



**ParadigmRisk**<sup>Ltd</sup>

Comment by **Paradigm Risk Limited**

on

## **Response to the Financial Reporting Council**

### **Consultation on the Revised UK Corporate Governance Code**

**Prepared by**  
**Peter Bonisch & Dr Mustafa Cavus**  
Directors

**March 2010**



## Executive summary

In relation to the provisions of the Code on risk management, FRC has introduced material new requirements: that the board define the company's risk appetite and risk tolerance.

In order to define meaningfully a company's risk appetite and risk tolerance, the company must consider its preferred risk holding both quantitatively **and** qualitatively. This is true for both financial sector firms and non-financial sector companies. Ultimately, risk appetite relates to trading off probability of achieving financial targets for expected higher returns which are, necessarily, quantitative issues. The assertion that risk appetite can be considered meaningfully solely qualitatively (or using unquantifiable concepts such as 'risk attitude') is not supported by either theory or practice.

A major difficulty in formulating regulatory policy on risk is the absence of robust empirical analysis of corporate risk practice. While there have been multiple recent examples of opinion-based research, none of which we are aware have attempted to examine failures in corporate risk practice. This matters. Without 'counterfactuals', it is impossible to test or to understand what **does not work**; knowing what does not work is as important or more important than knowing what does.

We advocate a range of amendments to the text of the Code; most notably, to create a separate section relating to management of risk in order to distinguish the **forward-looking** activities of risk management from the **backward-looking** activities of corporate reporting and assurance over internal control. Wherever possible, these related but distinct activities should be separated logically and in the Code text.

We believe the relationship between risk management and internal control is frequently unclear in the Code. These activities are often confused in practice and just as often in theory. Here, we believe additional guidance from FRC to clarify the relationship, or at least the meaning of the terms used in the Code, would be useful.

We believe that prevalent current approaches to corporate risk management and internal control create an "entire pretend reality" of assurance of risk and internal control. We believe this pretend reality is illustrated by findings in a recent survey by Independent Audit in which there are considerable discrepancies between attitudes of non-executive directors and executives on effectiveness of certain aspects of risk practice. Again, without robust empirical analysis, it is not possible to discount real differences between reality and perception in assurance over corporate internal control and risk management.

Based on these concerns, as well as the fundamental nature of consideration of risk appetite, we believe considerable additional guidance will be required to support companies to implement the changes in the Code. Simply revising the guidance will leave firms without a clear understanding of expectations in relation to risk appetite and risk tolerance. This may result in adopting simplistic approaches of limited value to achieve compliance rather than investing in improved capabilities and analysis of risk appetite and tolerance which would yield a longer-term benefit to the firm.

## Commentary

### INTRODUCTION

Given that we have already provided an extensive and substantive submission to the Financial Reporting Council on revising the Combined Code, in this comment we will limit our observations to the issues around the “board’s responsibility for overseeing risk management and setting the company’s risk appetite and tolerance”.

Under the heading “Main principles”, the revised Code states:

#### SECTION C: ACCOUNTABILITY

The board should present a balanced and understandable assessment of the company’s position and prospects.

The board is responsible for defining the company’s risk appetite and tolerance. The board should maintain a sound system of risk management and internal control to safeguard shareholders’ investment and the company’s assets.

The introduction of a new requirement for the board to define the company’s risk appetite and tolerance suggests the FRC believes these two, related ideas – risk appetite and risk tolerance – warrant board-level attention and action. We concur. However, the challenge is to ensure that the Code encourage the best engagement by boards and that it be realistic given observed (or observable) levels of competence and understanding in boardrooms. Given the evidence of confusion among executives and non-executive directors over these concepts, there is considerable scope for unintended consequences to emerge from the very strong requirements stated by the revised Code.

Our comments fall in to the following areas:

- conflation of risk and internal control
- capacity for action
- immaturity of the concept of risk appetite
- terminological problems
- extent of risk knowledge available to boards
- methods and evidence of corporate risk management performance
- the need for additional guidance

## STATEMENTS OF MAIN PRINCIPLES

The statement: “[t]he board should maintain a sound system of risk management and internal control” appears both simple and obvious. However, for the purposes of regulatory drafting, we need to attend closely to the range of potential interpretations of the phrase in practice. Several interpretive issues arise:

- The board cannot and will not, *itself*, **maintain** a sound system of risk management or internal control in the company. These activities are the role of managers; the concomitant role of the board is to review, challenge and ultimately endorse parameters for risk acceptance both ‘at the margin’ and as a portfolio of total risk held by the firm.
- The phraseology conflates risk management with internal control and the phrase could validly be read in both of the following ways:
  - (i) the board should maintain a sound system of [**risk management and internal control**] – one concept, or
  - (ii) the board should maintain a sound system of [**risk management**] and should also maintain a sound system of [**internal control**] – two concepts

Either of these is potentially valid but each has a different meaning and implies a very different relationship between [risk management] and [internal control]. There is, validly, some dispute over the relative hierarchical ordering of these concepts; the issue is not merely semantic.

- The use of the phrase “risk management” itself reduces clarity. Because the phrase is used so often, in so many contexts and with widely varying underlying meanings, interpretation of the phrase is problematic.

Similarly, in the following paragraph of the “Main principles”, the revised Code states

The board should establish formal and transparent arrangements for considering how they should apply the corporate reporting, risk management and internal control principles and for maintaining an appropriate relationship with the company’s auditors.

Again, by conflating “risk management and internal control principles”, the Code, as drafted, is ambiguous in its intended relationship between these concepts. Also, that paragraph of the Code lists the board’s responsibilities as:

- establishing (*sic*) formal and transparent arrangements for considering how they should apply the corporate reporting principles, and
- establishing (*sic*) formal and transparent arrangements for considering how they should apply the risk management and internal control principles and
- establishing (*sic*) formal and transparent arrangements for maintaining an appropriate relationship with the company’s auditors

Here, the Code implies that the four concepts of (i) applying corporate reporting principles, (ii) risk management, (iii) internal control and (iv) maintaining an appropriate relationship with the company's auditors are qualitatively similar and related. Furthermore, because of the tight association of (i), (iii) and (iv) with the external auditors, the statement implies, quite **unjustifiably**, that (ii) 'risk management' is a valid and topic for auditors' attention and, by extension, logically and observably within their skill set. Both these latter implications are highly questionable.

*Distinguishing internal control and risk management*

On the contrary, Sir David Walker, in his report on governance and risk in financial institutions<sup>1</sup>, delineates clearly between backward-looking and forward-looking activities. He states:

In practice, the audit committee has clear responsibility for oversight and reporting to the board on the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other related matters. This vital responsibility is essentially, though not exclusively, backward-looking ...

Sir David contrasts this with . . .

. . . responsibilities for the determination of risk tolerance and risk appetite through the cycle and in the context of future strategy and, of critical importance, the oversight of risk in real-time in the sense of approving and monitoring appropriate limits on exposures and concentrations. This is largely a forward-looking focus.

In the same paragraph, he concludes:

There is an important concentricity between these functions, above all in assurance from internal audit that the processes in place for the management and control of risk are fully adequate to the overall strategy decided by the board . . . But a clear differentiation is needed to in ensuring that appropriate and separate attention is given to backward and forward-looking risk functions.

In its final report on the Review of the Combined Code (December 2009), the FRC refers to the Walker Review, as follows:

- 3.48. In his report Sir David Walker has recommended some specific processes to ensure the boards of banks and other major financial institutions carry out this role effectively, such as the establishment of a board risk committee.
- 3.49. The majority of commentators on the FRC review considered that the same processes were not necessarily appropriate for all non-financial companies. This view was supported by research carried out by Independent Audit for the ICAEW Foundation, which found "clear differences between financial services organisations and corporates, not only in the nature of their business

---

<sup>1</sup> Sir David Walker, (November 2009). A review of corporate governance in UK banks and other financial industry entities: Final recommendations, (London: HM Treasury).

and risk exposure but also in the role that risk management plays in the organisation. These differences mean that the nature of the problem to be addressed by board governance of risk is different”.

In rejecting the need for separate risk committees (Walker’s recommendation 23), the FRC also loses the critical but separate distinction between backward-looking and forward-looking activities. This distinction necessitates that great caution be used assigning board-level (and, for that matter, executive) responsibilities relating to risk.

In support of rejecting broader application of Walker’s recommendation 23, the FRC cites the work of my former colleagues at Independent Audit Limited (IAL). Because of this reference, and the close association between ICAEW Foundation, FRC and its related bodies, the IAL study warrants detailed review.

*The Independent Audit study*

The nature of the research IAL undertook to prepare their study for the ICAEW Foundation was neither objective nor empirically based. By questioning board members and senior corporate officers, their research elicited these peoples’ opinions only. Their research did not seek to test empirically either the validity of the opinions expressed or to gauge the effectiveness in practice of the methods advocated; no ‘counterfactuals’ were sought or reviewed; the methods stated to be effective by those interviewed were accepted to be effective, without systematic evaluation. This approach is common used in reviews of business policy issues in the UK; that does not make it methodologically valid. Rather, it suggests its results must be interpreted with considerable care and caution.

Perhaps the most revealing aspect of the IAL report, and certainly the most germane to the consideration by the FRC of amendments to the Code, are shown in their Table 1, below.

Table 1  
How well...

	Management average score	NED average score	Difference in average scores	Companies where management scored lower	Companies where NEDs scored lower	Companies where NEDs and management scored the same
Is risk management embedded?	2.1	4.2	2.1	23	0	1
Does risk management keep up with change?	2.3	4.1	1.8	24	0	1
Do risks find their way up the organisation?	2.7	3.8	1.1	16	5	4

The report’s authors explain the scores as follows:

We put [the difference in scores between management and NEDs] down to a combination of factors. One is that most things look better from a distance, and NEDs are relatively remote from the

practicalities of most risk management activity. This reinforces the need for NEDs to guard against over-optimism and the ever-present threat of complacency.

The other, offsetting, explanation is that most executives do take risk management very seriously, as we saw in our interviews; they know they could always do more and so are readier to acknowledge that in an ideal world they would spend more.

However, there is another, equally plausible explanation: that the assurance reporting required by the Turnbull Guidance on the internal control provisions of the Code produces a systematic divergence between the confidence of NEDs and executives because of something inherent in and internal to the usually-applied process of preparation, collation and provision of that assurance. It is equally conceivable that the typical ‘Turnbull process’ provides exactly what is envisaged: assurance over the effectiveness of internal control (and related reporting on risk management effectiveness), regardless of the actual effectiveness of the corporate systems over which the assurance is provided. The “entire pretend reality” of assurance<sup>2</sup> may equally explain the divergence in reported scores observed in the IAL study’s data.

If this hypothesis were true, it should have an enormous impact on the FRC’s requirements in relation both to internal control and to the identification and management of risk and comparison of risk held by the firm against some pre-defined appetite and/or tolerance. Unfortunately, there is no current basis for assessment of its validity or invalidity. However contentious, the hypothesis does fit with views of directors and senior officers expressed in other studies and review exercises, as well as with many examples of corporate underperformance and even failure observed empirically where internal control and risk disclosures (as well as internal reporting directly observed) provided little or no anticipation of problems.

The IAL report, on which FRC appears to have relied, also contains several other dubious assertions relating to risk. For example, the IAL report states:

In financial services organisations, risk is usually approached in separate categories such as credit risk and market risk, each being separately used in the calculation of the capital cushion required. Operational risk is one of these separate categories, covering a wide range of risks including those relating to people, process and organisation. It is usually the category which is the most difficult to calculate for capital purposes.

In corporates, risk is not used as the basis for calculations of required capital.

This (rather dubious) descriptive statement highlights several key difficulties. First, operational risk is one of 19 types of risk referred to in regulatory guidance on risk in the financial services firm; it is only Basel Pillar 1 that restricts discussion to the classes referred to by IAL. Secondly, that operational risk is the “most difficult to calculate” reflects both inherent methodological challenges (a state of affairs not unique to operational risk) and the more recent introduction of operational risk measurement to the banking world.

---

<sup>2</sup> The phrase “entire pretend reality” is borrowed from a landmark article by aviation journalist William Langewische: Langewische, (1998). The lessons of ValuJet 592, *Atlantic Monthly*, March.

Thirdly and more importantly, the statement that risk is not used as the basis for calculations of required capital in non-financial businesses is at one level wrong and at another deficient normatively. Risk and its calculation are both essential to any process of valuation of the firm as well as rating the firm from a bond pricing or credit default perspective. Both of these make consideration of risk vital to calculation of the firm's required capital and "signaling capital"<sup>3</sup>. Also, the suggestion ignores the normative point: that greater use of analysis of risk in calculation of capital relative to corporate risk appetite and risk holding would improve, possibly substantially, the validity and utility of risk management in many corporate businesses.

The IAL report continues:

Nor has it been broken apart in the way that it has in financial services organisations. Instead, what is usually known as operational risk reflects the full spectrum of management activities involved in running a business. Corporates treat the management of risk as an inseparable part of business, and therefore as an inseparable responsibility of line managers.

This highlights a serious definitional challenge: the statement is all but impossible to contradict because it is so general a point; the language gets in the way.

Usefully, IAL distinguishes between the risk oversight and marginal decision roles of the board:

This report will make the distinction between the two ideas by using the terms 'board oversight of risk processes' and 'board-level risk acceptance'.

In light of the new FRC requirements, to these must be added:

- specification of target (portfolio) aggregate risk-holding (ie. risk appetite)
- comparison of risk holding in marginal decision-making against the (portfolio) aggregate risk-holding of the firm (ie. risk tolerance)

However, there is much debate about how to do these in practice. We believe that to do either of these meaningfully requires use of both quantitative and qualitative techniques. In contrast, the IAL report states:

Risk appetite, like many of the techniques of risk management, has its home in the financial services industry, where it has been interpreted to mean the financial quantification of acceptable risk exposure. Corporates well understand and appreciate the concept of 'acceptable' in relation to risk exposure, but struggle over giving it financial quantification. This is hardly surprising since so many of a corporate's risks are non-financial in nature, even if they will ultimately have financial consequences.

Elsewhere in its report, IAL makes its opposition to quantification plain:

[T]he day-to-day business of a corporate is primarily concerned with 'operational risks', more broadly defined than in financial services, and which are much more difficult to measure in financial terms.

---

<sup>3</sup> Prakash Shimpi, (1999). *Integrating Corporate Risk Management*, (NY: Texere).

Some risks, such as the risk of loss through contract overruns, can be estimated financially, but in many other cases (such as health and safety or the delivery of essential services to the public) the financial quantification of exposure and appetite is usually impracticable or unhelpful, or both.

The conclusion appears to be: if it is difficult or requires making assumptions in order to quantify impact, it is not worthwhile. This astounding conclusion is incompatible with estimation of risk appetite and tolerance.

Furthermore, in direct contradiction of the significant conclusions of the growing body of literature in risk perception (and without apparent reference to it), IAL states:

‘Risk attitude’ is a better descriptor of what most corporates understand to be useful, and in most corporates it is communicated to management implicitly, by inference from the board’s decisions. It is in fact possible to communicate it more explicitly, using words rather than numbers, and some boards could do more to make their attitude to risk explicit. This would make it more consistently understood across the organisation, and therefore more likely to be followed.

The challenges of establishing a consistent approach to risk for an individual in a single risk class are well documented (eg. prospect theory and asymmetric risk preferences). The inconsistencies of applying risk knowledge and perceptions consistently by an individual across risk classes are similarly well documented as are tendencies for individuals to make decisions inconsistently in general (eg. ‘decision heuristics’ such as anchoring or framing of risk). The challenges of interpersonal risk preferences (and utility preferences generally) are well established (eg. Kenneth Arrow (1951)) and the perils of group decision making under conditions of stress and uncertainty are well established (eg. Irving Janis’ landmark ‘Groupthink’ work in the 1970s). Collective formation of ‘risk attitude’ appears to be an unlikely source of improved corporate clarity on risk.

## **OBSERVATIONS ON THE PROPOSED TEXT FOR CODE PRINCIPLES AND PROVISIONS**

‘C.2 Risk management and internal control, Main principles’ states

The board is responsible for defining the company’s risk appetite and tolerance. The board should maintain a sound system of risk management and internal control to safeguard shareholders’ investment and the company’s assets.

### *Active language*

The language used in the first sentence of this principle is very active: it implies that the board should *itself* define the company’s risk appetite and tolerance. This contrasts with more usual practice that the board review, challenge and ultimately approve (or reject and require re-submission) the company’s statement(s) of risk appetite and tolerance. The language used can be contrasted with the language of the Code in relation to strategy:

As part of their role as members of a unitary board, non-executive directors should constructively challenge and help develop proposals on strategy.

The FRC should decide on its preferred activeness of language and maintain consistency across activities of the board.

*Definition of 'risk tolerance' and 'risk appetite'*

The concepts of risk appetite and risk tolerance are not defined by FRC. Establishing a requirement that is enormously difficult to operationalise without clear direction on definition risks creating a vacuum in to which expedient and 'pragmatic' solutions will rush; rigour, relevance and subsequent utility will be overlooked in order to achieve rapid and painless compliance.

In our experience, very few firms **even in the financial services sectors** have successfully or meaningfully defined risk appetite at a corporate level. The task is complex and requires considerable thought and subtlety. Among the very few that have genuinely tried, even some of the UK's most sophisticated corporate firms are struggling with making risk appetite and tolerance relevant and useful.

A critical issue is the limited number of professional firms capable of providing informed and meaningful advice on risk appetite and risk tolerance. The language of the revised Code implies that these areas are clearly within the purview of major audit firms; however, the major audit firms' record in relation to risk management in both the financial services and corporate sectors is decidedly mixed. The issues of risk behaviour and the feedback mechanisms between behaviour at personal and group level (sometimes called 'culture') and analytical risk approaches are complex; accounting training is not especially helpful to understanding that complexity and may, because of its deterministic nature, actually be counter-productive.

Similarly, experience may not be a useful starting point. Most corporate practice in risk (outside corporate finance and treasury) has focused on the creation of 'systems of risk management' built upon risk registers and risk matrices. While very widely accepted as 'best practice' (a dangerous concept in itself), there is little or no empirical evidence supporting the effectiveness of these approaches. Where evidence has been marshaled it has typically challenged the utility of these crude, control-based approaches and shown myriad instances in which they have been either non-contributory or counter-productive.<sup>4</sup>

With his usual clarity, Michael Power sums up the problem thus:

The policy question is whether operational risk specifically, and internal control in general, really stimulate **an intelligent risk management capable of challenging existing ways of making sense of the world within and outside organisations**, or whether they simply end up as the 'normalisation of deviance' in a dense network of procedures and routines. The suspicion is that, while operational risk facilitates a greater '**managerialisation of risk**' via new organisational processes, and extends the scope of the risk manager's and the regulator's work into more corners of organisational and social life, it also reinforces **myths of controllability** in areas where this is at best limited – for example, the

---

<sup>4</sup> See for example Tony Cox, (2008). What's Wrong with Risk Matrices? *Risk Analysis*, Vol. 28, No. 2, 497 – 512.

senior management culture and the often discussed ‘tone at the top’ of organisations” (*emphases added*)<sup>5</sup>.

Adding the further complexity of stating appetite or tolerance on to these systems or requiring consideration of ‘risk attitude’ of the firm will simply compound an already unsatisfactory state of affairs.

In order to overcome the gap in understanding we have described, we believe FRC should state within the principles an expectation that risk appetite and tolerance should have both quantitative and qualitative aspects. Ample precedent and support for such a view is available.<sup>6</sup>

#### *Conflating risk management and internal control*

To avoid conflating risk management and internal control, we believe FRC should separate the sections on management of risk and internal control, possibly thus:

- C.1 Management of risk
- C.2 Corporate reporting
- C.3 Internal control
- C.4 Audit Committee and auditors

The objective stated for risk management and internal control at present is “to safeguard shareholders’ investment and the company’s assets”. This is appropriate for internal control but is inadequate in relation to risk. First, it ignores the real and important issue of physical risk. Secondly, “safeguarding” shareholders’ investment is a limited objective; a more appropriate objective is to optimize the trade-off between risk assumed by the firm and expected rates of return on shareholders’ investment. Thirdly, the focus on “the company’s assets” is implicitly restrictive; focus must include tangible assets and intangibles generally including human capital. Failure to make that explicit will lead to these vital sources of value being overlooked or excluded.

Here, the distinction drawn by IAL between ‘board oversight of risk processes’ and ‘board-level risk acceptance’ is instructive. The requirement in C.2 would be clarified by incorporating the distinction alongside the other activities of definition of risk appetite and risk tolerance.

#### *Risk systems and processes, oversight & assurance*

Provision C.2.1 states:

C.2.1. The board should satisfy itself that appropriate systems are in place to identify, evaluate and manage the significant risks faced by the company.

The usually-depicted idea of risk process is linear<sup>7</sup>. However, in reality, risk processes are messy and non-linear – risk management is not a well-ordered, sequential process. It is better thought of as a continual and

---

<sup>5</sup> Michael Power, *The Risk Management of Everything*, (2005). *The risk management of everything: rethinking the politics of uncertainty*, (London:Demos)

<sup>6</sup> NACD, 2009, *Risk Governance: Balancing Risk and Reward* (Report of the NACD Blue Ribbon Commission)

recursive process of sense-making informed at personal and group level, grounded in a focus on operational process, financial outcome and external events and triggers. Because of this, the path referred to by the draft Code [that is, identify > evaluate > manage] is misleadingly simplistic.

More useful would be recognition of multiple, related and simultaneous processes involving:

- anticipation of risk
- detection of threats and emerging risks
- development of (financial and operational) resilience to risks
- assessment of risk exposure and impact and scenario analysis
- responses to risk

Under C.2.2, the review requirement should relate to ‘board oversight of risk processes’ (in IAL’s terminology). Also, at C.2.2, the conflation of risk with internal control – “controls, including financial, operational and compliance controls and risk management systems” – is at its clearest. By separating the provisions for risk management and internal control, FRC would get around the problem of conflation and the confusions it will create for users of the Code.

The unhelpful conflation also arises at C.3. Consistent with our suggestion to separate management of risk from internal control, we further suggest that C.3 should be re-worded as follows:

The board should establish formal and transparent arrangements for considering how they should apply the principles relating to management of risk, corporate reporting and internal control and for maintaining an appropriate relationship with the company’s auditors.

#### *Audit Committees*

C.3.1 imposes the requirement on the Audit Committee that at least one member have “recent and relevant financial experience”. This requirement relates to and is satisfactory for review of financial reporting and disclosures and financial aspects of internal control. However, by expanding the remit of the audit committee to incorporate review of the firm’s “risk management system,” the Code also imposes a *de facto* requirement for expertise in disciplines relating to corporate management of risk; the distinction of Walker between backward-looking and forward-looking requirements is, or should be, instructive.

In order to flow through the changes we suggest to earlier provisions, we suggest the following changes to C.3.2:

C.3.2. The main role and responsibilities of the audit committee should be set out in written terms of reference and should include:

- to monitor the integrity of the financial statements of the company and any formal announcements relating to the company’s **[historic]** financial performance, reviewing significant financial reporting judgements contained in them;

---

<sup>7</sup> For example, A/NZS 4360 : Risk Management (1995) and the recent BS 31100 (2008)

- **[unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to monitor the integrity any formal announcements relating to the company's prospective financial performance, reviewing significant risk assumptions contained in them];**
- unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the **[structure, focus and performance]** of the firm's risk management systems **[and processes and its risk capabilities];**
- to review the **[structure, focus, capabilities and performance]** of the company's internal financial control systems **[and processes];**

## CONCLUSION

We believe that, taken together, these changes will strengthen the board's role in an effective structure of corporate risk governance and management of risk. However, FRC should ensure that adequate and properly-informed guidance be made available to reporting companies on:

- quantitative and qualitative approaches to risk appetite and risk tolerance;
- risk governance and assurance;
- behavioural issues in risk;
- issues in integrating risk and control-related functions (including internal audit).

For these to be effective in improving corporate risk performance, FRC will need to accept:

1. in order to support a rigorous approach to risk appetite and risk tolerance, where the distinctions between risk management and internal control systems and processes of the firm are clear, FRC will need to sponsor a wholesale revision to guidance on risk management and on internal control;
2. to support analysis of corporate risk appetite and risk tolerance, corporate risk performance needs to improve materially, especially in behavioural risk practice and quantitative and qualitative analysis of risk; broader or deeper application of existing practices will not suffice for meaningful analysis of risk appetite or risk tolerance;
3. because of the very different needs of companies across sectors, stages of competence and maturity, competitive intensity, ownership and leverage, different firms will have very different requirements for risk management – there will be and should be diverse risk management practices;
4. there is no such thing as 'best practice' in risk management, any more than there might be 'best practice' in strategy; each firm will have different behaviours for making sense of its external and internal risk environments and a different mix of capabilities with which to do so;
5. there will need to be a diversity of sources of knowledge and expertise on corporate risk management practice; no single type of provider will have either a monopoly on or comprehensive coverage of risk expertise;

6. knowledge on corporate risk practice will only move forward with far greater emphasis on empirical analysis of risk systems and process effectiveness. Opinion-based commentaries shed little light on what works in practice and, more importantly, what does not. Even if they have the knowledge to do so, corporate interviewees face very limited psychic or organisational incentives to question norms of corporate risk practice and performance or to question its efficacy at firm level.