February 21, 2018

Catherine Horton
Financial Reporting Council
8th Floor
125 London Wall
London
EC2Y 5AS

COMMENT LETTER – DECEMBER 2017 DRAFT UK GOVERNANCE CODE

Thanks for the opportunity to provide comments on the December 2017 Proposed Revisions to the UK Governance Code. As an international member of the London based ACCA Global Governance Forum I have been participating in a robust discussion of the proposed changes. A major theme of the discussions has been on the question of how well, in practice, has the UK Governance Code performed on the goal of preventing major harm to stakeholders and, most importantly, is this revision of the Code likely to do a better job addressing current and past corporate governance regulation performance problems.

I believe most people would consider preventing significant harm to shareholders and other important stakeholders a primary purpose of the FRC and, by extension, the UK Governance Code. My view is that the current revision of the Code appears to focus on laudable social aims, not FRC's primary purpose, perhaps by design. I believe that prior UK Governance Codes and this draft suffer from what are sometimes termed "fatal flaws" – flaws that result in significant and sometimes fatal damage to stakeholders. It is very important to note that I consider the UK's governance code to be the best in the world currently. One of the fatal flaws in my view is in section 4 of the Code – Audit, Risk and Internal Control – the section in the December 2017 UK Governance Code revision the FRC has concluded requires no changes. This flaw impacts many other sections of the Code. This is quite disturbing. A large percentage of experts in the governance field are of the view that failures like Carillion, and tens of thousands like it over the past 30 years globally, are closely linked to governance oversight failings of boards and, specifically, board oversight of risk.

My comments are drawn from the following: 1) perspective of an experienced global risk and assurance consultant and forensic/litigation accountant; 2) as an outside expert who has worked very closely with earlier versions of the UK Governance Code as a board/CEO risk and assurance advisor from 2012 to 2016 for a FTSE 250 company; 3) my participation as a member of the ACCA Global Governance Forum; and 4) 30 plus years of work around the world in the field of corporate and risk governance with Fortune 500 companies and public sector departments. A sample of my work researching causes of major corporate governance failures globally and my prescriptions how to prevent future breakdowns published in the International Journal of Disclosure and Governance is attached for your information. Be warned however - it is a fairly lengthy and rigorous analysis of root causes of corporate governance failures and what needs to change - not a quick read. I have also written for the London School of Economics describing what I consider to be major regulatory failures (much shorter article copy attached), as well as Ethical Boardroom, Conference Board Director Notes, and Harvard and Columbia law and governance blogs on what needs to change if better corporate governance is the aim.

In my opinion the "fatal flaw" in the current UK Governance code is that a large percentage of UK companies and boards focus, very likely with prudent legal advice, on whether they have done/followed processes/steps prescribed in the UK Governance code (i.e. "ticking the box); not focusing on the real desired end result – sound corporate oversight; fair, balanced and understandable disclosures to stakeholders; and effective board oversight of significant risks that threaten the top value creation and preservation objectives. Many companies all over the world point to the existence of an annual/semi-annual risk register process as evidence of an effective risk management framework. It isn't clear from FRC 2016/2017 public disclosures whether the FRC itself uses a risk centric/risk register approach to risk management. Risk registers have failed in many instances to provide boards with the type of information necessary to oversee management's process to manage risk to top value creation and preservation objectives and effectively oversee management's risk appetite. Risks when divorced from the objectives they relate become an exercise done largely to satisfy regulators, not make better decisions. There is even some evidence that the UK Governance Code may be one of the major reasons risk centric/risk register methods have proliferated globally over the last decade - largely as a placating mechanism to pacify securities and bank regulators; not make real improvements in board risk oversight.

On another front, the current UK Code also requires companies to simply indicate whether they do, or do not, have an internal audit function with little real identification of what an effective internal audit function should accomplish in terms of end results. This may be because the FRC itself doesn't see the need for a robust and dedicated internal audit function (see quote below); in spite of the enormous importance of FRC's role to the wellbeing of UK society and long term economic success. The fact the FRC is relatively small in terms of budget and number of employees is not relevant in my view given FRC's enormously important role in terms of stakeholder protection. The fact that Grant Thornton, the current firm engaged by the FRC to perform a limited, perhaps even token, internal audit function for FRC, is regulated by the FRC raises other issues beyond the focus of this letter.

Internal Audit - The FRC has not established a dedicated internal audit function because of its size and nature. The Committee reviewed the approach during the year and concluded that for 2016/17 it should be retained. On that basis, Grant Thornton (an independent third party) was reappointed to carry out the internal audit reviews. The Committee will review whether an internal audit function should be introduced for 2018/19. Throughout the year the Committee received reports on progress against the internal audit plan. (FRC 2016/2017 Annual Report p.49)

An excerpt from my attached article on regulatory failure published in the London School of Economic's Center For Risk and Regulation on the impact of UK Governance Code guidance is below:

Although the UK has opted not to follow the US decision to require costly and ineffective opinions on accounting control effectiveness from CEO s, CFOs, and external auditors, it has been equally remiss in not carefully studying the costs and actual effectiveness of regulatory responses in the UK. Hundreds of UK companies now religiously update their "risk registers" each year to comply with rules calling for reports on the effectiveness of their risk management processes. There is little evidence that slavish adherence to the widespread practice of developing and maintaining risk registers is, in fact, resulting in better corporate governance. The only good news is that many of those companies creating and maintaining risk registers are spending a small fraction of the money public companies in the US are spending on complying with SOX 404 requirements to report on control effectiveness.

Simply put the desired outcome of effective corporate risk governance should be:

Boards of directors have a materially reliable picture of the current state of risk related to the top value creation and preservation objectives to allow them to assess if the current retained risk status being accepted by management is, or is not, within the board's risk appetite/tolerance.

Board Chairs should have to describe simply, candidly, and in reasonable detail in annual reports how they believe the board satisfies this outcome.

Current ERM, internal audit, and strategic planning methods used by a large percentage of organizations today do a poor job on this core risk governance effectiveness dimension. A full presentation of what needs to change to address this problem is beyond the remit of a short comment letter. My most recent Conference Board Director Notes article – "Board Oversight of Long Term Value Creation and Preservation: What Needs to Change?" provides an overview of the changes I believe are necessary for boards to do a better job overseeing risk. A copy of that article is also attached for your information. I would be happy to provide additional details on the changes I think are necessary to the UK Governance Code and support documentation if the FRC is interested.

In closing, I encourage the FRC to revisit its decision to make no changes to section 4 of the UK Governance Code and supporting guidance. If the significant deficiencies that exist today remain in Section 4 of the Code and supporting guidance, no one should be surprised if many more large and important UK companies like Carillion fail and board members of those companies quite sincerely claim they had no idea just how bad it really was!

Yours sincerely,

Tim Leech FCPA CIA CRMA

Managing Director
Risk Oversight Solutions Inc.