

# Matthew Leitch Associates Limited

[www.internalcontrolsdesign.co.uk](http://www.internalcontrolsdesign.co.uk)

tel 01372 815 856

29 Ridgeway, Epsom  
Surrey, KT19 8LD

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

11 December 2009

Dear Chris

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

Thank you for the opportunity to comment on the Code and I hope you find my analysis helpful. These comments are limited to analysis of just one important phrase.

I personally welcome action to put more focus on the board's responsibility for governing risk taking by the company and the idea of guiding management in their consideration of risk during planning and decision making. Poor risk taking has been a problem.

However, I strongly recommend avoiding the phrase 'risk appetite and tolerance' because of the confusion likely to result and because it refers to an incomplete approach.

In section C the phrase '...defining the company's risk appetite and tolerance.' could be replaced with something like '...setting policies governing the company's risk taking' or "...setting policies governing the company's risk taking, including overall limits."

This would be a more complete statement of what is needed, without the technical gaps, and would result in less confusion.

These issues were debated at length by the RM/1 committee at the British Standards Institute when we were drafting *BS 31100:2008 Risk management - Code of practice*. In addition, I have recently completed a survey of published definitions of the phrase

‘risk appetite’ and found a situation that will not support use of this phrase in the UK Corporate Governance Code.

### **Potential for confusion**

A sense of familiarity with phrases like ‘risk appetite’ and ‘risk tolerance’ is not the same as a true understanding.

Although definitions of ‘risk appetite’ have been published, even the most authoritative do not agree with each other. Some refer to limits while others envisage propensities. The related terms ‘risk attitude’ and ‘risk tolerance’ seem almost interchangeable at times. These variations, flowing from the inherent difficulty of the concepts involved, have made this whole area confusing for most people.

Added to this variety is the fact that interpretations of ‘risk appetite’ in practice differ from the published definitions. While most definitions refer to a single limit placed on assessed risk, in practice organizations have used:

- statements in words as well as statements using numbers;
- multiple limits, not just one; and
- limits on activities (e.g. extent of investments), tolerances on KPIs, and limits based on risk factors, not just limits on assessed risk.

In effect the systems companies describe under the heading of ‘risk appetite’ are systems of limits operated rather like a budgetary control system.

It is significant that the ICAEW’s report *Getting it Right* found that companies recognize the phrase “risk appetite” but tend not to use it internally.

In addition, many people see the phrase ‘risk appetite’ as implying a psychological construct. It is seen as something personal, like a facet of a person’s personality or mood. This idea is applied to organizations too, by analogy.

Consequently, some people are inclined to see ‘risk appetite’ as something that cannot be objectively wrong. Like preference for certain wines or holiday destinations, if you like it you like it, and that’s all that matters.

One unfortunate effect of this is to divert attention away from important, objective factors that should be considered when deliberating over a risky course of action or a risk limit. These objective factors include financial resources, organizational flexibility, management skills and experience, ability to monitor risks, and predictability of future income.

Another effect is that many people think the maximum level of risk that is acceptable exists in isolation, when in fact it depends on the level of reward and other objective factors. Consequently, they do not appreciate the need to revise their ‘risk appetite’ frequently enough for it to remain relevant and usable.

Given the audience of the UK Corporate Governance Code many readers would refer to the definition of ‘risk appetite’ used in COSO’s ERM framework. This describes ‘risk appetite’ as an overall limit stated in broad terms and ‘risk tolerances’ as specific limits placed on key measures of performance.

Even here there is a small but significant difference between their thinking and the wording of the consultation draft, which refers to ‘tolerance’ in the *singular*, suggesting there is just one and it is different from ‘risk appetite’.

This is a terminological minefield that the UK Corporate Governance Code should keep well clear of.

In contrast, a phrase such as ‘risk limit’ does not have these psychological connotations and resulting problems. It is obvious what is meant. People are not distracted from the more logical behaviour they would naturally prefer.

### **Technical gap**

If ‘risk appetite’ is interpreted as a limit or system of limits on assessed risk then this provides incomplete guidance on how to incorporate risk in decision making.

Once risk has been managed to within a ‘risk appetite’ risk continues to be relevant. For example, suppose a business decides to launch a new product, having weighed the potential risks and rewards and decided that the risks are acceptable, given the rewards anticipated. That does not mean that the business has no interest in further improvements to the risk profile of the product. If a control is thought of that would be easy to implement it could very well be worthwhile even though the risk is already ‘acceptable.’

*BS 31100:2008 Risk management - Code of practice* says in section 4.5.5

‘The process should be repeated until the level of residual risk is within the risk appetite and pursuing further control changes does not seem worthwhile.’

Deciding what is worthwhile requires further consideration of risk.

Just as budgets limit spending without ensuring that money is well spent, so risk limits place an upper boundary on risk taking without ensuring that good risks are selected.

Company policies governing risk taking can do more than impose limits, and often they do.

### **Referring to the broader governance of risk taking**

A statement such as:

‘The board is responsible for setting policies that govern the company’s risk taking.’

would encourage boards to consider all policies relevant to risk taking.

Additional guidance might suggest defining how risk should be considered in decision making, and perhaps even list objective factors that should be considered, such as financial reserves, predictability of future income, stakeholder requirements, flexibility of business systems and processes, and management's ability to cope.

If it is felt that the UK Corporate Governance Code should be more explicit in requiring the board to be involved in setting limits then the statement could be extended to:

‘The board is responsible for setting policies that govern the company’s risk taking, including setting overall limits.’

This wording makes it clear that limits are intended and that the board must set at least some of them (not just one, and not all of them at all levels). It also avoids implying that the limits should all be placed on assessed risk per se, which is only practical for some risks.

By simple wordings such as these it should be possible to express exactly what was originally intended without inadvertently causing confusion and subsequent compliance problems.

Yours sincerely

A handwritten signature in black ink that reads "Matthew Leitch". The signature is written in a cursive, slightly slanted style.

Matthew Leitch