Matthew Leitch Associates Limited

Tutoring, research, authoring, consultancy
www.WorkingInUncertainty.co.uk
29 Ridgeway, Epsom
Surrey, KT19 8LD

Catherine Woods
The Financial Reporting Council
5th Floor, Aldwych House
71-91 Aldwych
LONDON WC2B 4HN

22nd January 2014

Dear Catherine

Consultation on Draft Guidance to the Directors of Companies applying the UK Corporate Governance Code and associated changes to the Code

Thank you for the opportunity to respond to this consultation. In my response I will briefly highlight some very positive directions in the consultation draft, but then focus on one crucial technical and drafting issue that needs to be addressed.

My comments are informed in particular by my years of service on the Risk Management committee at the British Standards Institution, including my work on both editions of BS 31100, a standard on general risk management, for which I was awarded two distinguished service certificates. They are also informed by a series of surveys I have conducted over the past few years to uncover what most people think on a variety of risk management issues.

These unique surveys show that what most people want from risk management is not yet reflected in the most prominent guidance. Those of us involved with writing that guidance have work to do.

Directions that will be welcomed

1. Integration of risk management and internal control

The draft guidance brings together internal control and risk management into one document and then avoids trying to make a clear distinction between the two.

This is something a lot of people have been wanting for some time. IFAC's survey in 2011 showed that a vast majority wanted an end to separate guidance on risk management and internal control[1].

[1] IFAC (2011). *Global Survey on Risk Management and Internal Control*. See especially questions 2.3 and 2.4. Available online: http://www.ifac.org/sites/default/files/publications/files/global-survey-on-risk-manag.pdf

This probably reflects the recognition that there is such an overlap between risk management and internal control work and people that it is hard to draw a clear and consistent boundary between the two.

For example, the Institute of Internal Auditors' standards currently talk about auditing risk management, internal control, and governance. Some have interpreted this as requiring three separate opinions but in practice it is extremely difficult to get auditors to classify issues and evidence between these three categories consistently. Ask ten auditors to classify twenty issues between the three categories and you will get ten different patterns of answers.

My own observation is that proposed methods for risk management and internal control are often virtually identical and that no meaningful distinction can now be drawn between them.

The draft guidance does not say this, and indeed maintains the idea that risk management and internal control are different things, but it's a step in the realistic direction.

2. Risk control as an integral part of management

Another welcome theme in the draft guidance is its emphasis on the importance of risk control being an integral part of good management, and not a separate process or function, especially not an annual ritual with no real effect on important business decisions.

My surveys confirm that managing risk within core management activities such as decision-making, planning, and designing the business is overwhelmingly preferred to separate processes with separate meetings, documents, reports, and so on[2].

3. Integration with going concern

This is another integration that makes sense, though I do not have survey evidence as to whether this is widely preferred.

4. Move towards ongoing monitoring rather than annual reviews

Again, this makes sense but I do not have relevant survey evidence.

The technical issue

The technical issue that needs to be addressed is an answer to your question about whether the guidance is at the right **level of detail**. It is not. It is much too detailed and, in particular, it is repeatedly very prescriptive about the method to use, making it difficult for companies to do anything other than use a 'risk-listing' approach.

The risk-listing approach, though instantly recognisable when described, does not have an established name at present. I use 'risk-listing' as the name because it strongly suggests one of the key characteristics of the method.

In order for this issue to be resolved sensibly and fairly it is important for those responsible for the final form of the guidance to understand clearly:

1. what risk-listing involves and how it can be distinguished from more established approaches;

[2] For example, Leitch (2011). *Results of a survey on 'project risk management'*. Available at: http://www.workinginuncertainty.co.uk/study_pram_report.shtml

2. the key limitations of each approach;
3. the extent to which the draft text prescribes risk-listing, and how it does that; and
4. what changes would be necessary to the draft to stop is prescribing risk-listing as the sole approach.

The following sections provide information on each of these points that I hope will be helpful.

1. Approaches to risk management

The challenge of making decisions under conditions of limited knowledge and control has been with us always, but the first great steps towards rigour were taken some 350 years ago by the pioneers of probability theory. Over the centuries these ideas developed and spread, appearing as actuarial science to rescue the insurance industry from pure guesswork, and as operations research to help with numerous challenges in war and industry. Today we apply science and mathematics to the big decisions on matters such as nuclear safety, space missions, medical interventions, and major financial investments.

Not all risk management by science and mathematics involves detailed analysis. Sometimes careful consideration leads to a policy decision to adopt particular management strategies as a matter of policy, and then those strategies are used without further analysis.

Some typical tools used in a management science approach are explicit forecasting models for decision support, scenario planning, game theory ideas, and decision trees.

Risk-listing has arisen more recently. Rather than applying science to improving core management activities (decisions, planning, business model design, etc), risk-listing involves making a list of ‘risks’ and then managing the ‘risks’ on that list. This is typically done using separate meetings, documents, databases, reports, and roles, despite the aspiration to somehow embed this approach within management.

The tools most commonly used in risk-listing are risk registers and probability-impact matrices with risk criteria/appetite lines.

In summary, the management science approach to risk management is to apply science and mathematics to improve existing management activities such as decision-making. The risk-listing approach to risk management is to add a new process that creates and then manages ‘risks’.

2. The limitations of alternative approaches

The logic of the risk-listing process is that actions and related decisions are considered only once ‘risks’ have been listed, and the actions are responses to those ‘risks’. This means that the scope of risk-listing is restricted to actions seen as wholly or principally responses to one or more ‘risks’ (e.g. buying insurance, fitting a fire sprinkler system, or building an extra crash barrier).

This leaves out many important business decisions, perhaps most, such as whether to launch this product or that, whether to build a bridge or a tunnel, and the choice of contractor for a major project.

Through surveys I have confirmed that the vast majority of people think that risk management should help with all significant decisions, not just those that are

responses to ‘risks’. I have also found that most people regard techniques drawn from the traditional management science approach as much better examples of integrated risk management than techniques involving making lists of risks. People are also much more likely to recommend techniques seen as more integrated.

This issue with risk-listing is sometimes not recognized because people think the leading guidance on risk-listing says something sensible that in fact it does not say. A survey in 2013 done to inform future work on ISO 31000 showed that many people think ISO 31000:2009 advises doing a risk analysis of each option in major decisions and that it would support a ‘bridge or tunnel’ decision[3]. In fact, this is not the case.

This misunderstanding is probably due to our wishes to make sense of what we read and to see the best in things that many people appear to support.

The limitations of management science are also important and some serious mistakes have been made from time to time. Their consequences have been great simply because we rely on these methods so heavily, but when problems occur the reaction is always to try to do things better within the same basic scientific approach, not to abandon models and data and instead rely on a brainstormed list of ‘risks’.

In summary, the consequence of prescribing a purely risk-listing approach for companies would be to focus them on a method that has a much narrower scope and lesser effect than most people would like. It would also mean that companies using other, perhaps more effective and comprehensive, methods would not be able to offer those as evidence of good risk management. Boards would then tend to focus on the wrong risk management work.

3. The extent to which the draft guidance prescribes risk-listing

Individual phrases combined with an overall risk management process model make the draft guidance strongly prescribe risk-listing as the sole approach to risk management.

Language that steers readers towards risk-listing includes the following phrases:

‘risks’ : This word – the plural of risk – is the simplest and strongest cue indicating risk-listing.

‘principal risks’ : This includes ‘risks’ and also carries the subtle implication that ‘risks’ are pre-existing entities (rather than concepts defined by the analyst) that can be ranked and selected for size. This idea is characteristic of risk-listing.

‘principal risks and uncertainties’ : This adds the additional implication that ‘risks’ are not uncertain, reinforcing the risk-listing notion that they exist as external realities rather than as ideas.

‘emerging risks’ : Again this implies that ‘risks’ are real-world objects.

‘identify risks’ : This carries the implication that the ‘risks’ already exist and just need to be spotted. This is characteristic of risk-listing and quite different from the scientific idea that we create models to help us think about the world.

‘manage risks’ : This refers to the main goal of risk-listing, which is to manage ‘risks’ – not risk, and still less a business.

[3] Leitch (2013). *Results of a survey on ISO 31000:2009 and future editions.* Available at: http://www.workinginuncertainty.co.uk/study_iso_report.shtml

'acceptable risks' : This brings in another characteristic risk-listing idea, which is that a 'risk' can be acceptable or unacceptable without considering any other factors, such as the difficulty of mitigation.

'risk management process' : The idea that risk can be managed using a process is another typical of risk-listing guidance, where it is normal to show a diagram of that process with no reference to any other aspect of management, such as business planning, business model design, and other decisions.

These phrases appear on most pages of the draft guidance, continually reinforcing the sense of risk-listing.

In addition, the overall sequence of headings and some statements made within the text explain that risk is to be managed by following a process that involves risk identification, followed by assessment and management of those risks. This is the classic risk-listing process.

4. Changes to make the draft guidance less prescriptive of risk-listing

A combination of simple strategies can be used to open up the guidance so that it conveys a sense of the required level of rigour but without prescribing risk-listing as the only approach.

4.1 Principal risks and uncertainties

The phrase 'principal risks and uncertainties' strongly conveys the concepts of risk-listing. To understand the alternative approaches to avoiding this problem it helps to understand clearly the underlying theory.

When people create a risk analysis for something (either a risk-list or to support a business decision) they do so by structuring and dividing their overall uncertainty in a way that makes sense to them and helps them think. Different people, with different perspectives and ideas about how things work, will produce different analyses. Even with risk-listing, different people will produce lists that are different and yet equally valid (though not necessarily equally useful). Survey evidence shows that this is understood by most people[4].

If the 'risks' in a list are sorted to put the 'biggest' at the top then their order depends on how the overall risk was divided up into 'risks'. The 'principal risks' (i.e. the ones at the top) will be different depending on who made the list and how.

In contrast, risk-listing is only consistent with the idea that 'risks' are pre-existing objects whose boundaries are not chosen by people.

An additional flaw in risk-listing's approach to prioritisation is that it tends to focus on risks at the top of the ranking list (called 'key', 'principal', or 'top 10') regardless of the proportion of total risk these represent. In most cases nobody knows if the top 10 'risks' represent 5% of the total or 95% of the total. Clearly, it matters.

Ways around the phrase 'principal risks and uncertainties' include:

- Removing the phrase completely and writing 'an analysis of the risk and uncertainty facing the board'.

[4] Leitch (2007). *Alternative risk lists: results of an online survey.* Available at: http://www.internalcontrolsdesign.co.uk/idquizresults/index.shtml

- Retaining the phrase but explaining that the 'principal risks and uncertainties' represent an analysis of the total risk and uncertainty facing the board. (This can be further refined by requiring the analysis to exclude no more than some small proportion of the total risk.)

4.2 Specific words for code changes

The existing main principle under C.2 is proposed as:

> The board is responsible for determining the nature and extent of the *principal risks* it is *willing to take in achieving its strategic objectives.* The board should maintain sound risk management and internal control systems.

The phrases in this text that convey risk-listing have been italicised. In addition to the problem that 'principal risks' conveys risk-listing the phrase is also ambiguous in this context because 'risks' here can be interpreted as 'actions whose outcome is uncertain' rather than 'risks' in the usual risk-listing sense. Finally, there is the problematic idea of setting risk limits regardless of prospective reward, which most people do not agree with[5].

Here is an alternative wording that is more open and closer to comprehensive:

> The board is responsible for governing decisions in the company and should determine policies that help it do so. The board should maintain sound risk management and internal control systems[6].

Such policies would include policies on risk assessment as well as on decision-making once assessments have been made.

The proposed code rule C.2.1 is:

> C.2.1. The board should carry out a robust assessment of *the principal risks* facing the company, including *those* that would threaten its solvency or liquidity. In the annual report the directors should confirm that they have carried out such an assessment and explain how *the principal risks are being managed or mitigated*. They should indicate which, if any, are *material uncertainties* in relation to the company's ability to continue to adopt the going concern basis of accounting.

Again, italics have been added to highlight the phrases that prescribe use of 'risks' as opposed to other concepts for risk management. Here's a revision that is more open:

> C.2.1. The board should carry out a careful and open-minded assessment of the future prospects of the company, including its solvency or liquidity, that considers the likelihood of alternative possibilities. In the annual report the directors should confirm that they have carried out such an assessment and explain how risk is being managed. They should provide an analysis of the uncertainty around the assessment such that any uncertainty not presented in the analysis is immaterial to the company's ability to continue to adopt the going concern basis of accounting.

[5] Leitch (2011). *Results of a survey on 'integrated risk management'*. See the item called 'policy on project acceptance'. Available at: http://www.workinginuncertainty.co.uk/study_integ_report.shtml

[6] These suggested wordings may be used in the final guidance without copyright problems.

With this wording a company using an integrated probabilistic forecasting model for its business planning and other decisions would comply, as would a company that lists 'risks' and manages them.

4.3 Systematic wording changes

Risk-listing language is very common throughout the draft guidance but some systematic word replacements throughout would dramatically reduce their effect. In each case, replacing the phrase will need to be accompanied by other grammatical and occasional logical edits to the sentences affected.

- Replace 'risks' with 'risk'. (In some cases it is easier to delete the word risk because it adds nothing, e.g. 'risk culture' becomes 'culture'.)
- Replace 'the principal risks' with 'the company's analysis of risk' or 'most of the risk'.
- Replace 'solvency and liquidity risks' with 'chance of insolvency or illiquidity'.
- Replace 'identify risks' with 'analyse risk'.
- Replace 'risk appetite' with 'policies on risk taking' or 'policies governing decision-making'.

In relation to the last point on this list, a survey specifically on 'risk appetite' performed in 2010 showed the extent to which people find other phrases more self-explanatory and clearer than 'risk appetite'[7]. In view of the massive preference for other phrases over 'risk appetite' found in 2010 it is unlikely that there has been any significant change since.

4.4 Overall outline and process model

Sections 4 and 5 of the draft guidance are particularly prescriptive, with risk-listing logic stated in detail, particularly in paragraphs 25 and 34.

Here is paragraph 25 with the risk-listing material italicised:

> 25.The board should *identify the principal risks* facing the company and evaluate *the likelihood of their incidence, and their impact if they were to materialise.* It should assess the availability and likely effectiveness of actions that it would consider undertaking, either in advance or when a trigger event occurs, to avoid or reduce the impact of the *underlying risks.*

In addition, the second sentence places actions *after* risk analysis, making them responses to the 'risks', as in risk-listing.

Here is a more open alternative:

> 25.The board should assess the future prospects of the company and analyse its uncertainty around those prospects in a rigorous way. It should consider alternative courses of action that might provide the same or greater rewards at less risk.

This way a company that projects the future with a sophisticated model is complying with the requirement, and so is a company that makes a risk-list.

[7] Leitch (201). *Results of a survey on risk phrases.* Available at: http://www.workinginuncertainty.co.uk/study_raphrases_report.shtml

Here is paragraph 34 with the risk-listing material italicised:

34.When developing a system of risk management and internal control that is suited to the particular circumstances of the company, the board should consider:

- the *nature and extent of the risks facing, or being taken by, the company which it regards as desirable or acceptable for the company to bear. For example, the higher the risks accepted, the greater the likely need for stronger and more timely monitoring controls and contingency planning; while an exposure to low probability but high impact risks may increase the need for effective crisis management systems*;
- *the exposure to risks before and after the application of controls and mitigations, as appropriate;*
- *the likelihood of the risks concerned materialising, and the consequence of related risks materialising as a result or at the same time*;
- *the company's ability to reduce the incidence and impact on the business of risks that do materialise, and to withstand such instances*;
- *the effectiveness and relative costs and benefits of particular controls*; and
- the impact of the values and culture of the company, and the way that teams and individuals are incentivised, on the effectiveness of the system.

Here's that paragraph again, simplified and opened up:

34.When developing a system of risk management and internal control that is suited to the particular circumstances of the company, the board should consider:

- the risk facing the company and the features of its management system that are most important in managing that risk;
- the likely effect of features of its management system designed to manage risk;
- the likely effect of its values, culture, and incentives on management.

Conclusion

This response has highlighted some positive intentions behind the draft guidance concerning integration but has then focused on the problem of its prescriptive risk-listing language and content. Crucially, you cannot have integration with core management activities using a risk-listing approach. Risk-listing is always a separate process no matter how often you do it.

Prescribing risk-listing as the only acceptable approach would block true integration with management and focus boards on a very narrow subset of decisions in companies. It would reduce attention to the more conventional approaches to managing risk that our society relies on.

Yours sincerely

Matthew Leitch