

## Financial Reporting Council



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

Joint response by AIRMIC and the Institute of Risk Management (IRM) to the Financial Reporting Council consultation dated December 2009 on the revised Combined Code – to become the UK Corporate Governance Code.

#### **AIRMIC and IRM Membership**

AIRMIC has a membership of nearly 900 and represents the risk managers of about 75% of the FTSE 100, as well as very substantial representation in the mid 250 and other smaller companies. AIRMIC members facilitate risk management activities within their employer organisations and many AIRMIC members are also responsible for the purchase of insurance.

The Institute of Risk Management (IRM) has a global membership of nearly 3,000 representing a broad spectrum of risk professionals from commercial, industrial and public organisations. Established as a not-for-profit body and governed by its members, IRM is the leading provider of enterprise-wide integrated risk management qualifications and training in the world. IRM also has strong links with leading universities, business schools and other professional organisations, is active in the development of guidance and standards in risk management and is a widely-consulted source of opinions and knowledge on most aspects of risk.

AIRMIC and the IRM, together with Alarm, the public risk management association, have recently published a guide entitled *A structured approach to enterprise risk management (ERM) and the requirements of ISO 31000*. This guide sets out an approach to enterprise risk management that is compatible with the requirements of the UK Corporate Governance Code. Appendix A of the guide provides a checklist of the actions required to embed a comprehensive enterprise risk management culture within an organisation.

The opinions put forward in this submission are based on and compatible with this recently published guide. A copy of the guide can be obtained free of charge from:  
<http://tinyurl.com/ERM-iso31000>.

## AIRMIC and IRM Opinion

AIRMIC and the IRM wish to comment on the proposed amendments to Section C on **Accountability**. In particular, AIRMIC and the IRM wish to comment on part C2 on **Risk Management and Internal Control**, although part C1 on **Corporate Reporting** and part C3 on **Audit Committee and Auditors** are also relevant to the activities of our respective memberships.

### Section C – part C1: Corporate Reporting

Code Provision C.1.2 is a welcome addition, but it should be extended to include the requirement that the annual report should also explicitly describe the significant risks that could undermine “... .. *the basis on which the company generates revenues and makes a profit* ... ..”.

The additional requirement to describe the significant risks will give shareholders a clearer idea of the degree of uncertainty attached to the revenue and profit of the company. This will assist shareholders with an understanding of the quality of the revenues of the company.

### Section C – part C2: Risk Management and Internal Control

The Main Principles set out under part C2 are stated in terms that may be difficult to interpret and apply in practice. In particular, the (new) first principle that the board is responsible for defining the risk appetite and tolerance is not necessary a helpful starting point for successful risk management. Despite the difficulties, AIRMIC / IRM accept that a discussion at board level about risk tolerance and risk appetite may be helpful in formulating the overall attitude of the company to risk and risk management.

Risk appetite remains a very specific, difficult to apply, often ill-defined and much debated topic within risk management and business circles. Further guidance on precisely what is required will be necessary if this principle remains unchanged. A statement of risk appetite may be helpful and some types of organisations may be able to produce such a statement, it is more sensible and helpful for the principle to be stated in terms of the requirement for the board to define / establish / monitor the risk strategy of the company.

The board should be responsible for the risk committee structure and risk communication arrangements in the company. This is often referred to as the risk architecture of the company. The board should also be responsible for the risk strategy, as well as the risk protocols / procedures / policies that have been established. If the main principle is stated in a more general way than just risk appetite, it will be easier to understand the principle. Establishment of the risk architecture, strategy and protocols for the company will ensure that the board pays due regard to the full scope of what is required in order to successfully manage risks. This will enable the board to gain comprehensive risk oversight and subsequently provide relevant information to shareholders.

The second main principle under part C2 is sound, but could be extended to specifically include the safeguarding of the reputation of the company, as well as shareholder investment and company assets. It could be argued that reputation is one of the company assets, but it is sufficiently important to be explicitly mentioned.

Code Provision C.2.1 is sound, but could be extended to specifically require that systems are in place not only to identify, evaluate and manage the significant risks, but also to manage the potential impacts should the risks materialise. These additional words will focus the attention of the board on the consequences of a risk materialising, by requiring the identification of the undesirable impacts that the board is seeking to mitigate / manage / minimise.

Code Provision C.2.2 is sound, but could be extended to specifically require that the board reviews the risk assessment procedures that are in place, together with a review of any assumptions that underpin the approach to risk management.

## Section C – part C3: Audit Committee and Auditors

Main Principle C3 is well stated, but the Code Provisions place undue emphasis on the role and responsibilities of the Audit Committee and Auditors. The approach whereby the company makes decisions on how to apply risk management through an executive or management committee responsible for risk management is not described or even acknowledged. The approach described in the consultation paper relies heavily on the Audit Committee and this could lead to risk management being treated as a non-executive responsibility, rather than an executive responsibility.

Risk management is an executive responsibility that should be monitored and reviewed (rather than led) by the Audit Committee. AIRMIC / IRM are of the opinion that risk management responsibility should be allocated to a specific executive or management committee. In many organisations, there will not be a need to establish a new risk management committee. Risk management responsibility could be allocated to an existing committee or the responsibility for risk management could be a matter that is specifically included in those matters reserved for the board. The important point is that responsibility for risk management is explicitly allocated to a committee.

### **AIRMIC and IRM Recommendations**

AIRMIC and the IRM suggest that the range of actions that an organisation needs to introduce in order to ensure that an adequate risk management framework is in place are as set out in Appendix A of *A structured approach to enterprise risk management (ERM) and the requirements of ISO 31000*.

AIRMIC and the IRM suggest that the UK Governance Code should require organisations to introduce an appropriate risk architecture, strategy and protocols. The Turnbull guidance should then be enhanced to describe what this involves in practice. The necessary actions are presented in detail below and represent the full scope of what is required and the table below could form the basis of the advice that is set out in the revised Turnbull guidance.

The suggested scope of what is required is set out under the headings of risk architecture, strategy and protocols, as follows:

<b>Risk architecture</b>	
<ul style="list-style-type: none"><li>• Statement produced that sets out risk responsibilities and lists the risk-based matters reserved for the Board</li></ul>	
<ul style="list-style-type: none"><li>• Risk management responsibilities allocated to an appropriate management committee</li></ul>	
<ul style="list-style-type: none"><li>• Arrangements in place to ensure the availability of appropriate competent advice on risks and controls</li></ul>	
<ul style="list-style-type: none"><li>• Risk-aware culture exists within the organisation and actions are in hand to enhance the level of risk maturity</li></ul>	
<ul style="list-style-type: none"><li>• Sources of risk assurance for the Board have been identified and validated</li></ul>	
<b>Risk strategy</b>	
<ul style="list-style-type: none"><li>• Risk management policy produced that describes risk appetite, risk culture and philosophy</li></ul>	
<ul style="list-style-type: none"><li>• Key dependencies for success identified, together with the matters that should be avoided</li></ul>	
<ul style="list-style-type: none"><li>• Business objectives validated and the assumptions underpinning those objectives tested</li></ul>	

<ul style="list-style-type: none"> <li>• Significant risks faced by the organisation identified, together with the critical controls required</li> </ul>	
<ul style="list-style-type: none"> <li>• Risk management action plan established that includes the use of key risk indicators, as appropriate</li> </ul>	
<ul style="list-style-type: none"> <li>• Necessary resources identified and provided to support the risk management activities</li> </ul>	
<b>Risk protocols</b>	
<ul style="list-style-type: none"> <li>• Appropriate risk management framework identified and adopted, with modifications as appropriate</li> </ul>	
<ul style="list-style-type: none"> <li>• Suitable and sufficient risk assessments completed and the results recorded in an appropriate manner</li> </ul>	
<ul style="list-style-type: none"> <li>• Procedures to include risk as part of business decision-making established and implemented</li> </ul>	
<ul style="list-style-type: none"> <li>• Details of required risk responses recorded, together with arrangements to track risk improvement recommendations</li> </ul>	
<ul style="list-style-type: none"> <li>• Incident reporting procedures established to facilitate identification of risk trends, together with risk escalation procedures</li> </ul>	
<ul style="list-style-type: none"> <li>• Business continuity plans and disaster recovery plans established and regularly tested</li> </ul>	
<ul style="list-style-type: none"> <li>• Arrangements in place to audit the efficiency and effectiveness of the controls in place for significant risks</li> </ul>	
<ul style="list-style-type: none"> <li>• Arrangements in place for mandatory reporting on risk, including reports on at least the following: <ul style="list-style-type: none"> <li>○ Risk appetite, tolerance and constraints</li> <li>○ Risk architecture and risk escalation procedures</li> <li>○ Risk-aware culture currently in place</li> <li>○ Risk assessment arrangements and protocols</li> <li>○ Significant risks and key risk indicators</li> <li>○ Critical controls and control weaknesses</li> <li>○ Sources of assurance available to the Board</li> </ul> </li> </ul>	

Needless to say, AIRMIC and the IRM would be it pleased to be involved in the development of advice to assist organisations with the implementation of the actions set out in the table above.

**Paul Hopkin**

**Technical Director  
AIRMIC  
6 Lloyd's Avenue  
London EC3N 3AX**

**Director  
Institute of Risk Management  
6 Lloyd's Avenue  
London EC3N 3AX**

**e-mail: [paul.hopkin@airmic.co.uk](mailto:paul.hopkin@airmic.co.uk)**

**Tel: 020 7680 3081**

**4 March 2010**