THE ROAD TO RESILIENCE IS PAVED WITH SOUND RISK MANAGEMENT

New Paradigms for Risk Professionals

Dr Ted Dahms
Plum Concepts & Solutions

INTRODUCTION

Much public analysis and finger pointing has occurred in an attempt to identify the triggers for the recent 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. Those relevant to this paper include failures in legislation, regulation and governance practices. Running through all of these issues 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. The shortcomings of COSO ERM 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[1].

All of the above indicate that risk management as a concept is profoundly misunderstood and misapplied rather than any failure of the concept itself. The current push by some for resilience to replace risk management is another example of this misunderstanding and relies on an imprecise definition of resilience.

This paper takes the view that any organisation with effective risk management practices will also have sound governance and be resilient.

In the following discussion where the word board is used it is meant as the governing body, which can be any private sector company board, a university council, a local government council, a statutory body board, a single person in charge of a public sector department and so on.

[1] Michael Rasmussen, Jan. 2007. *AS/NZS 4360 – A Practical Choice over COSO ERM*. Best Practices www.forester.com.

PARADIGMS

The paper sets out 11 paradigms. In the first, complex adaptive theory is borrowed from evolutionary biology to present a new conceptual view and definition of resilience that sees it as a state of being rather than a process. The paradigms that follow illustrate how risk management may be integrated and leveraged to achieve resilience. The clear message from the paradigms is that compliance with a set of rules will not deliver sound governance and resilience, and that everything is interconnected in a constantly changing environment.

RESILIENCE

Resilience expresses the capability of an organisation or its parts to respond quickly to uncertainty. The following paradigm examines the complex nature of uncertainty, and the reasons driving this complexity, to form a new definition of resilience.

Paradigm 1: Resilience is a destination not a journey.

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 a state of being arising from activities to address 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*[2].

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.*

The meaning of this definition is that resilience is the outcome of the risk management process, i.e. managing uncertainty.

Complex adaptive system theory (evolutionary theory) was developed in biology, but has application to organisations. It is currently being applied to economic theory and is the subject of book by Eric Beinhocker[3] in which he says on page 187,

> *... evolution is a general-purpose and highly powerful recipe for finding innovative solutions to complex problems. It is a learning algorithm that adapts to changing environments and accumulates knowledge over time.*

[2] Organisational Resilience Standard. ASIS SPC.1 – 2009.
[3] Eric D Beinhocker, 2006. The Origin of Wealth. Evolution, Complexity, and the Radical Remaking of Economics. Harvard Business School Press 2006.

In contrast, traditional views of corporate governance and risk management mirror the earlier scientific view of the world as a linear space where the simple rules of cause and effect apply. In this space the universe and its parts (systems) were viewed as machines and it was thought that by understanding their component parts they would understand the whole. Additionally, by improving the performance of the parts they could improve the performance of the whole. This approach failed to achieve results and it became apparent that the systems were behaving according to a different set of rules. This set of rules is defined by complexity theory, which is

> *...based upon relationships, emergence, patterns and iterations. A theory that maintains the universe is full of systems, weather systems, immune systems, social systems etc and that these systems are complex and constantly adapting to their environment. Hence complex adaptive systems[4].*

A fuller discussion of the elements of complex adaptive theory is beyond the scope of this paper, but a concise account is given by Fryer (2009). Broadly speaking, organisations and parts thereof do not exist in isolation, but are part of an interconnected set of systems which are informed by feedback mechanisms. Such systems are aware or alert and learn by accumulating knowledge over time.

It follows that any conceptual view of governance, risk management and resilience that relies on linear theory is seriously unreliable. Compounding this is the application of tick and flick compliance programs to the linear theory. Certainly any system that restricts its view of control to internal financial control would be so woefully inadequate in addressing uncertainty as to be negligent (Paradigm 7).

In the second instance the process of corporate governance is risk management (Paradigm 8) and therefore resilience is the outcome of governance, not the reverse.

Resilience is reliant upon 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. The following paradigms address these matters and their underlying concepts.

Paradigm 2: strategic plans and competitive advantage are transitory.

The intent of strategic plans is to present a blue print for an organisation's direction and competitive advantage over a five year period. However, the dynamic complexity of the environment renders them transitory and in constant need of renewal.

A new approach is required. Rather than trying to predict the future it is more effective to build a set of competing business plans within the organisation to reflect the competition occurring outside in the market place. By creating options and keeping the tree of possibilities as bushy as possible an organisation can evolve into the future[5].

In concert with this new planning process is the development of what Beinhocker calls "prepared minds". This sees planning as a learning exercise preparing people for the future rather developing an answer in the form of a single, focused five year plan based upon predictions of the future. Its process involves robust analysis and debate around facts and environmental issues rather than opinions. The outcome from these new approaches to planning is awareness.

[4] Peter Fryer, 2009. A brief Description of Complex Adaptive Systems and Adaptive Theory. www.trojanmice.com/articles/complexadaptivesystems.htm

[5] Eric D Beinhocker, 2006. The Origin of Wealth. Evolution, Complexity, and the Radical Remaking of Economics. Harvard Business School Press 2006.

This is a leadership issue that provides resilience, variously referred to as adaptability or agility in resilience literature, at the head of the organisation. The creation of alternatives and developing "prepared minds" cascades throughout the organisation in the planning process creating an aware and resilient organisation.

INTEGRATION OF RISK MANAGEMENT

Many recent initiatives have been aimed at making risk management a more integrated process. The iterations are variously labelled Enterprise Risk Management (ERM) and Enterprise Wide Risk Management. Each has failed to reach the aim of full integration mostly because risk management remains a discrete exercise without clear integration as part of normal business practice. Managers therefore see it as additional financial and operational imposts, which are not balanced by practical benefits.

The key to breaking this resistance is a set of paradigms that illustrate not only the intuitive nature of risk management, but also that effective risk management delivers cost effective performance, resilience and competitive advantage using existing business systems.

Paradigm 3: Risk is part of each objective.

The aim of risk management is not the management of risk per se but the achievement of objectives, i.e. risk is part of each objective at all levels of the organisation. The linkage between risk and objectives is reflected in the definition of risk as – the effect of uncertainty on objectives (AS/NZS ISO 31000: 2009). This is the foundation paradigm from which all the others flow.

Paradigm 4: Uncertainty is an all encompassing concept.

The current risk management landscape is fragmented by several standards and professional specialist areas such as Compliance, Business Continuity/Disaster Management, Security, Safety, and Resilience.

By embracing the simple concept in Paradigm 3, risks and their treatments (which are also controls and strategies) cascade throughout the organisation with objectives and with the appropriate language for each level. This develops an integrated system and supports the view that none of the parts operate in isolation (complex adaptive systems theory). This also means that areas of uncertainty such as Compliance, Business Continuity/Disaster Management, Security and Safety cascade throughout the organisation along with other risk areas such as finance, IT, HR etc and their focus is on achieving objectives.

The logical inference therefore is that there need only be one standard and that is AS/NZS ISO 31000:2009 which covers uncertainty. Specialist areas such as Compliance, Security, Safety etc would be best accommodated as supporting handbooks. This does not infer any reduced importance to these issues, but connects them under the uncertainty umbrella and with each other, while continuing to recognise the distinctive nature of their risks and strategies.

Paradigm 5: The management of risk is an intuitive process.

Managing risk is an uncomplicated process used in everyday life to achieve objectives. Examples include getting to work on time and safely, meeting appointments and deadlines, driving, crossing the road and so on. The processes of setting the objective, identifying and assessing the level of risk and developing strategies (risk treatments) to achieve the objective are intuitive and occur unconsciously as part of normal activities. The focus is on the objectives and the strategies to achieve them, not the risks.

In contrast, organisations using the current ERM process develop a separate, resource-hungry risk management framework focused on the risks with tenuous linkages if any to objectives and strategies. This ERM process therefore unnecessarily duplicates the intuitive risk management activities in the standard business practices of planning and performance monitoring and works against resilience (Paradigm 6).

Paradigm 6: Risk management, planning and performance review are concomitant processes.

By applying the risk management process to objectives, risk treatments are at the same time controls and strategies. Consider that the objective is to cross the road and the risk is identified as being hit by a moving vehicle.

Assessment of the risk is a combination of likelihood of the event occurring and the consequence should the event occur. The consequences of being hit by a moving vehicle are evaluated as high; the level of likelihood varies depending upon the density of the traffic as follows —

- If the traffic is light, the likelihood is assessed as low and the residual risk is rated as low. The action is to look right, left and right again and then proceed to cross the road when a safe gap in the traffic appears.
- If the traffic is heavy, the likelihood is assessed as high and the residual risk is rated as high. The action is to proceed down the footpath to a traffic light and push the “WALK” button. The traffic is stopped at a red light reducing the residual risk to an acceptable level allowing the road to be crossed safely.

The act of looking right, left and right again or the pushing of a “WALK” button are risk treatment plans that reduce residual risk to an acceptable level allowing the objective to be achieved. The treatment plan is changed depending on the level of residual risk. The risk treatments are at the same time controls designed to ensure the objective will be achieved and also strategies for achieving the objective, i.e. risk treatment plans are controls and also strategies.

A number of significant outcomes arise from the above paradigms.

- 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).

Paradigm 7: Control is a broad concept.

The restrictive concept of internal financial control outlined in COSO and the ASX Corporate governance Council’s Supplementary Guidance to Principle 7 (Risk Management) ceased to be the overarching view of control more than a decade ago. This restricted view of control ignores significant non-financial and external risks and appreciably reduces resilience.

A more inclusive concept of control covers all activities after the strategic direction has been set and it includes external as well as internal factors. Control is defined as follows —

> *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*[6].

This broader concept acknowledges that organisations operate in complex dynamic systems (Paradigm 1).

RISK AND GOVERNANCE

Corporate governance is all about control assurance, which in turn is reliant on the effective management of uncertainty. The following paradigms develop the theme that risk management is the process of corporate governance, and examines how this relationship can be leveraged to promote resilience.

Paradigm 8: Corporate governance is an organisation's strategic response to uncertainty.

Dahms (2008)[7] clarified this concept by arguing that corporate governance is in essence risk management on the premise that corporate governance is essentially a set of common management practices that address higher level risks. These management practices include: strategic and operational planning; designing the corporate structure and populating this with capable and committed people; matching responsibility with authority and resources; setting the ethical standards; implementing a quality information system; monitoring performance, compliance and the operating environment; and finally reporting to provide accountability and assurance.

The management practices are in essence high level control activities addressing high level risks and can be universally applied to any organisation. Addressing control activities to develop capable and committed Directors, senior officers and employees who have a clear understanding of organisational and personal purpose establishes inherent controls. Because inherent controls are developed by refining and aligning existing management practices, their implementation is both uncomplicated and cost effective. For the same reason inherent controls are proactive, self sustaining, and promote awareness and resilience.

Paradigm 9: Corporate governance is more art than science.

The control activities in Paradigm 8 operate within a governance framework. Parts of this framework 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 size, purpose and operating environment.

Discretionary frameworks 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. Implementing a sound governance system by

[6] *Control and Governance, - Number 1. Guidance on Control.* The Canadian Institute of Chartered Accountants November 1995.
[7] Ted Dahms, 2008. Risk Management and Corporate Governance are They the Same? www.plumcon.com.au/Publications/Publications.html

governing bodies requires an understanding of the organisation's size, purpose and operating environment. Compliance against a universal set of rules reduces resilience.

Broadly speaking, the science of corporate governance is in implementation of the mandatory framework. The design of the discretionary elements of the framework and the creation of an inherent control system are the leadership elements of effective governance, and constitute the art. Both are rooted in common sense and common decency.

Paradigm 10: Effective governance is all about control assurance.

This paradigm examines the essence of corporate governance. A concise statement of corporate governance defines it as —

> *The manner in which an organisation is directed and controlled to achieve its objectives*[8]*.*

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 (Paradigm 8). It supports the view that the process of governance is risk management, i.e. it is the "manner" in the above definition.

Control assurance is aligned to control responsibilities and organisations may be broadly divided into a number of elements on the basis of control responsibilities[9]. The control elements are —

Planning: The core control element setting the purpose for the Board, 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.

The aim of the Control Assurance is to increase the focus on inherent control and reduce the reliance on formal control (compliance). In so doing, it provides a framework for moving the organisation towards self-management at the operational level and enhanced resilience.

It follows that responsibility for the implementation of assurance systems is also part of the framework for achieving resilience.

[8] *Corporate Governance, Beyond Compliance*. Audit Report N0. 7 1998-99. Queensland Audit Office, June 1999.
[9] Governance, Risk Management and Control. Standards Australia HB 254:2005.

Paradigm 11: Control Assurance System design is the responsibility of those assigning responsibilities, authority and resources for achieving objectives.

The quality of control assurance received relies on the effectiveness of the systems and culture put in place by those responsible and accountable for implementing and maintaining the control environment. This means that those 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. A critical part of this assurance system is the quality, quantity and timeliness of information, which supports awareness.

Control assurance for Boards is achieved though the elements of Management Assurance and Independent Control assurance and the quality and timeliness of information provided by these elements.

The complex adaptive nature of an organisation's operating environment require that Boards set the parameters for management reporting and delegate the responsibility to CEO's, but remain accountable for the timeliness and quality of the reports. There are a number of processes that Boards can implement to deliver management control assurance —

- Regular review of information provided to the Board in terms of timeliness, quality and quantity to ensure that it continues to meet the Board's decision-making responsibilities.
- Recruitment of a CEO with the appropriate skills.
- Development of an appropriate CEO performance contract and performance appraisal process.

Balancing and enhancing the above inherent control processes are the independent control assurance processes of internal audit, external audit and the Audit Committee. Through internal audit's activities the Board can have confidence in the accuracy of management reports and the company's systems for identifying and managing risk. Internal audit's assurance responsibility is discharged to the Board through the audit committee.

The responsibility for control assurance implementation cascades down through the organisation along with assurance responsibilities for the achievement of objectives. The control assurance program creates awareness throughout the organisation improving its responsiveness to the dynamic nature of its operating environment.

SUMMARY

Uncertainty, and its relationship to the achievement of objectives, is the concept linking risk management, corporate governance and resilience. In essence, an organisation that effectively manages uncertainty will also have sound governance and be resilient.

Risk management as outlined in AS/NZS ISO 31000:2009 is the process for managing uncertainty and achieving objectives.

Corporate governance is all about control assurance, which in turn is reliant on the effective management of uncertainty. Risk management therefore is the process of corporate governance.

Uncertainty is a complex concept due to the complex adaptive nature of the organisation's operating environment. Broadly speaking, organisations and parts thereof do not exist in isolation, but are part of an interconnected set of systems which are informed by feedback mechanisms. Such systems are aware or alert and achieve learning by accumulating knowledge over time. Facilitating this awareness is the effective integration of risk management, adoption of a broad view of control, and understanding control assurance processes.

Resilience is the ability of an organisation to anticipate and respond to uncertainty in a complex adaptive environment, i.e. its adaptive capacity. It is a state of being or outcome and the underlying process is risk management.

The development of a resilient organisation therefore requires that —

- The conventional linear, compliance method of addressing the management of uncertainty and corporate governance be abandoned in favour of complex adaptive theory, which more accurately reflects the nature of an organisation's operating environment.
- A simple change in the focus of risk management from the management of risk to the achievement of objectives be adopted. This change not only terminates the silo treatment of risk management within the organisation, but also the silo stratification of risks into strategic and operational. Carrying this one step further it brings Compliance, Safety, Security and Business Continuity/Disaster Management under the uncertainty umbrella. Removal of all the silos mentioned above develops connections, promotes synergy and enhances resilience.

The attractive part of applying the above paradigms is that governance and therefore resilience can be enhanced by the refinement and re-alignment of standard management practices. In short, the road to resilience is paved with sound risk management.

TED DAHMS
Principal Consultant
Plum Concepts & Solutions
Ted.dahms@plumcon.com.au