

Integrating Risk Management with existing methods of Strategic Control: Avoiding duplication within the Corporate Governance agenda

2GC Conference Paper

An original paper by G.J.G Lawrie, D.C. Kalff and H.V. Andersen presented at 6th International Conference on Corporate Governance and Board Leadership held at Henley Management College, UK, in August 2003.

© 2GC Limited, 2009. All rights reserved.

This document is licensed under a Creative Commons License. You are free to copy, distribute, display, and perform the work subject to the following conditions:

- o **Attribution.** You must give the original author credit.
- o **Non-commercial.** You may not use this work for commercial purposes.
- o **No Derivative Works.** You may not alter, transform, or build upon this work.

For any reuse or distribution, you must make clear to others the license terms of this work. Any of these conditions can be waived if you get permission from the copyright holder.

More information on this license from <http://creativecommons.org/licenses/by-nc-nd/2.0/uk/>

© 2GC Limited • Registered in England Number 3754183 • Registered Office: 16 Wentworth Road, Oxford OX2 7TD

2GC Limited
Albany House
Market Street
Maidenhead
Berkshire
SL6 8BE UK

+44 (0) 1628 421506
www.2gc.co.uk
info@2gc.co.uk

2GC Conference Paper

Abstract

This paper considers the overlap between recent discussions relating to Risk Management and the wider literature relating to Corporate Governance, particularly as it applies to issues of strategic control. The paper observes that corporate performance management methodologies are now in widespread use by both private and public sector organisations, and that these form a key part of the tools used by Management Boards to affect strategic control. It also observes that recent interest in risk management has led to the creation of risk management tools / methods that typically have been developed in parallel to existing performance management systems. The paper notes that performance management systems intended for use at Board level already have much in common, both in design and usage, with proposals for best practice Risk Management processes suggesting that the use of two distinct systems is not optimal. Drawing on existing performance and risk management literature, and on the case based experiences of public sector organisations in Australia and Europe we propose an alternative to the development of parallel control systems. The proposed integrates distinct design processes for each of the two systems, and supports their subsequent integration for ongoing usage. We suggest that this approach will deliver significant efficiency benefits to senior managers, while retaining the effectiveness of separate systems.

Introduction

The widely-held perception in the Anglo-Saxon economies that today's business environment is more volatile, faster-evolving and therefore less predictable than in the past has had profound impacts on both the regulatory landscape and the management agenda. Regulators have been increasingly active in passing new legislation intended to improve corporate governance in its broadest definition, but with particular focus on the management of risk. In the financial services industry this situation is even more noticeable with legislative compliance being a core process for Boards in this sector and a particular form of risk management, which is not the subject of this paper.

A division exists between risks that are both unmitigatable and exogenous (e.g. unpredictable catastrophes) and those that relate to the poor execution of managerial control within an organisation (e.g. failure to maintain safe working practices in a factory). This latter group of risks are largely (but not exclusively) endogenous. A key element of our proposition is that the management of endogenous risks (e.g. systems failure, loss of key executives, etc.) is by necessity an integral part of corporate performance management, whereas managing exogenous or external risks (e.g. impact of legislative changes, abnormal weather patterns, etc.) is principally a matter of ensuring that contingency planning is carried out on a periodic or campaign basis to anticipate and mitigate the most catastrophic possible scenarios. This paper addresses primarily the former element of this division.

This paper proposes that the implementation of any new approach to risk management needs to be regarded and treated as an amendment to existing approaches to corporate performance management and that those working on these approaches in distinct separate "silos" should be brought together. The proposition requires that a robust approach to corporate performance management already exists and is being used effectively. Where this is not the case, it is recommended that implementing a new or improved approach to corporate performance management needs to precede any other investment in risk management systems. This proposition, we will argue, is necessitated by the close affinity between risk management and

corporate performance management or strategic control (Hoffman, 2002). As strategic choices define an organisation's exposure to risk as well the degree of acceptable risk, an inherent part of this process must be the prioritisation of risk mitigating activities in the context of strategic choices in general.

Existing thinking on concepts of Corporate Governance, Strategic Control & Risk Management

Risk, and the need to manage it, is nothing new. Hoffman observes that Maslow implicitly recognised risk in his famous hierarchy of needs by placing food and shelter, both essential to survival, on the first rung of the ladder (Hoffman, 2002). A failure to manage the risk of these needs not being met can have catastrophic results, as much for organisations today as it was for the earliest life forms. Bernstein cites the impacts of wars on markets, and storms and piracy on shipping routes as some of the major risks faced and managed by our predecessors (Bernstein, 1996a). He also notes that only 350 years separate today's risk management techniques from decisions made on the basis of superstition and instinct (Bernstein, 1996b).

Living in a riskier world?

If risk is nothing new to organisations, why is risk management generating rising levels of interest at present? The subject is certainly topical: a search of the ABI/Inform database under 'risk management' generates more than twice as many articles for the first quarter of 2003 as for the equivalent period in 2001, as represented in Figure 1 below.



Figure 1 – Risk management in the literature

Most of the current literature on the topic suggests that this interest is justified. For example, Stevenson et al propose that heightened levels of competition and a rapid pace of change are destroying predictability for organisations, implicitly raising the levels of risk faced (Stevenson, 1995), while Lewis claims that modified competitive, technological, social and political circumstances have magnified the potential impact of operations-related failures (Lewis, 2003). Delamontagne and Witzel echo this in stating that events such as the September 11th terrorist incident in New York and the Enron meltdown have moved risk management higher on the business agenda (Delamontagne, 2003, Witzel, 2002). Hoffman maintains that watershed changes in society, technology, science, and the interconnected nature of global society and business make the subject more relevant than ever before. He supports this position with reference to a database of operational loss events suggesting that the majority of reported commercial losses have occurred since the beginning of the 1990s. Whether this rise in historical trend levels might instead be due simply to improved record-

keeping and transparency is unfortunately not explored.

Mintzberg argues against the 'watershed' view proposed by Hoffman and others. He posits that the rate of change today, the major driver of the claimed rise in risk levels, is little different from historical rates of change. In his view it is perception that matters here, and that the perception amongst organisational leaders has always been that the 'current' interconnected pace of change and levels of risk are higher than ever (Mintzberg, 1994). But what has changed is the recent adoption of approaches that seek explicitly to identify and manage these changing demands. Hence the comment "Even the primary focus of risk management activities has shifted. Any possible source of uncertainty is now treated as a risk that might need managing. This "holistic" approach addresses all potential risk exposures to a company, from legal, political, and regulatory issues, to shareholder relations, the effects of competition, and management competence. It encompasses health and safety, product development, staff fraud, and company reputation, as well as the purely financial aspects of running a business." (Anonymous, 1998).

Risk Management by another name

Seeking to understand the likelihood and impact of future events, be they favourable or unfavourable, in order to maximise future business performance, is a decades old activity: by the late 1960s, Royal Dutch Shell had begun to develop scenarios that were designed to help management prepare for future uncertainties. This preparation was useful in enabling management to react more quickly to the 1973 oil crisis, for example (Wack, 1985). In 1978 King et al were describing 'long-range planning' in terms similar to those used for risk management today (King, 1978). Here the authors discussed the need to generate predictions of the future along multiple dimensions (staff, product, competition, etc.) and compare these predictions to the desired future organisational state, so as to identify management interventions required. They noted that this planning process would not eliminate risk, but should identify and help to manage risks, thereby increasing the "benefit/risk ratio". In 1981 Pomeranz et al used similar words to describe 'strategic planning' (Pomeranz, 1981). They observed that companies were increasingly engaging in strategic planning in an effort to better manage the "shifting conditions which can disrupt achievement of a company's long-range plan". They characterise strategic planning as a process that attempts to match environmental threats with corporate resources, and go on to suggest that the auditing of strategic plans can help to define business risks and verify that these risks have been "appropriately considered".

Although the concepts described in these earlier papers have much in common with risk management as it is understood today, efforts have been made over the last several years to develop the frameworks, tools and processes to drive and support improved risk management as a discipline aligned with but separate from strategic performance management.

It is noteworthy that, although managers have been addressing risk for centuries, a formal definition is still not agreed. In the early 1990s a definition of operational risk was first proposed, based on what it is not, rather than what it is. This early definition described operational risk as any type of risk not market-related (a risk caused by changes in asset prices) or credit-related (a risk caused by a failure to meet payment obligations) (Bernstein, 1996b). More recently, the influential Risk Management Group of the Basel Committee on Banking Supervision has proposed a more inclusive definition: "the risk of loss resulting from inadequate or failed processes, people, and systems or from external events" (The Basel Committee, 2001).

Risk Management and management action

Using the Basel definition above, the management of risk must therefore involve actions taken by management to minimise the likelihood of asset damaging or loss-generating events from occurring, and mitigating the impact on the organisation should they occur. Carey, in assessing the Turnbull Report, issued to provide guidance to listed UK companies to help them improve their internal controls, notes that the report calls on boards to identify risks that are significant to the fulfilment of corporate business objectives and to implement a sound internal control system to manage these risks effectively (Carey, 2000).

Although this process has not been standardised across firms, a generic version (EIU, 1995) typically has five stages as illustrated in Figure 2.

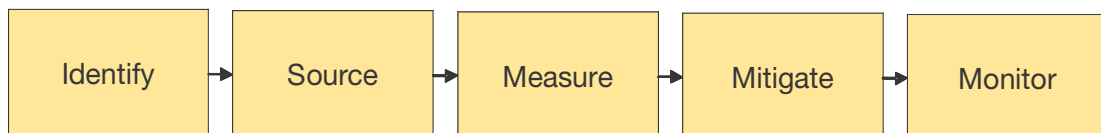


Figure 2 – A generic risk management methodology

The above stages include the following activities:

Identify: application of various tools, potentially including: scenario analyses, internal audit reviews, business process analyses, independent reviews, interviews, roundtable risk debates/workshops, checklist/questionnaires, brainstorming

Source: analysis of underlying root-causes of identified top level risks to facilitate measurement and mitigation activities

Measure: evaluation of likelihood and impact (operational, financial) of identified risk

Mitigate: development of plans to reduce or eliminate risk, based on the organisation's risk appetite/ability to cope with risk materialising, and cost/benefit analysis of mitigation activities; implementation of these plans

Monitor: review of plan implementation and effectiveness of control processes; continued identification of changes to risk profile and implementation of new actions to address

Over the last several years, Anglo-Saxon countries have also seen significant changes to regulators' expectations of what constitutes effective corporate governance, including rising pressure for improved risk reporting and for better integrated and more comprehensive risk management practices. Kleffner describes the conclusions of the Committee on Corporate Governance of the Toronto Stock Exchange as recommending that boards should take responsibility for stewardship, including strategic planning, risk management, and internal control (Kleffner, 2003).

Similar recommendations came from the Ludwig report, released in March 2002. This report summarised the findings of an investigation into the trading operations of Allfirst, the US subsidiary of Allied Irish Bank (AIB), and was initiated after massive losses were incurred through the fraudulent trading activities of a single employee. In reviewing the conclusions of the Ludwig report, Dunne notes that one of the report's key recommendations relates to improving the control environment within AIB, including that the AIB board take responsibility for matters relating to risk management and audit (Dunne, 2002).

The aforementioned Turnbull Report (ICAEW, 1999) provides another example of current regulatory practices. The report's primary objective is to assist company directors to embed and maintain effective internal control in the business processes by which the company

pursues its objectives, thereby helping to ensure compliance with the Combined Code governing listed companies in the UK. It states that a risk-based approach should be used to establish a sound system of internal control, and that this system should be incorporated within the company's normal management and governance processes, not treated as a separate exercise to meet regulatory requirements. The report emphasises that internal control systems play a key role in the management of risks to the achievement of business objectives, helping to safeguard shareholders' investments and company assets. The report also states that an effective system of internal control depends on the regular re-evaluation of the risks facing the company, as these risks continually change with the evolution of the company's business objectives, internal organisation, and external environment. Pragmatically, the authors recognise that even an excellent internal control system can not eliminate all risks, particularly those related to the occurrence of unforeseen circumstances. In this respect, the Report does not deal with exogenous or external risk management in any significant way.

Specifically, the Turnbull report recommends that the board of directors' responsibilities include:

- Identifying the risks facing the company
- Deciding the levels of risk acceptable to the company
- Evaluating the likelihood of these risks materialising
- Assessing the company's ability to reduce the incidence and impact of these risks
- Evaluating the costs and benefits of operating particular risk control systems
- Ensuring the ongoing effectiveness of the control system selected (while recommending that management be responsible for implementation of the board's risk control policies)

Although useful to UK directors seeking to comply with corporate governance regulations, the Turnbull guidance is not particularly original, having much in common with earlier advice on the implementation of sound 'strategic controls' within organisations, as illustrated by these recommendations from Muralidharan (Muralidharan, 1997):

- Agree unambiguous descriptions of a set of strategic goals, the achievement of which are likely to achieve the long-term vision of the organisation
- Agree the actions necessary to achieve these goals (causes) and the results they are expected to produce (effects)
- Monitor the implementation of the plan using indicators chosen and tailored to suit this particular purpose and subsequently use the information produced to inform management discussion/decisions about possible corrective actions
- Monitor changes in the external environment e.g. new/changed policy directives, sudden changes in the economy and update the plan on the basis of a) changes in external planning assumptions b) learning about the management team's cause and effect assumptions, identifying the need to change these when relevant
- Involve staff in the decision making process developing ownership and building on the combined operational insight of the organisation

Muralidharan highlights the need for this process to be continuous (as opposed to periodic strategic reviews) "in order for emerging strategic threats and opportunities to trigger timely changes to strategy".

Since 1995, Simons (Simons, 1995) has emphasised the same needs as those proposed by the Turnbull report and Muralidharan, encouraging managers to establish effective controls to

manage implementation of strategy as well as the inherent risks associated with strategic choices. Indeed Simons (Simons, 2000) describes 'strategic risk' as an unintended event or set of conditions that significantly reduces the ability of managers to implement their intended business strategy. He therefore argues that all strategic choices made by a management team invariably impact on the strategic risk profile of the organisation, thus providing a logical argument for the value of integrating approaches to risk management and strategic control/performance management. This argument is supported by the results of a recent survey identifying the failure to manage major projects as the highest operational risk facing organisations (McCraig, 1999).

Despite the similarities, a major difference between risk management and corporate performance management is the degree to which quantitative analysis is applied. The development of risk management tools has been led by the financial services industry, to allow better management of the major exogenous risk types facing this industry: credit and market risk. Both of these types of risk lend themselves to quantitative analysis, for example Monte Carlo simulation, financial statement modelling and loss scenario modelling (Hoffman, 2002), due in part to the wide availability of historical loss event data.

Hoffman's work suggests that the designers of risk management systems for assessing the impact of uncontrollable events or asset price movements tend to have a strong statistically-driven, predictive orientation, though these risk types may be special cases arising from the relatively mechanical characteristics of financial market transactions. Bielski warns that the unpredictable nature of human beings, coupled with an absence of comprehensive event loss data, means that a purely statistical approach to managing operational risk is inadequate (Bielski, 2002). She writes that risk management requires ongoing identification, evaluation and projection based on internal and external data, and that it necessitates prescriptive action. She goes on to say that management also implies total organisational involvement, versus gathering and creating numbers in some back room that are only seen by a few in the organisation and not acted upon in a timely manner at the line of business level.

Rucker builds on this in observing that simply identifying and monitoring these risks is insufficient and that organisations need to focus more on measuring and monitoring 'non-traditional' risks (Rucker, 2002). She argues that corporate leaders must be able to determine if risk management systems are actually working, and that one way to do this is through the use of 'key risk indicators' chosen to inform managers if the risk management activity dovetails with corporate goals.

We have recently seen this done well in a large multi-divisional hospitality company and badly in a major public sector organisation in the defence field. In the latter, the risks identified were focussed on the failure to achieve particular objectives rather than the factors underlying this failure, which could be managed.

This interest in qualitative and behavioural methods of risk assessment and management is consistent with the approach adopted by modern corporate performance management systems, which tend to rely on historical quantitative data and qualitative predictions about the future (Cobbold, 2002).

Case Study 1: Integration of Strategic Control and Risk Management

The following case study illustrates how one public sector organisation, an Australian environmental agency here referred to as AEA, uses risk management as an integral part of its strategic control process.

AEA's strategic control process is seen as part of a wider corporate governance framework and includes the responsibility for the Executive management team to set and communicate long-term strategic goals for the agency defining what the agency will deliver in order to meet the political outcome requirements stipulated by the state government to which it is accountable. Executive management translates these high-level long-term goals into 3-year action plans prioritising activities and initiatives deemed to deliver most effectively and efficiently the results required within existing resource constraints.

The 3-year plans are then translated into annual business plans defining the year's priority activities and initiatives for each division, section, and function of the organisation. The annual business plans are amended throughout the year as a result of an ongoing review process to incorporate new operational learning, threats and other changes to underlying planning assumptions, still in consideration of given resource constraints. Initial risk identification happens throughout the organisation as an integral part of this business planning and review process, and risk issues are referred for resolution in both a top down and bottom up manner.

AEA defines risk in a holistic fashion, as follows: "[A risk is] anything that may impede the achievement of objectives: the possibility of good things not happening, the threat of bad things happening and the potential that actual results will not equal anticipated outcomes". This broad definition means that for this organisation risk management overlaps much of what elsewhere is considered to be the strategic control process.

Identified risks are referred to five standing committees; Audit, Finance & Planning, Human Resources, Information Communication & Technology, and Gene Technology. The committees are composed of relevant subject matter experts from within the appropriate functional areas of the organisation, assisted by the Strategy & Risk department.

Each committee is responsible for evaluating the risks referred to them in terms of degree of risk (both likelihood and impact if crystallised) as well as effectiveness of existing controls or treatments, and the need for implementation of additional controls/treatments in the form of proposed culture, process and/or structural changes. The committees recommend appropriate courses of action directly to the relevant divisions, who are then responsible for incorporating the required risk mitigating activities into their business plans.

The committees are also responsible for monitoring both high-level risks and the implementation of their recommendations. However, where recommended new controls and treatments cannot be accommodated within existing budgets, new initiatives are prioritised by the Executive Management team as part of the ongoing strategic management and review process.

Assessing Risk within AEA

The risk assessment process consists of four distinct phases. The first phase of the process, Risk Identification, involves the generation of a comprehensive list of events that could negatively impact the achievement of the organisation's objectives and outputs, based on the high-level strategic plan and lower-level business plans. Next, during the Inherent Risk Analysis phase, the likelihood and consequences of these events are subjectively rated on a scale of 1 to 5, with consequences evaluated in terms of their impact on the organisation's stated objectives; impact is assessed on the dimensions of environmental impact, human impact, financial cost, business disruption and damage to reputation. The likelihood scale ranges from 'rare' to 'almost certain' and the consequences scale from 'insignificant' to 'catastrophic'. These ratings are then added to generate an inherent risk assessment. The third stage of the agency's process, Existing Control Analysis, begins by analysing the effectiveness of existing controls in addressing these inherent risks, with controls defined to include policies

and procedures, standards and specifications, codes of practice and other organisational protocols. These controls are first evaluated on a scale of 1 to 6 based on the existence of evidence that the controls have been implemented and are being reviewed. They are next rated on how well they are documented and communicated, this time on a scale of 1 to 3. Lastly the consistency of the application of the controls is assessed, again on a 1 to 3 scale. These three ratings are then summed to produce a total control rating, minimum 3, maximum 12, with scores of 7 to 12 defined as 'poor'.

The fourth stage, Residual Risk Analysis, involves the mapping of each identified risk on the dimensions of inherent risk and total control. The map is segmented into four quadrants with risks falling into the red quadrant (high likelihood and cost, low control rating) identified as requiring active management in the form of a new initiative or risk treatment plan. Risks in the yellow quadrant (high likelihood and cost, high control rating) are flagged for regular monitoring of control effectiveness. Risk in the blue quadrant (low likelihood and cost, low control rating) are deemed to require only the periodic review of inherent risk to identified changes to this. Finally, risks in the green quadrant (low likelihood and cost, high control rating) are identified as opportunities to re-allocate control resources to other areas exhibiting higher risks.

Managing Risk within AEA

When the risk measurement process is complete, a risk management plan is developed to document responsibilities associated with implementing and monitoring actions identified as required through the four stages of risk assessment. Based on this plan, risk treatment plans are developed for all risks in the aforementioned red quadrant, with these plans covering the allocation of responsibilities and resources, the establishment of milestones and deadlines, and reporting frameworks. Risk treatment plans are then embedded in the business plans of all applicable sections of the organisation. In this way, risk management is not the responsibility of senior management alone, but more appropriately the responsibility of all employees. The risk assessment and management processes followed at AEA are represented in Figure 3.

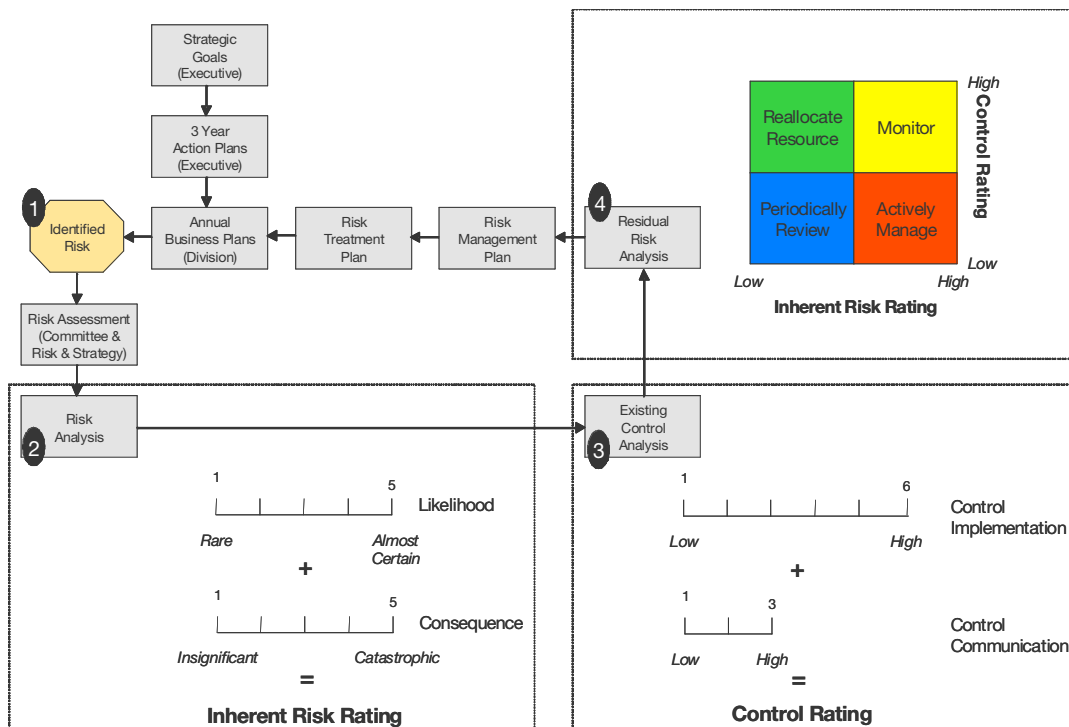


Figure 3: Risk processes within AEA

To maintain control effectiveness, risk treatment plans are reviewed on a periodic basis to ensure that the agreed risk mitigation activities are being conducted. To ensure the continued relevancy of this system, residual risks are re-evaluated on a periodic basis to capture the impact of the organisation's activities to mitigate identified risks. As with the best performance management systems, both the activities and the outcomes required to deliver the organisation's objectives are identified, and performance against activity completion and outcome achievement is reviewed. As with other deeply implemented performance management systems, actions, performance measurement, reporting and monitoring occur at all levels of the organisation. This risk management system is not analogous to the classical strategic performance management system, owned and operated at the highest levels of the organisation only. Rather it resembles a cascaded performance management system, where responsibility for its effective usage is allocated from senior management down to the front lines. For this agency, risk management is an organisation-wide undertaking.

Case Study 2: Identifying the Risks to Strategic Objectives

This case study, taken from a large European public sector organisation, illustrates the potential perils of failing to use a strategic control system to drive the risk identification process. The organisation, with an annual budget in excess of € 12b, is responsible for procurement and logistics to one of the largest ministries of the national government. For purposes of anonymity this organisation is hereafter described as the Government Procurement & Logistics Agency (GPLA).

The GPLA is governed through a three board structure consisting of a Main Board, a Programme Board, and an Executive Board. The Main Board sets the direction for the organisation through a strategic plan, monitors overall GPLA performance, and is responsible for managing the structural and process risks to the achievement of the strategic plan. The Programme Board focuses on delivery the organisation's change programme, covering all significant initiatives coming from the strategic plan, and is responsible for managing all risk to this change programme. Finally, the Executive Board has a shorter-term focus, managing the delivery of outputs to the levels defined in Customer Supplier Agreements (CSAs), and reconciling budgets, finance and outcomes.

Defining and managing the strategy

In 2003, the GPLA Main Board adopted the Balanced Scorecard as their key tool for monitoring and managing organisational performance to the levels required to achieve the strategic plan. Supported by the authors of this paper, the Main Board developed a 3rd Generation Strategic Balanced Scorecard, using a design process based around a series of highly facilitated, 1-day workshops attended by all board members. The resulting Balanced Scorecard consisted of a Destination Statement, a Strategic Linkage Model, and measures and targets for each of the 24 Strategic Objectives selected by the Board. The objectives were split between twelve Activity Objectives (which focused on the major actions required of the Board over the following 12-18 months) and twelve Outcome Objectives (which focused on monitoring the impact and / or consequences of these activities compared to key elements of the longer term strategy). The role of Balanced Scorecard for GPLA is described in the organisation's latest business plan,

“The fundamental principle behind the scorecard is ensuring that we achieve the expected results from the actions we take in order to achieve our goals. It is not only designed to check whether decisions have been successfully implemented but also to enable us to review whether we are taking the right actions and getting the right results.”

For example, a key element of the GPLA strategy was a move toward greater recognition of, and accountability for, the importance of satisfying its stakeholders' needs. But in the face of

tightening budgets, the Board believed that to do this would require GPLA (and its customers) to be even more clear about what was required, by whom, and when. GPLA planned to create and use 'Customer Service Agreements' to achieve this. Accordingly, one Activity Objective chosen by the Board was titled [GPLA ensures that its] "CSAs reflect customer requirements" (words in [] were implicit in the original and are added here for clarity). The objective relates directly to activities that the Board has identified that it needs to undertake itself. The objective also was seen by the Board as an essential contributor to achievement of one its selected Outcome Objectives titled "Satisfied customers". For both of these objectives, measures and targets have been identified, and together these measures allow the Main Board to track performance of what is considered to be a vital Board activity (ensuring the creation of better CSAs) and the impact of this activity on a key outcome (higher customer satisfaction).

Additional Activity Objectives were selected, the measures of which allowed the Main Board to monitor the performance of both the Executive and Programme Boards in meeting their primary responsibilities. One of these objectives, "Monitor Executive Board", is tracked using measures relating to the percentage of CSAs delivered on budget to the satisfaction of customers. The second objective "Monitor Programme Board (Progress on change)" is tracked using measures of programme benefits delivered and programme milestones achieved. The Main Board Balanced Scorecard is therefore useful in mitigating the risk that the other two boards fail to achieve their primary objectives, by making their performance visible and allowing the Main Board to intervene quickly if required.

The Main Board now meets quarterly to review and discuss performance against the 24 Strategic Objectives, and to evaluate the risks to the delivery of the Strategic Plan. The Main Board is also planning to review and reset their Balanced Scorecard on an annual basis, to redefine their Strategic Objectives as these are either achieved or supplanted.

Managing Risk and Performance

Separate from the design of a Main Board Balanced Scorecard, a draft risk register was produced by a non-executive director and then further developed by the Main Board. Although not in a form that can be reproduced here, the register included a mixture of operational management issues (for example, effective control of its budget) and several critical risks that themselves were beyond the direct control of the Board but for which contingencies could be prepared (for example, mitigation of the cost and service impact of consolidation or bankruptcy of major suppliers).

A 'risk management' hierarchy was also proposed, whereby each level of hierarchy within the organisation would be charged with identifying a similar set of 'top level risks' that related to management issues at that level. In addition, the issue of how the risk register could or should be validated was raised, but not satisfactorily resolved.

Similarities between the "top-level risks" that related to operational management issues and the activity objectives on the Corporate Balanced Scorecard were noted. To evaluate this, a cross-check between the two independently developed lists was carried out. The linkages between objectives and risks are illustrated in Figure 4 overleaf, with the grey cells indicating Strategic Objectives for which a comparable entry in the risk register was identified.

Top Level Risks

	1	2	3	4	5	6	7	8	9	10	11	12
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
23												
24												

Figure 4: Strategic Objective - Risk Mapping

It is noteworthy that not all Strategic Objectives were matched to risk register entries. In fact this mapping suggests that some 40% of the Objectives identified by the Board as being critical to the achievement of its strategy were not recognised as being critical by those preparing the risk register. Given the nature of the Objectives chosen, and the process used, this result seems to indicate that not all of the risks that should have been on the risk register were identified in the process used to create the risk register, and that consequently the risk register did not reflect accurately the true risk profile of the GPLA. If true, this suggests that the identification of organisational risks in isolation from the development and

management of strategic objectives has the potential to leave organisations exposed to significant, unrecognised risks.

Implications for risk and performance managers

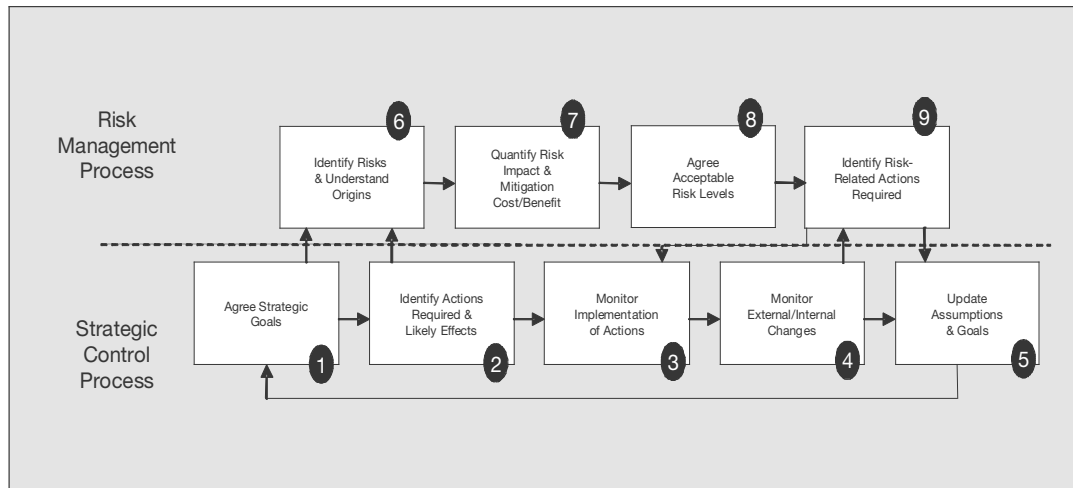
The review of risk management methodologies reveals that they are designed primarily to help managers identify the actions required to maximise the likelihood of organisational objectives being achieved - something managers have been doing as an integral part of their approach to strategic control and corporate performance management since well before the phrase 'risk management' entered the business lexicon. As a result, the risk management systems that are being implemented across organisations today have much in common with systems designed to manage organisational strategic performance. This implies considerable scope for duplication of effort, and also (if the GPLA case is representative) exposes weaknesses arising from their separation.

The recommendations of the Turnbull report for integrating the management of risk and organisational performance in general as part of a coherent approach to corporate governance therefore seems both prudent and practical. This not least because an organisation's exposure to risk and its willingness to accept risk is ultimately decided by the strategic choices it makes, as stated by Simons.

Simons' view is also reflected in the approach used by the organisation in the case study. AEA uses the strategic objectives produced by its strategic control process as the starting point for risk management. Recommendations outlining risk mitigation activities and initiatives evaluated against existing business plans - another outcome of a strategic control process - are reported back to the management team for evaluation and prioritisation. The result of this prioritisation process feeds back into the strategic control process in the form of a) additional activities included in business plans and b) as additional performance indicators used to monitor development in residual risk i.e. the effectiveness of the risk mitigating action plans.

The above suggests that the existence and effective use of a robust approach to corporate performance management and strategic control is a major critical success factor for the successful implementation of a combined solution. Risk management without an effective strategic performance management system to provide the context for risk evaluation will in the best case provide only limited value and in the worse case can misguide the organisation's control efforts, possibly even obscuring more important strategically defined risks.

We therefore propose an approach that uses the process outlined in Figure 5 below.



The strategic control framework selected is not itself important, although it must meet the requirements outlined by Muralidharan above. In our experience, however, the 3rd Generation Balanced Scorecard (Cobbold, 2002) provides a good example of a proven framework for strategic control into which risk management sub-processes can readily be incorporated.

The components of the 3rd Generation Balanced Scorecard design process match components 1 – 3 of the Strategic Control process as illustrated in Figure 5:

- **Destination Statements:** long-term goals describing in some degree of detail what the organisation should look like at some point of time in the future (equivalent to component 1 above)
- **Strategic Objectives:** activities and their expected outcomes defining what needs to happen to ensure achievement of the long-term goals and intermediate goals on the way to the long-term destination (equivalent to component 2 above)
- **Balanced Scorecard Performance Measures and Targets:** measures for each strategic objective are chosen to inform management of progress in achieving the strategic objectives; targets are set for each measure to enable performance evaluation (equivalent to component 3 above)

An additional output of a well-structured Balanced Scorecard design and review process is a number of discretionary initiatives or projects that are usually identified to initiate, for example, the implementation of new processes and activities.

By using the Balanced Scorecard/Strategic Control components 1 and 2 as input to the risk assessment process, it is possible to identify risks to: a) the achievement of agreed strategic objectives/goals, and b) the successful completion of actions necessary to deliver these goals (components 1 & 2). Thereafter the risk assessment activities of component 7 can be conducted, typically by specialists rather than generalist senior managers. With this

understanding of the organisation's risk profile and the costs and benefits of various risk mitigation options, senior managers are then able to make decisions about the levels of risk they are prepared to accept (component 8), allowing them to then agree the actions required (component 9), generally in discussion with line management, the people who will be responsible for completing these actions. This agreed list of actions should now be used to update the strategic goals/objectives where these risk mitigation activities are significant enough to warrant inclusion in the organisation's strategic goals. Thereafter, senior management should regularly review progress in the implementation of activities chosen to deliver the organisation's goals, including the activities selected as part of the risk review (component 3). They should also periodically assess changes to their original assumptions about the business model, including their assumptions about the organisation's risk profile (component 4). Any significant changes that are identified will then drive changes to both risk mitigation requirements and the organisation's higher level goals. Thus a cycle of planning, acting, and reviewing can be embedded, allowing senior management to manage risk within the strategic control framework.

Conclusions

Corporate Governance as an activity carried out by the Board of an organisation appears to be little different from what elsewhere is considered to be classical 'management' activity. The various levels of management within an organisation may have differing priorities, agendas and resources, but all are essentially concerned with using the resources directly within their control to meet the achievable expectations of their key stakeholders. At Board level, particularly for quoted firms and public bodies, the key stakeholders typically include some form of regulator (e.g. stock exchange authorities) which set expectations, often supported by legislation, for the visible, and effective management of "risk" by board members. Other stakeholders will have expectations that also demand "risk management" of one form or another, for example, ensuring the delivery of high levels of organisational performance will necessarily require the Board to identify and mitigate any identifiable risks that might prevent this outcome.

We conclude that performance management and risk management have the same ultimate goal, ensuring the achievement of an organisation's strategic objectives. The terminology used is different: performance management has typically focused on ensuring that 'good things' occur as planned; risk management has typically focused on ensuring that 'bad things' do not occur. We believe that the difference between these two approaches is largely linguistic.

Risk management is increasingly perceived to be an essential element of good corporate governance, and the requirement for visible 'risk management' processes from stakeholders will require it to continue to be actively addressed by top level management teams. However, this paper has shown that much of what is considered to be Risk Management also features in best-practice Performance Management activity, which is itself also of current interest to organisations. Accordingly, there appears to be an opportunity for Risk Management and Performance Management to be combined into a single, holistic, process. It is therefore useful to first develop a robust approach to ensuring strategic control of the organisation, before implementing risk management processes. A sequential approach should not only improve the efficiency and effectiveness of both systems, but more importantly create a strategic context for the calculation of risk, thereby better informing decisions on risk management investment. The paper also concludes, that of the performance management frameworks currently available, the latest "3rd Generation Balanced Scorecard" framework has potential utility as the basis for such a combined system.

About 2GC

2GC is a research led consultancy expert in addressing the strategic control and performance management issues faced by organisations in today's era of rapid change and intense competition. Central to much of 2GC's work is the application of the widely acknowledged Balanced Scorecard approach to strategic implementation, strategy management and performance measurement.

References

- Anonymous (1998). "The changing face of risk management", *The Internal Auditor*, Vol. 55, Issue 5, pp. 11-12.
- Bernstein, Peter L. (1996a). *Against the Gods: The Remarkable Story of Risk*, New York: John Wiley & Sons, Inc., p. xxii.
- Bernstein, Peter L. (1996b). "The new religion of risk management", *Harvard Business Review*, Vol. 74, Issue 2, pp. 47-52.
- Bielski, Lauren (2002). "The Great Risk Debate", *American Bankers Association Banking Journal*, Vol. 94, Issue 2, pp. 58-64.
- Carey, Anthony and Nigel Turnbull (2000). "The Boardroom Imperative on Internal Control", *Financial Times, Mastering Risk Supplement*, 25 April 2000.
- Cobbold, Ian and Gavin Lawrie (2002). "The Development of the Balanced Scorecard as a Strategic Management Tool", PMA2002, Boston.
- Delamontagne, Robert P. (2003). "Reducing risk through training", *Industrial Safety & Hygiene News*, Vol. 37, Issue 2, pp. 1-2.
- Dunne, Theresa M. and Christine V. Hellier (2002). "The Ludwig report: Implications for corporate governance", *Corporate Governance*, Vol. 2, Issue 3, pp 26-31.
- Economist Intelligence Unit (1995). *Managing Business Risks*, pp. 25-33.
- Hoffman, Douglas G. (2002). *Managing Operational Risk: 20 Firmwide Best Practice Strategies*, New York: John Wiley & Sons, Inc.
- King, Dennis and Walter G. Beevor (1978). "Long-Range Thinking", *Personnel Journal*, Vol. 57, Issue 10, p. 542.
- Kleffner, Anne, Ryan B. Lee and Bill McGannon (2003). "The effect of corporate governance on the use of enterprise risk management: Evidence from Canada", *Risk Management and Insurance Review*, Vol. 6, Issue 1, Pg 53-65.
- Lewis, Michael A. (2003). "Cause, consequence and control: Towards a theoretical and practical model of operational risk", *Journal of Operations Management*, Vol. 21, Issue 2, pp. 205-224.
- McCraig et al., (1999). *Deloitte & Touche Finance Directors Risk Benchmarking Results*, p. 12.
- Minzberg, Henry, (1994). "That's not 'turbulence' Chicken Little, it's really opportunity" *Planning Review*, November 1994, Vol. 22 Issue 6.
- Muralidharan R (1997). "Strategic Control for Fast-moving Markets: Updating the Strategy and Updating the Performance", *Long Range Planning*, Vol. 30, pp. 64-73.
- Pomeranz, Felix and James Gale (1981). "Auditing the Strategic Plan", *Journal of Accounting, Auditing & Finance*, Vol. 4, Issue 2, p. 162.

Rucker, Susan (2002). "Gauging success with key performance indicators", *Risk Management*, Volume 49, Issue 2. p. 6.

Simons, Robert (1995). "Control in an age of empowerment", *Harvard Business Review*, Vol. 73, Issue 2.

Simons, Robert (2000). *Performance measurement & control systems for implementing strategy*, New Jersey: Prentice Hall.

Stevenson, Howard H. and Mihnea C. Moldoveanu (1995). "The Power of Predictability", *Harvard Business Review*, Vol. 73, Issue 4, pp. 140-144.

The Basel Committee on Banking Supervision (2001). *Consultative Document: Operational Risk*, Basel, Bank for International Settlements, p. 2.

The Institute of Chartered Accountants in England and Wales, Internal Control Working Party (1999). "Internal Control: Guidance for Directors on the Combined Code".

Wack, Pierre (1985). "Scenarios: Uncharted Waters Ahead", *Harvard Business Review*, Vol. 63, Issue 5. pp. 72-90.

Witzel, Morgen (2002). "Risk prevention is the best cure", *Financial Times*, *Understanding Risk Management Supplement*, November 20, 2002.