Richard Anderson & Associates
Independent Governance Risk & Assurance

The Thatched House, Bisham Road, Marlow, Bucks, SL7 1RL
e-mail: rc.anderson@tiscali.co.uk
Telephone: 07703 503196

Chris Hodge
Corporate Governance Unit
Financial Reporting Council
Fifth Floor
Aldwych House
71-91 Aldwych
London WC2B 4HN

9 October 2009

Dear Chris

Review of the Combined Code

I set out below my views on certain aspects of the Combined Code. I have also written separately to Sir David Walker, and I copied you in by e-mail to that letter. You have also seen my report to the OECD[1], which I forwarded to you earlier in the year.

No-one, unless they are a banker hoping for a bonus this year, can possibly forget that we have been witness to the most wide ranging set of failures in Corporate Governance in modern times. After all, many of us either are suffering, or know people who are suffering from what have been atrocious economic conditions far away from the banking sector. This was the set of failures which was never supposed to happen, especially in the UK. As far back as 2001, just post-Enron, commentators said "it" could not happen in the UK because of our approach to principle-based comply-or-explain Corporate Governance. But the financial crisis did happen, and it happened big. Until recently, virtually no-one was denying that better corporate governance was now required, with at least the implication that better corporate governance could, might, should have mitigated the worst affects of the financial crisis. The self-serving complacency of many commentators post-Enron, some of whom served on boards or as advisors to boards at the time did not serve the rest of us well this time round. As a consequence, right now it has to be odds-on that we will find ourselves in a similar situation within the next ten years as incumbent directors and boards argue against more stringent rules. We are at a tipping point and we risk seeing the best chance of change for decades slipping away from us. That is truly scary.

The feedback that we have seen in public to Sir David Walker and your own review suggests that directors, and chairmen in particular, have a strong antipathy towards tightening the Combined Code. Their views seem to hold the greatest sway. And so, there is a severe risk of everyone settling back down to their previous norms with a few tweaks at the edges. Yet, these are norms that should

[1] **Corporate Risk Management: A review of the link between risk management strategies and remuneration policies, and the role of the board of directors in establishing and monitoring risk management strategies and remuneration policies.** See http://randerson-assocs.co.uk/oecd.aspx.

have been severely discredited by the failures in the banking sector, both here and abroad. Given that taxpayers have bailed out the financial services industry and will go on doing so for many years in higher fees, lower returns and more penal interest rates, all because of the need for tighter capital rules, society is surely entitled to see a paradigm shift in attitudes to Corporate Governance in Banks and Other Financial Institutions ("BOFI"s) (and other large corporates in other sectors) which have a societal impact. There simply will be no change in boardrooms in the UK or abroad, unless there is a re-framing of the importance of Corporate Governance so that it is seen as being relevant to the wider public, rather than simply to the Chairmen and Board Members of listed companies. It is for this reason that there should be a review of the legal duties and responsibilities of directors (at least of BOFIs and other societally important organisations) with a view to requiring them to discharge their Corporate Governance responsibilities with due and diligent care. This would require a change in the existing law because the level of challenge available under current directors' duties is set at such a low level by English case law. As a consequence directors can currently act almost with impunity: the only real challenge that any directors have seen in the UK has been either from the media or to a small extent from the Treasury Committee. This proposed new duty should be set in law at a considerably higher level so that it has the potential to bite. It is only with that in mind that we will see the required cultural shift in boardrooms. This is not a trivial change suggested as a matter of revenge: unless and until there is a potential penalty for failing to comply with such a duty, we will see no more than lip-service paid to Corporate Governance compliance.

This recommendation is not going to win the popularity stakes with Chairmen and Directors of listed companies, many of whom believe that Corporate Governance is already overly intrusive. It is not meant to be popular: it is meant to drive a fundamental change in behaviours and attitudes so that directors take their Corporate Governance fiduciary duties seriously and individuals in society can see that happening.

Risk Oversight Committees

Despite the concerns expressed above, there is one small window of opportunity that could be seized on to drive through fundamental change. That opportunity is the creation of Board Risk Committees, or as the SEC might have it: Risk Oversight Committees. This might just be the basis upon which change is created.

At the moment, too little emphasis has been placed on the importance of developing a comprehensive approach and structure to risk management and the requirement for ROCs or BRCs to oversee the output from that. There needs to be much more clarity as to the role, remit and mechanisms of these committees. The remit and mechanics need to:

- Encompass the development of a balanced view of risk;
- Include the oversight of the development and implementation of a robust ethics programme;
- Encompass the periodic assessment of the maturity of risk management maturity;
- Include the development of a risk management and assurance framework that is fit for purpose; and
- Address the development of an appropriate risk management organisation

These are each considered in more detail below.

I Balanced Risk

The failure of the financial system is often explained in terms of sub-prime mortgages, CDO's and a resulting liquidity crisis. But these are just the symptoms that happened to be around because of a much more fundamental malaise. That malaise can best be described as a fundamental breakdown of two critical balancing acts in the boardroom:

- Firstly, the balance between risk taking and risk avoidance: clearly BOFIs, and indeed all other organisations, have to continue taking more managed risk if they are to prosper and grow. Equally they need to avoid those risks that can harm their value, however that value is measured. On the other hand they do not want to do too much or too little of either of these things: the problems from too much risk taking (however well an organisation attempts to manage it) are now well documented. The problem of too much risk avoidance is that nobody in the organisation is prepared to take any risk in the pursuit of growth because of the potential pitfalls, and this will lead to corporate stagnation.
- The second balance is that between the performance culture and corporate ethics. The problems associated with too demanding a performance culture where almost unlimited sums of money appear to be available are now obvious (even if they were not obvious before...) Equally there are potential problems associated with too high a level of corporate ethics in that people become obsessed and begin to suffer from an "egg shell syndrome" where they feel obliged to consult every tangential stakeholder before making a decision, with the consequence that decisions are never made.

It is the board's responsibility to manage these two balancing acts, and in many BOFIs the boards manifestly failed to do so in the run up to the financial crisis. This approach to "Balanced Risk" should replace rather arcane and dry debates about risk appetite. As we stand at the moment, risk appetite is almost impossible to measure and can never sensibly be expressed (except for a limited number of risks that are subject to quantitative techniques – and even they have their now well-known limitations) until the four dimensions of Balanced Risk are taken into account. The suggestion that risk appetite is an elusive concept is anathema to many risk practitioners and risk consultants. However, there is no adequate approach to risk appetite that fits comfortably within a risk management framework.

Members of ROCs will need to familiarise themselves with their organisation's positioning on the Balanced Risk equation, and identify whether they are like Enron (very high risk taking, very high performance culture, very low corporate ethics, very low risk avoidance), or whether they have got the balance right.

II Robust ethics programmes

Balanced risk implies the need for appropriate corporate ethics. Yet there is a strong sense that ethics and an ethical view of life have become something of a luxury that did not fit with the pursuit of profit or indeed the pursuit of the end of year bonus. Mortgage salesmen were adopting unethical approaches to selling mortgages in the sub-prime market, there were questionable ethics in the way that traders developed products that obfuscated the level of risk and investors were pushing for higher profits at any cost. Had anyone had the ethical courage to call a halt at a much earlier stage, then many of the problems could well have been avoided.

Ethics programmes can become bureaucratic nightmares with little more than lip-service being paid to them. It is incumbent on the board, and particularly to a ROC, to ensure that they are truly embedded into the organisation. This will have a double benefit: it will help on the way towards restoring trust in the fallen institutions over the long term (and it will be very long term before trust is restored) and it will also encourage BOFIs and others to listen to the weak signals of emerging risks that could have been picked up much earlier had there been appropriate mechanisms before the financial crisis. Weak signals were not picked up in thick skinned banks: they needed a taser to stun them into an action, rather than the comparatively weak signals that might alert a more sensitive organisation to impending problems.

The ROC has a major role to play in setting the ethics policy, in conjunction with the board as a whole, and then in reviewing the implementation and subsequent assurance that it does indeed function as required.

III Mature risk management

We may never now know how many of the banks that failed had a mature approach to enterprise risk management: it is too late to measure the maturity without the colouring of hindsight. However, in light of what little is known, it is now incumbent on ROCs to establish a view as to the level of sophistication and maturity that they require for their enterprise risk management approach. They need to be able to hold a mirror up to the organisation so that they can see just how good the mechanisms are, and whether there is any hope that they will act in the ways intended.

Based on work at a large number of organisations, conclusions that can be drawn from reviewing risk maturity are that:

- On the whole non executive directors decline to talk about the risk maturity of their organisations – they often claim not to know;
- Executive directors tend to believe that they have got it just about right;
- Risk experts, including CRO's and heads of audit tend to be critical of the smoke and mirrors that they use in reporting to the board; and
- Just about everyone else could not care less.

This simply is not good enough. Risk oversight committees should examine:

- Maturity of attitudes to risk management, governance and compliance;
- Maturity of risk processes;
- Extent to which their organisation is prone to disasters – there are well recognised warning signs;
- Maturity of their organisational corporate ethics and behaviours; and
- How staff would behave under pressure and equally how the organisation as a whole would cope with severe difficult operating conditions.

Many BOFIs would have found themselves wanting had they conducted reviews of all of these elements of risk management maturity throughout their organisations prior to the financial crisis.

IV Risk management and assurance framework

A robust risk management and assurance framework will facilitate the discharge of a board's Corporate Governance fiduciary duties. It will also serve to underpin sustainable performance within an organisation.

The absence of any reference to internal audit or any other form of internal assurance in the Walker consultation paper is an unfortunate omission. It leaves the impression that internal audit is unimportant. To the contrary: internal audit is an important (probably indispensable) element of the risk management and assurance framework that any BOFI should have in place, and which needs to be overseen by the ROC. There is a perception in some quarters that internal auditors are not providing the degree of comfort that some boards and in particular Chairs of Audit Committees might like, but that does not mean that the function is irrelevant. If internal audit is perceived not to be working, then the shortcomings need to be rectified by the creation of a strong and purposeful function that will demonstrate its importance to the board.

Having a mature approach to balanced risk, supported by an effective ethics programme are the key foundations to ensuring that what the board thinks is happening is in fact taking place, in other words "assurance". It is essential that the board should be able to derive appropriate assurance about its activities, and this should be supported by an actively managed assurance programme. The development of robust Assurance Maps to supplement the risk registers and other risk management activities will help to ensure that the right messages are being given in a consistent and coherent manner to a wide range of stakeholders who require assurance on a diverse range of matters.

V Risk organisation

Many commentators have argued that the organisation of risk departments, their staffing and reporting lines were inadequate in the run up to the financial crisis. The ROC might well contemplate the creation of a board level Director of Risk Management and Assurance. Representation at the top table will in itself send an important message to the entire organisation and its stakeholders: a message that the fiduciary duties that go with corporate governance are at least as important as the fiduciary duties associated with financial reporting. However, in itself that representation is not sufficient. For risk management to work properly requires five other attributes:

- **Chief Executive and Non-Executive Director sponsorship**: there has to be absolute clarity that there is total buy-in to the remit, function and conclusions derived from risk management and the assurance function, otherwise the risk management and assurance framework will never be taken seriously by line managers.
- **Enterprise-wide buy-in**: the board sponsorship needs to translate into proper policies, procedures and reporting that ensure that the full organisation swings behind the risk management and assurance framework.
- **Robust risk management processes**: it almost goes without saying that the organisation will need to ensure that there are appropriate processes that will achieve the risk management objectives and fulfil reporting requirements. However, that is not necessarily the case in many organisations, including BOFIs as of today.
- **Appropriate informational support**: all of this is going to require appropriate investment in IT support and infrastructure.

- **Constant consciousness of Risk Management and Assurance performance**: members of the risk oversight committee will need to ensure that they maintain a keen overview of the risk management and assurance processes so that they do not deteriorate over time.

In following the five themes set out above, ROCs will enable BOFIs (and others) to develop as risk intelligent organisations (for a definition of a risk intelligent organisation see the box below). This will enable risk management to fulfil one of its key objectives, which should be to pierce the "perfect place arrogance" so often demonstrated in large, sophisticated, global organisations. In fostering that spirit, risk oversight committees would be discharging a role that is of vital importance to society at large.

A Risk Intelligent Organisation

Risk management is about bringing a **perspective** to the management of **complicated issues** in **complex organisations**. It is about the **management** (and not the **avoidance**) of risk. It helps to **prioritise** your work and that of others in a **fast moving context** with an **approach** that is **better than simple intuition** and which **facilitates communication** between **people**. It is a **style of thought**, and is definitely **not a paper chase**.

Conclusion

This letter has only skimmed the surface of some of the issues that have been raised, but hopefully it will contribute to an emerging discussion about the remit and mechanics of risk oversight committees which have to be relevant to any organisation that has a high societal impact. However, these issues are fundamental to rebalancing boards away from pure performance and unfettered risk taking to a more balanced and long term approach to sustainable (as opposed to volatile) value creation. Without fundamental change to our system of Corporate Governance we run the risk of falling back into what are now discredited approaches that failed not only the banks but also society at large. With this in mind, I would urge both Sir David Walker and yourselves to push for a radical and challenging Corporate Governance environment, uncomfortable as that might be for incumbent board members.

With kind regards

Yours sincerely

Richard Anderson
Principal, Richard Anderson & Associates