Risk-Intelligence-Security-Control
R.I.S.C. International (Ireland)

The Requirement for a Director of Corporate Defence in UK Banking Institutions

SUMMARY PROPOSAL

Subject Matter:	Measures to Improve the Corporate Governance of UK banks
Date Report Issued:	26th May 2009

The attached proposal specifically addresses measures to help improve corporate governance in UK banks. The report represents an independent representation and was not commissioned by any of the parties referred to in the report. Therefore the views and opinions expressed should be considered to be the personal views and opinions of the author.

By Sean Lyons
Principal
R.I.S.C. International (Ireland)
sean.lyons@riscinternational.ie

R.I.S.C.
International

R.I.S.C. International

CONTENTS

A. THE REQUIREMENT FOR A DIRECTOR OF CORPORATE DEFENCE IN UK BANKING INSTITUTIONS

B. EXECUTIVE SUMMARY

The banking crisis has cruelly exposed how UK banks failed to adequately defend the interests of their multiple stakeholders and has resulted in the reputation of the banking sector being severely tarnished. This proposal specifically addresses measures to help to improve corporate governance in UK banks, by focusing on the requirement to strategically manage the critical components which constitute an organisation's program for self-defence (i.e. governance, risk, compliance, intelligence, security, resilience, controls & assurance). The central theme of this proposal is that there is now a strategic imperative to create the position of Director of Corporate Defence in UK banks.[1] The report proposes that the presence of this position within UK banks would help to urgently address the following matters:

- The requirement to improve the existing lines of defence in UK banks
- The requirement to re-balance the boardroom culture in UK banks
- The requirement to align business generation and operational activities
- The requirement to adequately defend the diverse interests of the stakeholders

The following recommendations are therefore proposed:[2]

- The position of Director of Corporate Defence should be created as a requirement for all UK banks.
- This position should have oversight responsibility for the strategic management of all defence related functions.
- This position should be the champion for all defence related activities throughout the enterprise.
- This position should be a full board appointment.
- This position should report directly to the Board.
- The focus of this position should be on helping the institution to deliver sustainable value in the long term.
- This position should help in the alignment of their business generation and operational activities.
- This position should be entrusted with helping to safeguard the interests of all the stakeholders of the institution.

In summary this report proposes that the appointment of a Director of Corporate Defence, to effectively safeguard stakeholders interests, will help provide tangible evidence that the current weaknesses are being addressed, and will go a long way towards helping to restore public confidence in UK banks, and the challenge of helping to repair the damage done to the reputation of the UK banking sector.

[1] Akin to the senior cabinet position occupied by the Minister for Defence in the UK government.
[2] Please refer to section E of this report for further details on these recommendations.

C. BACKGROUND

The Banking Crisis

In recent times there has been a significant change in the economic conditions which UK companies in the banking sector have been operating, so much so that it is now regularly referred to as the banking crisis.

Wide Ranging Reviews
A number of reviews have been performed by different groups in relation to identifying the causes of this banking crisis and many have been accompanied with recommendations on how to help create a more robust banking system going forward. Examples of some of these reviews include the Turner Review[3], the Treasury Committee Review[4] and a review currently in progress by the FSA[5].

Review Recommendations
Completed reviews have identified common causes of the current banking crisis and there has been numerous recommendations focusing on the remedial action required. Generally these recommendations can be classified as follows:

- Recommendations which require international agreement (i.e. require the general consensus of multiple international organisations).
- Recommendations which can be implemented domestically (i.e. can be independently implemented in the UK).
- Recommendations which can be addressed by the individual banking institutions themselves.

Corporate Governance Reviews
Many of these reviews have identified failures in corporate governance and the management of risk as issues which have contributed to the occurrence of this banking crisis. This specific area is now the subject of further review, with the expectation of future recommendations on how best to remediate these failures in order to improve governance structures and the management of risk going forward. The objective clearly is to avoid a recurrence of these or similar failures occurring again at some point in the future. Ongoing reviews addressing this specific area include an independent review by Sir David Walker[6] and the FRC's review[7] of the combined code of corporate governance. Internationally the OECD[8] has already reported on the lessons to be learned from the international financial crisis.

[3] The Turner Review: A regulatory response to the global banking crisis – FSA (March 2009)
[4] Banking Crisis: dealing with the failure of the UK Banks – House of Commons Treasury Committee (April 2009)
[5] A regulatory response to global banking crisis – FSA
[6] The Walker Review – Sir David Walker
[7] Review of the Effectiveness of the Combined Code – FRC
[8] The Corporate Governance Lessons from the Financial Crisis – OECD (February 2009)

The Science and Art of Corporate Defence

The banking crisis has highlighted that the interests of the stakeholders were not adequately defended in this instance and it has exposed failings in the traditional lines of defence which were relied upon to safeguard the banking sector. Lessons need to be learned from these failings in order to ensure that the sector is adequately insulated against financial, physical and reputational damage going forward. This requires an appreciation of the concept of defence. The verb defend is generally defined as to take measures to make or keep safe from danger, attack or harm, and implies the actions of protecting, safeguarding, shielding, supporting or preserving. The requirement to defend can be associated with an individual, group, place or thing, and can be associated with honour, reputation, territory, assets and allies.

Defence in the National Context

In most developed economies governments consider their duty to defend their citizens as a fundamental duty, and consequently the responsibility for national defence is held in high regard. The post of Minister or Secretary of Defence is generally considered to be a senior cabinet position, reporting to the Prime Minister or President. The Minister or Secretary of Defence has responsibility for managing the Ministry or Department of Defence. The Ministry or Department of Defence in turn generally has ultimate responsibility for formulating defence strategy and policy, and for integrating policies and plans in order to achieve defence objectives. All defence related activities, including Army, Navy, Air Force, Marine Corp etc ultimately report to this Department or Ministry while still retaining responsibility for tactical planning and for on the ground operation, implementation and execution. This allows for the strategic alignment of all defence related activities while also (if competently applied) facilitating the tactical co-ordination and operational integration of these activities.

Defence in the Sporting Context

In team sports in particular there is a real appreciation of the requirement to focus on defensive strategies and tactics in order to ensure that these are successfully implemented in the field of play. There is a clear understanding of the relationships which exist between the interaction of both offensive and defensive personnel and how collectively as a team there is a requirement to have an appropriate balance between these two inter-dependent disciplines. Coaches are aware that in order to be successful on the field of play, the game-plan must include the team's ability to be able to both attack and defend as required, and be capable of turning defence into offence and vice versa as the occasion demands. Many teams have specialist defensive coaches who are dedicated to helping to develop the diverse skills required in order to execute their strategies and tactics effectively. These coaches are very much aware that the defensive unit as a whole is made up of individual specialist positions which need to be filled by players of suitable character and ability. Developing the unit begins with recruiting the

required squad of individuals and by coaching these individuals on the necessary technical skills required. The selection of the starting line-up is based on the players best suited to address the team's defensive requirements. These selected players must then be coached on how to play as a cohesive defensive unit. This unit must learn to play and interact with the offensive unit as a team so that all the players involved are contributing to the greater common goal. Finally the team must learn to continually develop both its individual and collective skills in order to constantly improve, and in order to reach the increasingly higher levels of performance required if they are to achieve sustainable success.

Defence in the Corporate Context

Although the term "corporate defence" has been in use for many years and is perhaps intuitively understood, its specific meaning can differ from person to person and indeed from organisation to organisation. Its precise definition can also vary depending on the circumstances in which it is applied. Typically it is addressed only as a reactive response to legal compliance or pending litigation. Other times it is only addressed in a very narrow focus such as a security or resilience issue. As a result the very objective of defending the organisation appears not to be fully understood or indeed its requirement fully appreciated. Many defence related activities are however employed by organisations to help to safeguard and mitigate against risks, threats and hazards. These activities do share a common high level objective, that of helping to defend the organisation, and therefore it could be said that they represent different lines of defence, or multiple layers of defence. Corporate defence therefore in its broadest sense could be said to represent an organisation's collective program for self-defence. The traditional lines of defence in the corporate world are represented by the Board having responsibility for corporate governance, executive management having responsibility for the control environment, with oversight committees and various defence related functions (i.e. compliance and risk management etc) having responsibility for providing supplementary support and assurance. Additionally internal audit has responsibility for auditing the previously mentioned aspects, and external audit for providing independent assurance in relation to the preparation of accounts etc. Unfortunately all too commonly these activities are very often not managed in a coordinated manner and are therefore not operating in unison towards common goals and objectives. Frequently they actually operate independently and in isolation of one another in silo type structures.

Lessons to be Learned

Perhaps one of the lessons to be learned from this banking crisis is the requirement for banking institutions to prioritise the strategic alignment and co-ordination of their defence related activities and perhaps begin addressing defence in the corporate context in a manner similar to that adopted in the national and sporting contexts.

D. PROPOSAL SCOPE AND APPROACH

The scope of and the approach taken to this proposal was as follows.

Proposal Scope

This proposal is intended to only address a specific aspect of the wide-ranging measures required to improve the corporate governance of UK banks. It is not intended to address all the corporate governance issues which may need to be addressed, however it should go some way to addressing many of these issues both directly and indirectly. It is also not intended to address the broader issues which have been identified as the common causes of the current banking crisis.

The solutions recommended in this proposal are intended to relate to recommendations which can be introduced domestically (via the financial regulator or otherwise) and which can be implemented in the immediate future by the individual banking institutions themselves. It therefore focused on the re-organisation of elements of existing corporate governance structures which can separately by accompanied by more prescriptive regulation if necessary. Any such prescriptive regulation is considered to be outside the scope of this proposal.

Proposal Approach

The approach taken in preparing this proposal consisted of reviews and analysis of the relevant sections of the numerous reports already available on the topic of corporate governance itself, and wider ranging reports. It also involved reviews of numerous papers, articles, statements and comments from various journals, magazines, newspapers, websites, blogs and discussion groups[9] etc. All of this was blended with the author's experience, research, and development in this space over many years[10] (see Appendix IV for author bio details).

[9] A special reference should be made to the international Governance Discussion Group (GOV DG) which is moderated by Dan Swanson. Many of the issues which have been addressed in this report have been the subject of much debate within this group in recent months.

[10] Including a recent Q&A series entitled "Corporate Defense Insights: Dispatches from the Front Line" which featured expert commentators from around the globe sharing their insights, experience and expertise in relation to the critical components which constitute an organisation's program for self-defence (see Appendix IV).

E. MATTERS TO BE ADDRESSED

1. Requirement to Improve the Existing Lines of Defence in UK Banks

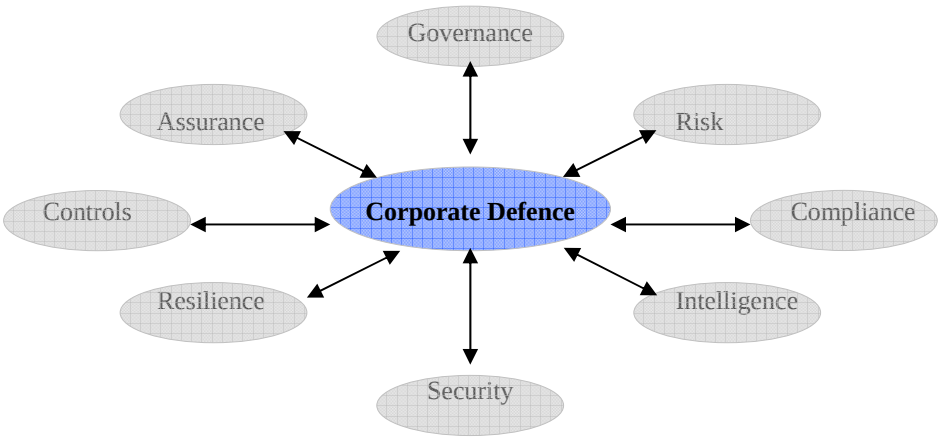
The Chancellor of the Exchequer, Alistair Darling, when commenting on the UK government request for a review to recommend measures to improve the corporate governance of UK banks (chaired by Sir David Walker) is reported to have stated the following:

> "*As part of our review of supervision of financial institutions it is clear that corporate governance should have been far more effective in holding bank executives to account. I have therefore asked Sir David [Walker] to carry out a thorough review and to make recommendations for improving what should have been the first line of defence.*"

Critical Components of a Program for Self-Defence

The recent crisis has highlighted a need to re-organise the various lines of defence in a more effective and efficient manner. Addressing the broader issue of corporate defence (i.e. safeguarding, protecting, shielding etc) can only help organisations in the adoption of a longer term view on how best to safeguard the welfare and wellbeing of the organisation. Addressing the longer term agenda (rather than a short sighted kneejerk reaction to individual issues in isolation) requires focusing on corporate defence as an umbrella term used to describe an organisation's overall program for self-defence. A comprehensive corporate defence program therefore involves incorporating the critical components which constitute this program for self defence. All of these critical components (see figure 1) are increasingly inter-connected and interdependent, and therefore continuously impact on one another (see Appendix I).

Figure 1 – Critical Components of Corporate Defence



A comprehensive program of self-defence certainly includes the management of governance and of risk[11], but it also includes the management of the other critical components. Effective corporate defence requires that each of these components is strategically managed as part of a coherent corporate defence program.

Oversight and Strategic Management of Defence Related Functions

Unfortunately in many organisations these defence components tend to operate in silo type structures. This means that they are not in alignment with one another, but rather they operate in isolation as there tends to be little or no interaction, sharing of information, or indeed collaboration. Frequently there is also very little cross-functional support among these components as each is operating towards its own narrow view and objective, and as a result they can very often be the subject of internal disputes and power struggles. Very often the overall responsibility and accountability for corporate defence is dispersed or fragmented, diluted or ambiguous, meaning that at times oversight is effectively non existent. As a result an organisation can be subjected to typically negative consequences. Confusion relating to overall responsibility and accountability can result in omissions or gaps, and these in turn can create vulnerabilities which can later be exploited, rendering many other related best efforts ineffective in the process. Silo type structures typically result in multiple intersections, duplications and overlaps of activities which can result in considerable inefficiencies and unnecessary redundancies. In worst case scenarios the power struggles which can occur can actually develop into full scale turf wars, and this can be extremely detrimental to its corporate health and can lead to a the creation of a dysfunctional organisation.

Corporate defence management requires a paradigm change (see Appendix II) as it should ultimately be about maintaining oversight of these defence related activities (see Appendix III). Success in corporate defence requires a strategy or program which can be managed across the organisation. Ultimately, the organisation needs to identify and prioritise major risks resulting from its activities as well as maintain oversight and control over business processes to mitigate these risks. This requires the organisation to deploy an infrastructure and supporting processes that deliver transparency across the business and its relationships. A streamlined defence program is one in which responsibility and accountability is effectively managed and the business has a framework to

[11] The term risk management in UK banking generally means prioritising the management of financial risk, hence risk committees can tend to prioritise credit and market risk above operational risk. In fact operational risk in many banks is focused solely on the most effective use of risk capital and on the abstract measurement of risk using complicated risk models and quantification techniques. This narrow focus on risk led to a misplaced over-reliance on sophisticated maths to manage risk. However not all risks can be measured solely in quantitative terms. For example reputation risk can be the result of an event that at first glance may be perceived as trivial and its direct 1st order consequence may only represent an immaterial monetary amount. Its indirect 2nd and 3rd order consequences can however cascade, creating a negative emotional impact on stakeholders which can indirectly result in a substantial monetary impact. Corporate defence involves addressing financial risk as a subset of corporate risk but also involves ensuring that a more comprehensive risk assessment process is in place to evaluate potential exposure.

understand and manage the diverse complexity of defence issues.

The Status Afforded to Defence Related Activities

In hindsight many of the issues which led to the financial crisis seem to be self evident with an obvious outcome, even to the lay person. Given that the professionals responsible for this crisis in banking were perceived to be the best and brightest, how was this crisis allowed to occur? How did so many defence related activities fail to safeguard their institutions against the banking crisis? How did corporate governance structures and risk management systems allow these damaging activities to occur, and where were the other layers of defence such as the Compliance Officer, General Counsel, Company Secretary and the Internal Auditor[12] etc when all these issues first began to surface?

It seems that the institutions which appear to have weathered the storm relatively well were those which generally had a balanced view of both the upside and the downside. These institutions seem to have had a comprehensive approach to viewing company wide exposures, while also communicating information effectively on these exposures across the organisation. In those institutions that were not so "lucky" it appears that in many cases the strong drive for short term profit was the primary focus and this overrode any other concerns including any caution expressed by the defence functions. It appears that this focus on the production of short term profits meant that these organisations had little regard for the operative business risks and therefore any concerns or warnings simply fell on deaf ears. In some cases no concerns appear to have been expressed, or were not expressed in a strong enough manner. There are many reasons for this failing but it is perhaps primarily to do with the lack of status[13] and authority afforded to these defence functions, and the development of a culture whereby these functions were stigmatised as business disablers. In many instances representatives of defence related functions were therefore not included in the decision making loop, leading to an imbalance in the decision making process. In some cases the functions themselves proved to lack sufficient professional competence to rise to the occasion, whereby the functions lacked the necessary qualifications, experience and expertise required to adequately address the challenges they were faced with. Unfortunately there are also cases where the heads of these functions simply lacked the conviction, determination and moral fibre to deal with the issues in a manner which would have been expected by the stakeholders.

[12] In relation to the assurance component, internal audit is considered to be an activity which can certainly add value to the corporate defence process by being in alignment with the corporate defence program. However it is probably best that it retains a separate reporting line in order to be in a position to provide independent assurance on the operations of the corporate defence program itself, and its individual components, in an objective and impartial manner.

[13] In the financial world rarely (if ever) were those with responsibility for preventing the dollar from going out the back door held in the same high esteem as those with responsibility for bringing the dollar in the front door. Defensive activities have traditionally been mocked as "business prevention centers" and often considered as no more than pure cost centers that stood in the way of making money. As we have seen the result of such an attitude can be catastrophic, the financial tsunami being a prime example.

Recommendations

1.1 The position of Director of Corporate Defence should be created as a requirement for all UK banks.

The Director of Corporate Defence should be responsible for helping to ensure that the organisation has a coherent corporate defence program in place. The creation of this position should ideally be mandatory in nature, perhaps a legal requirement to retaining or procuring a banking licence. Such an appointment will help the organisation to focus on the broader set of risks and threats to which these organisations are exposed. The creation of such a position means taking a longer term view and goes beyond the governance and risk management issues identified as causes of this particular crisis, although it does address many of these issues in the process. It will help to provide broader protection against a very different set of circumstances which may present themselves at a time of future crisis, where banking institutions are faced with a totally different set of risks (i.e. corporate terrorism, pandemics etc).

1.2 The Director of Corporate Defence should have oversight responsibility for the strategic management of all defence related functions.

This means having responsibility for harmonising these functions at strategic, tactical and operational levels, and recognising the interconnectivity and interdependence which exists. It means having responsibility for developing a holistic framework for corporate defence which involves coordinating and integrating all of the defensive activities so they are managed in a coherent manner, ensuring that all activities are operating in unison towards common objectives so that they are collectively defending the organisation.

1.3 The Director of Corporate Defence should be the champion for all defence related activities throughout the enterprise.

The position of Director of Corporate Defence would help to redress the imbalance relating to the lack of status and authority afforded to defence activities. Not only would the position provide a single reporting line to the Board for all defence related activities, it would also have an important role to play as the champion of these activities within the organisation. This position therefore involves promoting a more positive image of defence related activities throughout the enterprise and to help ensure that they receive the appropriate standing within the organisation. The position is also responsible for ensuring these activities possess sufficient competence to perform their duties. In this capacity the Director will be required to fill a number of different roles including those of watchdog, teacher, coach, counsellor and leader.

2. Requirement to Re-Balance the Boardroom Culture

Board Failures

While the details of the causes of this unprecedented crisis continue to unfold, the findings of a number of reviews have already pointed out that serious deficiencies in corporate governance were experienced, whereby boards failed to adequately identify and constrain excessive risk taking. It is commonly accepted that the necessary challenge was missing from governance structures and in particular in relation to the boards, where a "follow the herd instinct" led to a reluctance to "breakaway from the pack" and express dissenting views. Non-executive directors (NED) appear to have failed in their role to provide strong independent oversight of executive management and lacked the necessary resolve to restrain overbearing CEOs. Indeed it has been stated that often eminent and hugely experienced individuals acting as NEDs failed in the proper scrutiny of the banks activities.

It has been suggested that a different mindset is now required and that there needs to be a re-balance of culture in the boardroom itself. The Turner Review has noted that (while awaiting the findings of the Walker Review) issues and implications for overall governance principles need to be looked at in an integrated fashion. However in practical terms the Board must remain responsible and accountable to shareholders for the governance of the organisation in all respects, including the design and execution of any governance structures. Therefore any proposed changes to existing governance structures within the organisations themselves will require the full participation and involvement of the Board, as it is still very much responsible for setting the "tone at the top".

Separation of Powers

Many commentators have argued that one of the critical issues which will need to be addressed is that of separation of powers. It has been suggested that in general the balance and separation of powers was just far too weighted in favour of the CEO and their executive. Many of the governance shortcomings have been attributed to flaws in the compensation systems which existed in banking where the design of remuneration policies and the incentives being offered actually encouraged a culture where short term achievements were rewarded even though they were not in the best interests of the long term success of the organisation. This lack of alignment to long-term strategies and goals resulted in undue risk taking through an endless "search for yield" at all costs. It also had the affect that management in turn tended to focus on measures which were defined and rewarded to the exclusion of those which were not, including prudent risk management. All of which led to what has been described as a "cultural indisposition to challenge" the chain of command, not only in the boardroom but throughout the organisation. Such a culture of stifling contrary opinions helped create an environment rich in over confidence leading to overly optimistic strategies. Of course any proposed changes in governance structures will need to rectify the above starting with a review of compensation and remuneration.

However it has also been suggested that structural changes[14] in relation to the composition of the Board are required within the organisation itself, with a view to counterbalance any possible future weaknesses in remuneration incentives etc.

Delivery of Long Term Sustainable Value

In a low interest environment investor pressures were fierce, leading many financial institutions to undertake risks that simply were not in the best long term interest of the organisation. On top of that remuneration for many senior executives in banking institutions were composed of a high contingent of conditional remuneration or bonuses which unfortunately was a strong motivation to influence the nature of risk taking which occurred in many banking institutions. The addiction to wealth generation through the achievement of short term targets encouraged banks to design ever more complex financial products and seek higher returns by making riskier investments and indeed a rather cavalier approach regarding risk management in general. In many instances the basic principles of good governance being accountability, transparency, objectivity, and putting the organisation's long term interests ahead of all other considerations, were also ignored.

Banking culture now needs to get back on track and start putting the organisation's long term interests ahead of all other considerations. This begins by re-focusing on long term sustainability and resisting pressure to increase profits in the short term, with a view to delivering shareholder value over the longer term in the best interests of the organisation and its shareholders.

[14] A number of proposals have already been put forward in other reports in relation to possible changes in reporting lines which would have an impact on the composition of the Board and with a view to acting as an effective counterbalance to the Executive Management. In many organisations the Chief Risk Officer (CRO) and the Chief Audit Executive (CAE) currently report directly to an executive director or to the CEO. There have been calls to replace these indirect reporting lines to the Board with a direct reporting line to the Chairman. Other suggestions have included having an individual director being solely responsible for the management of risk and/or assurance at the main board level. Some have suggested that this oversight responsibility should rest with an independent director with the CRO and/or the CAE having reporting lines in to this new position. The concept of a full-time NED with responsibility for this oversight has also been put forward. In the US the Schumer Bill requires that all publicly listed issuers establish a risk committee, comprised entirely of independent directors, which shall be responsible for the establishment and evaluation of the risk management practices of the issuer. The common theme here being the suggestion that by independently reporting and providing feedback to the Board on the organisation's environment and activities from a risk perspective, the Board is provided with a more balanced view and it is therefore in a position to make more informed decisions.

Recommendations

2.1 The Director of Corporate Defence should be a full board appointment.

The position of Director of Corporate Defence should be appointed by the Board and the approval of any associated charter should also require full board approval. This would help to re-balance the Board focus and would also send out a strong message in relation to developing a more balanced corporate culture. The position also provides an additional level of support to the Board[15], by providing an extra layer of assurance. This would enable the Board to broaden its own oversight responsibilities. It would also help the Board members in the discharge of their corporate governance duties by helping them to constructively challenge business proposals in a more mature manner.

2.2 The Director of Corporate Defence should report directly to the Board.

Ideally the position itself should be a full board position (similar to the senior cabinet position occupied by the Minister of Defence) reporting directly to the Board independently of CEO and the Executive. This appointment should be allocated a separate budget which is set by the Board and remuneration structures should be based on the achievement of the long term best interests of the organisation. The Director of Corporate Defence should have direct access to the Board and its members at all times and should also be expected to attend all board meetings (and relevant sub-committees of the board i.e. Audit and Risk committees etc) in order to fully brief the Board.

2.3 The focus of the Director of Corporate Defence should be on helping the institution to deliver sustainable value in the long term.

The role should be seen as that of a guardian, representing the required counterweight to the focus on short term objectives, particularly if these short term aspirations could jeopardise the long term sustainability of the organisation. The role would be responsible for helping to ensure that the organisation exercises the appropriate degree of caution in all of its activities and this requires a strong voice with a clear mandate. Being in a position to offer alternative perspectives helps ensure that there is an equality of focus between achieving the upside and avoiding the downside. This means that the role must also act as a business enabler where possible to help enable the achievement of short, medium and long term business objectives.

[15] Recommendations made elsewhere that in the future NEDs will need to improve their skills competence and make greater use of advisors employed in an independent advisory fashion would be supplemented by the creation of the position of Director of Corporate Defence.

3. Requirement to Align Business Generation and Operational Activities

Constructive Challenge Not Conflict

Re-balancing corporate culture should be about embracing integrity and ethical values which means doing the "right thing". This may require a sacrifice of short term gains in order to enhance long term sustainable value. It has been suggested that there is now a need to create a culture of challenge throughout the enterprise but that this must be done without creating a culture of conflict. Obviously a balance needs to be struck between creating a credible deterrence and an environment in which people can still do business. It is important to bear in mind that the objective of the front office business generation side of an organisation is primarily to increase revenue, earnings and profit, subject to various risk constraints. It is therefore important to recognise that the goal is not to eliminate risk but rather to assist the organisation in judging whether prospective returns warrant assuming the risks involved. It also needs to be recognised that some risks are necessary for a business to survive and prosper.

Minimise Time-lags

The middle and back office operational sides of the business should be viewed as the process of assuring that risk versus return decisions are made on a well informed basis with as much insight as possible into possible adverse events. By their nature, operational activities must always react to innovations on the business generation side of an organisation, and this can create an inevitable lag in the ability of the organisation to implement a proposed change (product or service etc) in a manner which does not expose the organisation to excessive risk. The organisation therefore faces the dual challenge of being able to take full advantage of identified business opportunities in a timely manner, and also being able to manage this business in an appropriate manner. This dual challenge can be best addressed by aligning the business generation and operational activities so that the organisation can minimise the time-lag caused by these two complimentary yet antagonistic objectives.

Alignment with Business Strategy

In order to help achieve these objectives in an optimal manner all operational activities must therefore be in alignment with business strategy and objectives. This also applies to all defensive activities and means that these traditionally cautious and reactive activities must adopt more of a business focus going forward. This means that a change in mindset must also occur in the middle and back office, but it is important that the previous mindset of kowtowing to business requirements at all costs does not get replaced with an inflexible mindset which prevents business from being done. Here again a balance is required and this balance involves an appreciation by the business generation side of the importance of transacting business in a manner which does not expose the organisation to an unacceptable level of risk, and appreciation on the operational side that short term workarounds may be required from time to time in order to

facilitate the business. To get the required balance there needs to be an appreciation that these activities represent two sides of the same coin and in order to prosper both must be operating effectively.

Recommendations

3.1 The Director of Corporate Defence should help in the alignment of the business generation and operational activities.

Defence related activities are a core element of middle and back office processes. The objective of the Director of Corporate Defence is to help ensure that the critical components become embedded throughout the enterprise, at strategic, tactical, and operational levels. This means helping ensure these components are present in front, middle, and back office practices. To do this these components need to be adequately embedded in the mechanisms which facilitate these practices including its people, processes, and systems. It means not only embedding these components into the processes and systems, but also of equal importance is being present in the mindset of the individuals involved in these activities so that they become part of the organisation's DNA.

The challenge for the Director of Corporate Defence through education, training and communication is to help to embed all of these activities across the institution, including pushing responsibility for these activities closer to the point of risk origination such as its front office processes. By creating the required level of appreciation and awareness in the front office, the organisation is creating a solid first line of defence which can relieve the pressure on the other lines of defence by being more selective in the business they choose to transact. Defence related activities however must also adopt a mindset whereby they are viewed as a business enabler rather than a disabler. This can be done by ensuring that they are proactively trying to identify solutions to the challenges presented, rather than simply objecting if new proposals are not a good fit with existing processes. The overall objective is to assist the organisation in conducting business which will generate sufficient revenues in a prudent manner, resulting in an acceptable level of risk. The Director of Corporate Defence will have a very important role to play in helping the organisation to achieve the required balance, particularly in relation to the development of new products and services. [16]

[16] The input of the office of the Director of Corporate Defence should be a requirement in relation to the proposed development of new products and services, or where changes are proposed to existing products and services. The extent of the required input may vary on a case by case basis.

4. Requirement to Adequately Defend the Diverse Interests of the Stakeholders

Impact on Stakeholders

One of the lessons to be learned from the current crisis is that the activities of the banking system have had a negative impact on a very wide spectrum of stakeholders and this impact has been felt through all levels of society. Stakeholders in this context refer to all those parties with a vested interest in the success of the sector, including the shareholders, clients, business partners and employees. In the banking context however stakeholders also refer to the financial regulators and the general public. In this instance banking institutions had a corporate duty (including corporate social responsibility) to act in an appropriate manner, so that their actions did not have an unnecessary adverse impact on their stakeholders and their subsequent failure to do the right thing has seriously damaged the reputation of the industry. This has resulted in a great deal of stakeholder anger and a strong sense of grievance and injustice has been directed towards the banking sector.

Stakeholder Focus

Going forward stakeholders need to be considered valued partners both within and outside these institutions and there also needs to be a comprehensible appreciation that the interests of the multiple stakeholders can vary substantially. In terms of shareholders interests there has to be an economic and monetary focus, but it is also important to recognise that other stakeholder concerns may not always be centred around bottom line financials, as these concerns don't necessarily resonate with all of the stakeholders. As individuals, stakeholders are human beings with human needs and human expectations which means they are also concerned with their health and safety, and their welfare and wellbeing. In order to safeguard and adequately defend these diverse interests, all relevant stakeholders must be clearly identified and their interest thoroughly assessed. The successful development of a framework to defend these stakeholder interests will require the input and participation of the relevant stakeholders where all the participants are consulted in relation to their expectations and their required contribution. It also requires a shared recognition that all of the members have an important role to play. Through teamwork all participants can work towards a common good which will be of benefit to all, and can help foster a sense of unity, trust and mutual respect. Perhaps in the process the reputation of the banking sector can be rebuilt.

Joint Responsibilities

Everyone in an organisation is to some extent accountable for defending the interests of the stakeholders. The CEO should assume ownership while executive management should support the organisation's ethics and integrity programs. Operational line management are responsible for managing day to day issues within their spheres of responsibility in accordance with established protocols and consistent with the values of organisation. Defence related functions in particular are obliged to address essential requirements deemed necessary to safeguard the

interests of the stakeholders of these institutions. The Board should provide an important oversight of these duties, and approve and support the organisation's ethics and integrity programs. A number of external parties often provide information useful in effecting these duties, but they are not a part of the organisation's own governance structure. The Board should ultimately remain accountable to the stakeholders for the quality of their governance structure.

Recommendations

4.1 The Director of Corporate Defence should be entrusted with helping to safeguard the interests of all the stakeholders of the institution.

Defence related functions have key support responsibilities in relation to the fulfilment of corporate responsibilities. The Director of Corporate Defence being responsible for the oversight of all defence related functions therefore is in a unique position to help ensure that the diverse interests of the multiple stakeholders are adequately defended. The presence of such a role not only provides the Board with an extra line of defence but it is also in a position to provide additional assurance to the regulators.[17] The role should also provide additional comfort to the other stakeholders of the organisation, by helping to ensure that their interests are being considered and that appropriate steps are being taken to help ensure that they are adequately defended. The presence of this new position (effectively acting as the guardian of the stakeholders) could also help to restore much of the stakeholder trust which has been lost as a result of the banking crisis.

[17] To some extent the Director of Corporate Defence could be equated to an internal regulator with responsibility for ensuring that the organisation's activities are in line with both voluntary and mandatory requirements.

F. APPENDICES

Appendix I

The Critical Components of an Organisation's Program for Self Defence

Governance
Management of the governance component is required to help ensure there is a system in place to address how the organisation is directed and controlled, all the way from the boardroom to the factory floor. It involves specifying the distribution of rights and responsibilities among different stakeholders and spelling out the rules and procedures for decision making. It involves multidimensional layers, both vertical and horizontal, which reflect the measures and mechanisms in place throughout the organisation for setting and achieving organisation objectives and the means for monitoring performance. This component not only impacts on all of the other defensive components at strategic, tactical and operational levels but its impact is felt throughout the entire enterprise.

Risk
Management of the risk component is required in order to systemically address how the organisation identifies, measures and manages the risks it is exposed to, whereby risk is understood as the uncertainty or possibility that an event will occur which can have an adverse impact on the achievement of the organisation's objectives. Risk management is therefore concerned with addressing the relationship between potential risks and their related potential rewards while ensuring that risk exposures are in line with the organisation's risk appetite. While inherent risk can perhaps be established in isolation, an organisation's residual risk can only be satisfactorily determined after considering the organisation's capabilities in relation to the other critical components.

Compliance
Management of the compliance component is required in order to help ensure the organisation's activities are in conformance with all relevant mandatory and voluntary requirements. It involves clearly defining applicable laws, regulations, codes, best practices and internal standards etc, and how the organisation can demonstrate how it manages to ensure that it is in strict adherence with all relevant requirements. The management of the compliance component is both impacted by, or impacts on, all of the other critical components.

Intelligence
Management of the intelligence component is required in order to help ensure that the organisation gets the right information, to the right person, in the right place, at the right time. It relates to mechanisms, processes and systems in operation as an organisation identifies, gathers, interprets, and communicates the information and knowledge available within (and outside) the organisation in order to be in the best possible position to make the timely and informed decisions which are necessary for the achievement of its objectives. It refers to both the larger organisation's capacity to create and use intelligence and the aggregate intelligence capacity of its stakeholders. The intelligence component is therefore a critical element in the management of all the other components.

Security
Management of the security component is required in order to help ensure that the organisation has the ability to protect their assets (i.e. people, information, technology and facilities) from threats or danger. This involves the ongoing management of both physical and logical security issues in order to secure the assets of the organisation. It requires the deterrence, prevention, or pre-emption of threats facing the organisation and mitigating these threats or minimizing any possible vulnerability that might exist. Assessing security requirements and planning for appropriate levels of asset protection involves consideration of each of the other critical components. Management of the security component is both impacted by, or impacts on, all of the other critical components.

Resilience
Management of the resilience component is required in order to help ensure that the organisation has the ability to withstand, rebound or recover from the direct and indirect consequences of a shock, disturbance or disruption. It is about focusing on its ability to sustain the impact of an emergency or interruption, and its capacity to recover from a disaster scenario, in order to resume its operations and continue to provide services with a minimum impact on performance and productivity. Organisational resilience relates to sustainability and involves adapting to the constantly changing business environment. It represents an organisation’s ability to keep its business critical processes, services and assets up and running in the face of adversity. The resilience component is also both impacted by, or impacts on, the management of all of the other critical components.

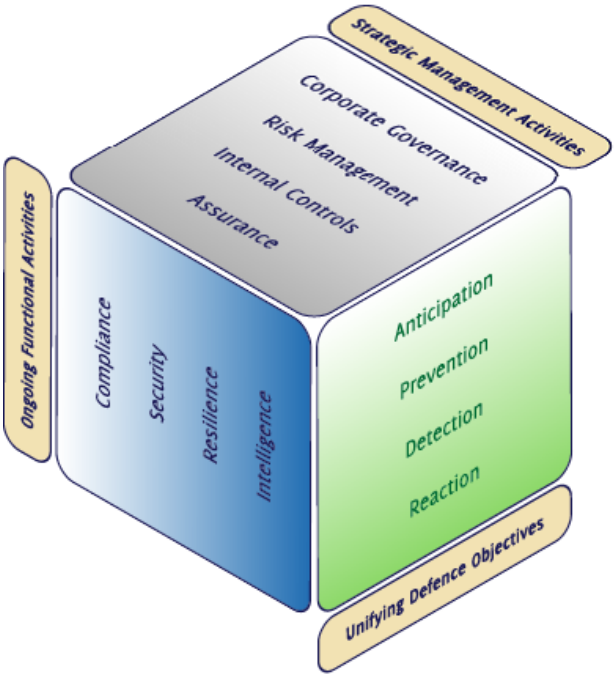
Controls
Management of the controls component is required in order to help ensure that appropriate actions are taken by the organisation in order to address risk and in the process help ensure that the organisation’s objectives and goals will be achieved. These actions include the practices and procedures employed by the organisation in order to provide the board with at least reasonable comfort that the organisation's objectives will be achieved in an effective, efficient and economical manner. The controls themselves may be either preventative or detective and can be either manual or automated. The terms control culture or control environment refer to the continuous operation of controls at all levels within the organisation. The control component therefore has a significant impact on the management of each of the other critical components.

Assurance
Management of the assurance component is required in order to help provide a degree of confidence or level of comfort to the stakeholders of the organisation. It involves the independent expression of a conclusion about the assessment or evaluation of the particular subject matter against specific pre-defined criteria. This requires the performance of an objective examination of evidence, in order to provide an impartial assessment on a particular subject matter. The assurance component includes an evaluation of both the management and the operational performance of all of the other critical components.

Appendix II

Applying the Corporate Defence Management (CDM) Paradigm

In order to integrate all of these necessary elements a 3 dimensional diagram has been conceived which represents this paradigm change, and can help us to conceptualise this integration. Each of these individual activities requires that all of the other elements are also operating effectively and when integrated effectively represent a framework of checks and balances through their continuous cross-referencing of one another.



All of the activities within this paradigm intersect and are intersected by each other. Deliberately no precise boundaries exist in this diagram in order to help avoid the traditional silo type mindset. In the modern era, each of these defence related disciplines needs to be continually cross-referenced against each of the other disciplines.

This paradigm is based on continuing to build on existing structures and frameworks where possible, rather than reinventing yet another new framework for an organisation to implement.

Strategic Management Activities

These represent core strategic management areas which correspond with fundamental frameworks and best practices. These activities are based on the 4 pillars of governance, risk management, controls and assurance, and consist of structural frameworks which need to be in place. These frameworks represent the backbone of corporate defence activities, around which ongoing functional activities operate. Examples of existing frameworks and best practices in these areas include the OECD[18] principles of corporate governance, the COSO frameworks for ERM[19] and integrated internal controls[20], and

[18] The OECD Principles of Corporate Governance, (2004), The Organisation for Economic Co-operation and Development (OECD)

[19] Enterprise Risk Management – Integrated Framework, (Sept 2004), The Committee of Sponsoring Organisations of the Treadway Commission (COSO)

[20] Internal Control – Integrated Framework, (1992), The Committee of Sponsoring Organisations of the Treadway Commission (COSO)

perhaps the IAASB's[21] international frameworks for assurance engagements.

Ongoing Functional Activities

These represent essential ongoing operational activities which are required to be continuously operating on an ongoing basis throughout the organisation. They intersect and are intersected by strategic management activities. The core activities include compliance, security, resilience and intelligence. There are also a variety of possible frameworks available in these areas.

Unifying Defence Objectives

The unifying defence objectives represent the cornerstones of corporate defence, and address the key drivers which need to be present in all defence related activities. Anticipation represents the timely identification and assessment of existing threats and vulnerabilities, and the prediction of future threats and vulnerabilities. Prevention represents taking sufficient measures to shield the organisation against anticipated threats and vulnerabilities. Detection represents the identification of activity types (exceptions, deviations & anomalies etc) which indicate a breach of corporate defence protocol. And finally reaction represents the timely response to a particular event or series of events, in order to both mitigate the current situation, and to take further corrective action in relation to deficiencies identified, and to prevent these events re-occurring in the future.

This CDM paradigm considers each of these activities as representing an organisation's toolkit, whereby each element is seen as a valuable component in defending an organisation. Individually each of these defence related activities actually have requirements in relation each of the other elements. In any one of these areas governance, risk management, control and assurance structures are required to be in place in order to actively manage strategy and policy. Systems and processes in any of these areas need to address requirements in relation to ongoing compliance, security, resilience and the communication of intelligence. Line management and staff involved in each of these activities need to be constantly focused on anticipating, preventing, detecting and reacting to issues which could have an impact on the organisation's performance, and also to help promote continuous improvement in their area. In truth each one of these individual elements is already required to be an integral part of each one of the other elements in order to operate effectively. What is now becoming quite clear is that there is now a growing recognition of the requirement for cross-functional expertise throughout the enterprise, and it is for this reason that it appears that we are only now beginning to see the forest from the trees in the area of corporate defence.

[21] International Frameworks for Assurance Engagements (2005), The International Auditing and Assurance Standards Board (IAASB)

Appendix III

Examples of an Organisation's Defence Related Activities

Governance

- Culture / Environment / Ethics
- Stakeholder Relations
- Design / Structure
- Strategy / Planning
- Corporate Responsibility
- Accountability
- Framework
- Methodology

Resilience

- Emergency Operations
- Crisis Management
- Disaster Recovery
- Contingency Planning
- Continuity Management
- Incident Response Management
- Health & Safety
- Insurance

Risk

- Enterprise Risk
- Strategic Risk
- Business / Financial Risk
  - *Credit Risk*
  - *Market Risk*
  - *Operational Risk*

Compliance

- Regulatory Compliance
- Legal Compliance
- Workplace Compliance
- Industry Codes
- Best Practice Guidelines
- Internal Standards

Controls

- Internal Controls
- Financial Controls
- Operational / Processing Controls
- Supervisory Controls
- Compliance Controls
- Security Controls
- Preventative / Detective Controls
- Primary / Compensating controls

Intelligence

- Business Intelligence (B.I.)
  - *Operational Intelligence*
  - *Market / Competitive Intelligence*
- Knowledge Management
  - *Content Management*
  - *Record Management*
  - *Document Management*
  - *Filing / Storage / Archiving Management*
- Communication

Assurance

- Inspection Review
- Internal / External Audit
- Regulator Review
- Rating Agency Review
- Standards Certification
- Self Assessment Review
- Due Diligence Review
- Fraud Examination
- Forensic Investigation
- Litigation Support
- Asset Recovery

Security

- Physical Security
  - *Premises Security*
  - *People Security*
  - *Information Security*
  - *Facility Security*
  - *Operations Security*
- Logical (I.T.) Security
  - *Client Security*
  - *Application Security*
  - *Operating System Security*
  - *Database Security*
  - *Network Security*
  - *Gateway Security*

Appendix IV

Author's Bio Details

Sean Lyons is an active pioneer within the contemporary corporate defence movement, being a firm advocate of the requirement for corporate defence to play a more eminent role in corporate strategy. His work is focused on the development of corporate defence programs, whereby corporate defence is used as an umbrella term representing all of those activities which are aimed at defending the organisation from risks, threats, dangers and hazards etc. Sean's vision is that corporate defence programs will address all of the activities which constitute an organisation's program for self-defence. Corporate defence therefore is seen to represent the management of these critical components which include governance, risk, compliance, intelligence, security, resilience, controls and assurance etc. Sean recently published a Q&A series entitled "Corporate Defense Insights: Dispatches from the Front Line", which featured expert commentators from around the globe addressing these individual components from a corporate defence perspective.

Sean is also the architect of the related cross-functional discipline of "Corporate Defence Management (CDM)" which aims at helping organisations to ensure that these multidimensional components are managed in a coordinated and coherent manner so that they are in strategically aligned, tactically integrated, and operating in unison towards common objectives.

Sean has had a number of papers published internationally on CDM and other corporate defence related topics. His work has been published by such publishers as Corporate Governance Quarterly (CGQ), the RiskCenter, the Bank Director, the Corporate Board Member, the Journal of Operational Risk, the Business Continuity Journal, StrategicRISK, Information Management (formerly the DM Review), GTNews, and by organisations such as the Global Association of Risk Professionals (GARP), the Risk and Insurance Management Society (RIMS), the Risk Management Association (RMA), the Open Compliance & Ethics Group (OCEG) and the Society of Actuaries (SOA).

Sean has lectured and spoken on these topics at seminars and conferences relating to corporate defence, CDM, ERM, GRC and business resilience, in both Europe and North America, including Canada, the United States, the United Kingdom, the Netherlands and Portugal. He has amassed two decades of experience in the banking and financial services industry, working as an Operational Trouble-shooter, Internal Auditor and Management Consultant. He has previously worked with, held senior management positions with, and/or been a professional advisor to, a number of leading financial organisations in the Republic of Ireland, United Kingdom and Australia. Employers and clients have included HBOS, KBC, INVESCO, CIGNA and Saudi International Bank.

Selected publications are available for download at: http://ssrn.com/author=904765

Publications - Q&A Series

Corporate Defense Insights: Dispatches from the Front Line

- *Continuity Central – www.continuitycentral.com – Operational Risk – 20th March 2009*
- *The RiskCenter – www.riskcenter.com – Top Story – 6th April 2009*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / 6th April 2009*

Individual Interviews

Summary Review
Sean Lyons, Q&A Series Editor & Producer
- *The RiskCenter – www.riskcenter.com – Top Story –13th January 2009*

Assurance
Michael J.A. Parkinson, Director on the Board of the Institute of Internal Audit (IIA) Global
- *The RiskCenter – www.riskcenter.com – Headlines News – 30th December 2008*

Governance
Richard M. Steinberg, CEO of Steinberg Governance Advisors
- *The RiskCenter – www.riskcenter.com – Top Story – 22nd December 2008*

Resilience
Kathleen Lucey, President of the Business Continuity Institute (BCI) USA Chapter
- *The RiskCenter – www.riskcenter.com – Top Story – 6th November 2008*

Intelligence
Stephen Walker, Technology Markets Analyst, the Aberdeen Group
- *The RiskCenter – www.riskcenter.com – Top Story – 22nd October 2008*

Governance, Risk & Compliance (GRC)
Scott Mitchell, Chairman & CEO of the Open Compliance and Ethics Group (OCEG)
- *The RiskCenter – www.riskcenter.com – Top Story – 12th August 2008*

Enterprise Risk Management (ERM)
Stephen Dreyer, Managing Director at Standards & Poor's (S&P)
- *The RiskCenter – www.riskcenter.com – Top Story – 5th August 2008*

Internal Controls
Jim Kaplan, Author, CEO and Founder of AuditNet®
- *The RiskCenter – www.riskcenter.com – Headline News – 23rd July 2008*

Compliance
Roy Snell, CEO of the Society of Corporate Compliance & Ethics (SCCE)
- *The RiskCenter – www.riskcenter.com – Top Story – 16th July 2008*

Risk Managment
Dr. David Rowe, Director of the Professional Risk Managers International Association (PRMIA)
- *The RiskCenter – www.riskcenter.com – Headline News – 8th July 2008*

Information Technology (IT)
Lynn Lawton, Global President of the Information Systems Audit and Control Association (ISACA)
- *The RiskCenter – www.riskcenter.com – Top Story – 3rd July 2008*

Security
Prof. Stephen Northcutt, President of the SANS Technology Institute
- *The RiskCenter – www.riskcenter.com – Headline News – 25th June 2008*

Operational Risk
Philip Martin, Chairman of the Institute of Operational Risk (IOR)
- *The RiskCenter – www.riskcenter.com – Top Story – 18th June 2008*

Publications - Papers

The Changing Face of Corporate Defence in the 21st Century
- *StrategicRISK – www.strategicrisk.co.uk / features – May 2008*
- *Corporate Governance Quarterly (CGQ) (Spring 2009)*

Risk Management's Role in Corporate Defense
- *ERM Symposium 2008 – www.ermsymposium.org / callforpapers – 14th April 2008*
- *Society of Actuaries (SOA) – www.soa.org /…monographs...ERM Symposium 2008 – 2nd March 2009*

Corporate Defence: Risk Management, Business Resilience and Beyond
- *The Business Continuity Journal, Vol. Two, Issue Four, January 2008*
- *Continuity Central – www.continuitycentral.com – Advanced Resources – 3rd October 2008*

The Corporate Defence Continuum
Part (1): Governance, Risk and Compliance (GRC)
- *The RiskCenter – www.riskcenter.com – Headline News - 23rd January 2007*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk -23rd January 2007*
- *Open Compliance and Ethics Group (OCEG) – www.oceg.org / Resources – December 2007*

Part (2): Intelligence, Security and Resilience
- *The RiskCenter – www.riskcenter.com – Top Story – 29th January 2007*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk - 29th January 2007*

Part (3): Controls and Assurance
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk – 5th February 2007*
- *The RiskCenter – www.riskcenter.com – Headline News – 6th February 2007*

Part (4): The Quest for a Holistic Solution
- *The RiskCenter – www.riskcenter.com – Top Story – 13th February 2007*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk - 13th February 2007*

An Introduction To Corporate Defence Management (CDM)
- *DM Review – www.dmreview.com / Newsletters / DM Direct - 15th December 2006*

Challenges Facing Contemporary Corporate Defense
- *The RiskCenter – www.riskcenter.com – Headline News - 12th December 2006*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk - 12th December 2006*

An Executive Guide To Corporate Defence Management (CDM) - Whitepaper
- *The RiskCenter – www.riskcenter.com / Homepage / Global Reports – 16th November 2006*
- *The Bank Director – www.bankdirector.com / Resource Centre / Strategy & Risk Management – 15th Dec 2006*
- *The Corporate Board Member – www.boardmember.com / Resource Center / Risk Management - 18th Dec 2006*
- *GTNews – www.gtnews.com / Whitepapers – 6th March 2007*
- *GRC USA – www.grc-usa.com / Whitepapers – 4th April 2007*
- *Open Compliance and Ethics Group (OCEG) – www.oceg.org / Resources – December 2007*

Corporate Defence Management: A Strategic Imperative
- *The Bank Director – www.bankdirector.com / Resource Centre / Strategy - 16th October 2006*
- *The RiskCenter – www.riskcenter.com – Top Story - 15th November 2006*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk – 15th November 2006*
- *Risk and Insurance Management Society Inc.(RIMS) – www.rims.org / Risk Wire - 20th November 2006*
- *Risk Management Association (RMA) – www.rmahq.org / Risk News at-a-glance - Week of November 27th 2006*
- *Open Compliance and Ethics Group (OCEG) – www.oceg.org / Resources – December 2007*

Corporate Defence: Are Stakeholders Interests Adequately Defended?
- *The Journal of Operational Risk, Vol. 1, No. 2 Summer 2006*
- *The RiskCenter – www.riskcenter.com – Top Story -14th November 2006*
- *Global Association of Risk Professionals (GARP) – www.garp.com / Risk News / Op. Risk - 14th November 2006*
- *Risk and Insurance Management Society Inc.(RIMS) - www.rims.org / Products & Services*
- *Open Compliance and Ethics Group (OCEG) – www.oceg.org / Resources – December 2007*