agenda item;
  - have an executive summary accompanying detailed reports and submissions and where necessary executive briefings at the meeting; and
  - contain all the necessary reports and information for directors to make informed decisions.
- Regular review of information provided to the Board to ensure its continuing support of Board decision-making.
- Regular self-evaluation of the Board, individual director performance and operating charter.
- Recruitment and selection of a capable and committed CEO, regular CEO performance reviews and CEO succession planning.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

SUMMARY

Effective risk management and the resulting control environment are central to sound corporate governance and organisational resilience. The linking of risk management to objectives means that controls are also strategies. It follows that the reporting of performance in relation to each objective is also a report on the effectiveness of controls and strategies for that objective. Risk management therefore forms part of normal business practice rather than being a separate, unrelated task and is integrated throughout the organisation along with the associated, integrated objectives. Recent changes to the conceptual view of control from internal financial control to a broader concept covering all activities has seen a change in the focus of internal audit methodology from transaction-based financial compliance to one of processes and controls. Similarly, the linking of risk management with objectives is heralding a boarder, more influential role for risk managers in relation to their organisation's planning and governance practices.

Dr TED DAHMS
Principal Consultant
Plum Concepts & Solutions
07 3273 2396
0408 756 272
ted.dahms@plumcon.com.au
http://www.Plumcon.com.au

APPENDIX A

Figure 1

Components of Control assurance

ted.dahms@plumcon.com.au
www.Plumcon.com.au

APPENDIX B

DEFINITIONS (FROM HB254-2005)

Assurance

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 and authority for the achievement of an objective. Assurance is sought by the person or body assigning the responsibility and authority.

The level of assurance is reliant on the effectiveness of the systems and culture put in place by those persons or bodies responsible for implementing and maintaining the control environment. It follows that the persons or bodies assigning responsibility and authority, as well as seeking assurance, are responsible for the implementation of systems that provide and enhance that assurance.

Assurance Focus

Control assurance responsibility assigned by legislation, regulation, listing rules or by an organisation's governance system. It may apply to individuals or parts of the organisation including the Board.

Control*

Control comprises those elements of an organisation (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives.

Once the strategic direction of the organisation is determined everything that follows is part of the control environment.

Control Activities*

Routines established to provide assurance that processes operate as designed and meet the requirements of the organisation's policies. (Management practices or principles)

Control Criteria*

Criteria that are the basis for understanding control in an organisation and for making judgements about the effectiveness of control.

Control Elements*

Any part of an organisation, or the relationship between parts of an organisation, that contributes to reliable achievement of its objectives.

ted.dahms@plumcon.com.au
www.Plumcon.com.au

Organisational Objectives	The long–term results, with appropriate key performance indicators, set by the organisation.
Formal Control	Control processes of assigning, monitoring, reviewing and reporting (command-control style based upon a hierarchy).
Inherent Control	Control activities that promote purpose, capability, commitment, monitoring and learning, and information throughout the organisation, including the Board, and are reliant on sound HR, ethics and communication. They occur continuously and consistently throughout the organisation, are embedded as normal management practices, and are to a large extent self sustaining.
Organisation*	A group of people working together to achieve objectives. This includes the entity and its governing body.
Risk Management	The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse events.

* After *Control and Governance, Number 1 - Guidance on Control*. Canadian Institute of Chartered Accountants, 1995.

ted.dahms@plumcon.com.au
www.Plumcon.com.au