The Development of Systems of Internal Control and Risk Management in Higher Education in England: An Analysis of Nature, Roots and Relevance

Jane Broadbent

The Development of Systems of Internal Control and Risk Management in Higher Education in England: An Analysis of Nature, Roots and Relevance

Introduction

It has been argued that we live in a 'risk society' (Beck, 1992, 2004) and that we are engaged in the 'risk management of everything' (Power, 2004). Given this all pervading presence of risk and risk management it is, therefore, not surprising that higher education (HE) is also preoccupied with these issues. Despite the realisation that '...the meaning of risk remains indeterminate' (Beck, 2004: 2) the importance of this elusive concept and its management has become, the central and all encompassing concern in the internal control of all organisations (Power, 2004: 24). This applies as much to Higher Education Institutions (HEIs) as to any other organisations. In HE, as Middlehurst (2004) makes clear, there have been extensive changes over the last few decades in the 'internal governance' of HEIs. Internal governance, to Middlehurst, is closely aligned to, if not the same as, the internal control of organisations. The development of the latter to focus on risk management, and, the way this in turn has become a codified and standardised form of risk management that can be made public and transparent, is a more recent and, as this paper will argue, a potentially highly significant and damaging development in HEIs. This paper analyses these developments generally and specifically in HEIs giving particular emphasis to the way the '....private world of organisational internal control systems has been turned inside out, made public, codified and standardised and repackaged as risk management' (Power, 2004: 28).

Few would dispute the need for internal control of organisations, yet its path to be repackaged as risk management of the sort described in the above quote is complex. As Power (2007: 7) makes clear the process of organising in any formal sense '..... has always existed in a

fundamental, even trivial sense, to manage uncertainty'. 'Uncertainty management', or trying to make the unknown more knowable and manageable so that aspirations can be achieved is one of the key reasons why organisations exist and function and why people are actively involved in them. Uncertainty management is central to internal control, or, put another way: 'Organizing and managing are fundamentally about individual and collective human efforts to process uncertainty' (Power, 2007: 8). This 'processing' results in trying to make 'uncertainties' into 'risks', which can be managed, even though as Froud (2003) suggests, these terms have a 'Humpty Dumpty' sense to them (i.e. '...when I use a word.....it means just what I chose it to mean....neither more nor less' (Froud, 2003: 569)). Such a seemingly light hearted comment has a serious and insightful edge to it. Risk and risk management, like uncertainty and uncertainty management, are social constructs that can be shaped in particular ways and gain powerful social acceptance at particular points of time. More specifically a particular construction which has wide appeal is that risk management involves '....the organisational displacement of radical uncertainty....into something describable and, in aspiration, manageable.' (Power, 2004: 31). The general point is that to be able to describe something is to make whatever is being described transparent and therefore more knowable to more people. To be able to describe something does not necessarily mean that it is possible to manage whatever is being described. However, one common construct of what it means to be 'describable', often associated with risk, is being able to put a 'calculable probability on a future event occurring' (Broadbent, Gill and Laughlin, 2008: 42). In terms of social acceptance, if calculation is possible, it is deemed to increase the perceived possibility of making the 'describable' future indeed more 'manageable'[1].

[1] This is, however, only a perception. The simple allocation of numbers alone (i.e. without these numbers being meaningful in complex empirical ways) will not necessarily, or even actually ever, mean that manageability is increased. But due to the 'tyranny of numbers' (Boyle, 2000) there is a commonly, but falsely, held belief that

The paper seeks to trace the way internal control issues have become reduced to a particular codified, publicly transparent form of risk management *systems* notably in the private sector but also in the public and voluntary (third) sectors and, therefore, also in HE in England. Thus the paper will not dwell on trying to provide an unambiguous definition of internal control or risk management or even explore the distinction between 'primary' (more 'operational') and 'secondary' (more 'reputational') risks and risk management or how the latter affects the former, which Power, Schyett, Soin and Sahlin-Anderson (2009) explore. This paper, however, does not directly address these definitional arguments, but rather concentrates on the way, through current guidance and codes, such distinctive risks can be constrained when risk management is '....turned inside out, made public, codified and standardised' (Power, 2004: 28) and become a system. Put simply the paper does not question, and, in fact, is built on the assumption that operational and reputational risks and their management are important for all organisations, including HEIs. This, however, is not the main focus of the paper, rather it is with the way internal control issues have become a particular codified, publicly transparent form of risk management *system* and the way this has created a questionable way of thinking for all organisations, not least HEIs.

Codification and standardisation of risk management has become a central part of corporate governance reforms in the UK and across the world. As the focus of this paper is HE in England, concentration will be primarily given to these reforms in the context of the UK, even though this is not just a UK-centric development. Key in these specific risk developments in the UK is the thinking contained in the highly influential Turnbull Reports

allocating numbers to something makes whatever is measured more meaningful and exact and, in the context of the current argument, more manageable.

(1999, 2005) on internal control and the Smith Report (2003) on internal audit which have highlighted the importance of regulating and auditing both the design as well as information about internal control processes, and the risk management systems, which constitutes a key, if not the key, part of these processes. These Reports were developed for the private sector and their requirements are now part of the Combined Code of Corporate Governance (Financial Reporting Council (FRC), 1998; 2003; 2006; 2008), and the subsequent major review that is underway into this Code (FRC, 2009) which, amongst other concerns, forms a model set of requirements for the way private sector organisations are to behave in terms of their internal control arrangements. This form of regulation moves away from a direct 'command and control' regulatory process to one that is generically referred to as 'enforced self-regulation' (Ayres and Braithwaite, 1992; Hutter, 2001) which does not tell organisations what to do as such but attempts to target internal processes such that the checks and balances are in place to create the potential to achieve the outcomes intended.

The nature and reporting of internal control/risk management requirements in these UK Codes are like a mirror which reflects but also moulds similar recommended processes advanced notably in the United States of America, as contained in Reports from the Committee on Sponsoring Organizations of the Treadway Commission (COSO) (COSO, 1992, 2004, 2009) and the 2002 Sarbanes-Oxley Act. In Europe, they are to be found in the recommendations of the Basle Committee on Banking Supervision (BCBS), who developed a 'Framework for the Evaluation of Internal Control Systems (BCBS, 1998, 2001)[2].

[2] With the recent banking crisis it is interesting to note that these regulations have been in place in Europe since 2001. Clearly their effectiveness will be under considerable critical scrutiny and likely revision over the next few years once the immediate crisis is past. At the time of writing (2010), certainly in the UK, this has started to occur with a number of key reports appearing proposing major changes to the regulation of financial services.

These developments are also mirrored in the public services through a number of 'good governance codes'. This is apparent in the good governance code issued by the Chartered Institute of Public Finance and Accounting and the Office of Public Management (CIPFA and OPM, 2004) for the public services in general, for the voluntary ('third') sector by the National Council for Voluntary Organisations (NCVO, 2005) and for Departments of Government by HM Treasury (HM Treasury, 2005).

In terms of internal control and risk management and its increasingly systematised nature, the Turnbull Reports and Smith Report have been highly influential in the private sector *and* public sector *and* voluntary sector in the UK *and* internationally. Given the importance of these Reports, particularly the Turnbull Reports, for the Governance Codes, and the resulting codified and transparent risk management systems they generate, Power (2004: 24) refers to this collective set of changes colourfully as the 'Turnbullisation of organisational life'.

HE is subject to this 'Turnbullisation of organisational life'. The Higher Education Funding Council of England (HEFCE), which funds and oversees the sector on behalf of the Department of Business, Innovation and Skills (DBIS)[3] is itself subject to these processes and has made this thinking a requirement for all HEIs. This was communicated in a Circular Letter (24/00) to all vice-chancellors and principals and contained a requirement that these risk management systems should be fully operational by 2002/03. This initial instruction has been followed by a raft of further information, requirements and good practice guides etc. HEFCE's own risk management system is contained in its Assurance Framework

[3] DBIS is the latest Department of Government to be in charge of HE. HE has been in 3 different Departments over the last few years – originally in the Department for Education and Science (DfES) and then in the Department of Innovation Universities and Skills (DIUS) before moving to DBIS. Whether DBIS is the final 'home' for HE remains to be seen.

(http://www.hefce.ac.uk/AboutUs/riskman). HEFCE's risk management is complex due to its reliance on '.....universities and colleges and other organizations to help us deliver our objectives' (Paragraph 31 HEFCE Assurance Framework (http://www.hefce.ac.uk/AboutUs/riskman)). HEFCE's risk management is, therefore, interlocked in complex ways with the HEIs' own risk management processes. This paper explores not only this complex interaction but analyses HEFCE's and HEIs' separate risk management, codified and transparent, systems. This analysis will bring out not only the nature of these systems in HE but also demonstrate that these are another example of the 'Turnbullisation of organisational life' with its dominant emphasis on procedure, codification and transparency. It will also critically analyse this development in the conclusion of this paper.

The remainder of the paper is divided into two major sections followed by a reflective, analytical conclusion. The next, second, section explores what is meant by the 'Turnbullisation of organisational life' notably exploring the nature of the Turnbull Reports and the Smith Report, tracing their connections to wider international developments, and the way, through the private sector Combined Code of Corporate Governance and the public services Codes, they have given a particular direction and emphasis to internal control and risk management practices in all UK organisations in terms of increasing procedure, codification and transparency requirements. The third section looks at these dynamics in HE, tracing the way the thinking in the second section has influenced relevant guides, codes and practices in HE and the way this has led to codified and transparent forms of risk management systems in HEIs. Finally, the conclusion draws the analysis together and makes a number of reflective and critical comments about these developments in HE, speculating that despite the extensive introduction of risk management systems in HE, in the codified

form highlighted in this paper, they might actually lead to the 'risk management of nothing' as Power (2009) argues is the case in the private sector.

The 'Turnbullisation of Organisational Life': Tracing the Codification and Transparency Developments in Internal Control and Risk Management

(i) Private Sector Governance Changes in Relation to Internal Control

As the main focus of this paper is with the UK, the place to start this analysis is with developments in 'governance codes' from the Cadbury Report (1992) – named after the Chair of the Committee, Sir Adrian Cadbury. The Cadbury Committee was formed in 1990 following some major financial scandals that occurred in the late 1980s, notably, but not exclusively, in the management of the companies and pension funds of Robert Maxwell's corporate empire. The Cadbury Report's (1992: 11, Paragraph 1.2 and 1.3) recommendations were:

> '....focussed on the control and reporting functions of boards (of directors – authors' addition), and on the role of auditors.....At the heart of the Committee's recommendation is a Code of Best Practice designed to achieve the necessary high standards of corporate behaviour'.

Whilst Cadbury's brief was restricted '..to review those aspects specifically related to financial reporting and accountability' he and his Committee were well aware of the wider intentions to '...contribute positively to the promotion of good corporate governance as a whole' (Cadbury Report, 1992: 11, Paragraph 1.2).

The overall emphasis of Cadbury and all subsequent thinking on corporate governance in the UK has three key characteristics. First, as already noted, Cadbury changed the nature of regulation away from a 'command and control' approach to one based on 'enforced self regulation'. Hutter (2001: 380) describes the latter, as regulation which '...very explicitly

attempts to co-opt the regulatory potential of the corporation'. In other words the Cadbury model provides direction on a range of internal recommendations on how organisations should behave and attempts to ensure this occurs through requiring reports and assurances about compliance. As a result accountability about practices and audit of these practices, which can provide these assurances, are a central part of governance. Second, in the spirit of 'enforced self regulation', the requirements are not legal requirements as such, but are expressed through Codes where the overarching requirement is a 'comply or explain' approach to adoption. Compliance, in this sense, is expected and needs to be made transparent as does the assumed less normal cases when compliance does not occur where an explanation is required to be given. Third, the focus of these Codes are the boards of directors who are assumed to 'run the venture' (Editorial, 2000: 289) as the Editorial of *Corporate Governance: An International Review* graphically portrays the significance of boards.

The Cadbury Report set the scene for concerns with internal control and risk management, yet the recommendations of the Committee were limited. Despite this limitation, what was said has provided, as with so many other areas, a marker for future developments in the Combined Code as to how these issues should be dealt with. In this connection the Cadbury Report (1992) made a number of key points which are worth recounting in full to provide a flavour of the emphasis of the Committee's thinking:

> 'Since an effective internal control system is a key aspect of the efficient management of a company, **we recommend** that the directors should make a statement in the report and accounts on the effectiveness of their system on internal control and that the auditors should report thereon.
>
> The Committee is convinced that an effective internal control system is an essential part of the efficient management of a company. We have already recommended that directors should report on the effectiveness of their system of internal control, and that the auditors should report on their statement. A great deal of detail is now necessary to

develop these proposals and **we recommend** that the accountancy profession, in conjunction with representatives of preparers of accounts, should take a lead in:

(a) developing a set of criteria for assessing effectiveness;
(b) developing guidance for companies on the form in which directors should report: and
(c) developing guidance for auditors on relevant audit procedures and the form in which auditors should report.'

(Cadbury, 1992: 27 and 41, Paragraphs 4.31, 4.32 and 5.16; Emboldened phrase in original)

Spira and Page (2003: 650) captures well this emphasis when they point out that '....from Cadbury onwards, internal control has clearly been seen as a system'. By this they mean that internal control is something that can be systematised, codified, audited and made transparent.

Since the 1992 Cadbury Report a range of other Reports have addressed different refinements of the resulting Cadbury Code, leading to various versions of a Combined Code of Corporate Governance (Financial Reporting Council, 1998, 2003, 2006 and 2008)[4]. Rather than focus on the changing nature of all of the Combined Code this paper will concentrate on the way Cadbury's original specific recommendations on internal control have been built upon and developed. Key in this regard relates to the Hampel Report (1998), the Turnbull Reports (1998 and 2005) and the Smith Report (2003).

The Hampel Report (1998) downplayed issues related to accountability and transparency, but built important linkages between internal control and risk assessment. The underlying view of the Hampel Report (1998:7, Paragraph 1.1) was that the value of: '...corporate governance lies in its contribution both to business prosperity and to accountability', and that, in their view, in the UK, the latter has predominated but that they: '...wish to see the balance

[4] Even the wide ranging review of the Combined Code that is underway at the moment (Financial Reporting Council, 2009) which closes in March 2010 continues to reflect the concerns of the Cadbury Report.

corrected.... the emphasis on accountability has tended to obscure a board's first responsibility – to enhance the prosperity of the business over time'. As it transpired the 1998 Combined Code, that came from the Hampel Report, did not follow this advice for radical downplaying the importance of accountability and transparency. In this connection the pertinent paragraphs of the Combined Code (1998) in relation to internal control are more Cadbury than Hampel:

> 'The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets' (Combined Code (1998) Principle D.2).
> 'The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management.' (Combined Code (1998) Provision D.2.1).
> 'Companies which do not have an internal audit function should from time to time review the need for one.' (Combined Code (1998) Provision D.2.2)

Whilst internal audit remains a bit 'free floating' in the 1998 Combined Code, what was, much clearer in the Code (in Provision D.2.1) was the Hampel Report's explicit links between risk management and internal control.

The first Turnbull Report (1999) made the links between internal control and risk management even stronger than had been the case with the 1998 Hampel Report, whilst the second Turnbull Report (2005) retained this linkage, but, as will be apparent in the following sub-section, created an increasing concentration on codification, audit and transparency in these developments. Under a title 'Elements of a sound system of internal control' the 1999 Report notes:

> 'An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
> - facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial compliance and other risks to achieving the company objectives. This includes the safeguarding

of assets from inappropriate use of or from loss and fraud, and ensuring that liabilities are identified and managed;
    - help ensure the quality of the internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely relevant and reliable information from within and outside the organisation.
- help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business. (Turnbull Report, 1999: 7, Paragraph 20)

(ii) Intensifying Codification and Transparency on the Nature of Risk Management Systems Through Audit Processes

The 1999 Turnbull Report did not make clear the linkages between audit and internal control processes, which, as will become clear below, gives the internal control/risk management effectiveness judgement a particular auditable, codified emphasis. So, in relation to 'reviewing the effectiveness of internal control', the 1999 Turnbull Report doesn't require a particular audit emphasis but makes clear that reviewing:

> '.....the effectiveness of internal control is an essential part of the board's responsibilities.....The role of board committees in the review process, including that of the audit committee, is for the board to decide..... To the extent that the designated board committees carry out, on behalf of the board, tasks that are attributed in this guidance document to the board, the results of the relevant committees' work should be reported to, and considered by, the board. The board takes responsibility for the disclosure on internal control in the annual report and accounts.' (Turnbull Report, 1999: 8, Paragraphs 25 and 26).

This doesn't rule out the involvement of internal audit in this review but doesn't make it a necessity.

However, the second Turnbull Report (2005) changed this emphasis in two ways. First, even though the definition of internal control remains the same as in the 1999 Report, it was seen as a *system* the central focus of which was risk management: 'A company's *system* of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives'. (Turnbull Report, 2005: 3, Paragraph 1) (emphasis added). Second, all

reference to audit is removed completely in the 2005 Turnbull Report and reference is made to the Smith Report (2003) that takes precedence over any comment on the importance of audit.

The Smith Report's (2003) recommendations on audit focus, primarily, on an expanded role for the audit committees of boards of directors, initially required by the 1998 Combined Code. The Smith Report (2003: Paragraph 2.1: 6) recommended a major shift in the responsibilities of audit committees, one of which involved reviewing the '....company's internal financial control system and, unless addressed by a separate risk committee or by the board itself, risk management system'. The expected role of the audit committee in assessing risk management and internal control is clarified as follows:

> 'The audit committee, in the absence of other arrangements, eg a risk committee[5], should assess the scope and effectiveness of the systems established by management to identify, assess, manage and monitor financial and non financial risks..... Except where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should receive reports from management on the effectiveness of the systems they have established and the results of any testing carried out by internal and external auditors..... *Except to the extent that this is expressly dealt with by the board or risk committee, the audit committee should review and approve the statements included in the annual report in relation to internal financial control and the management of risk.*' (Smith Report, 2003: 11, Paragraphs 5.5 to 5.7) (Emphasis Added)

On the place of the audit committee, as a sub-committee of the board of directors in a 'unitary board structure[6]' (Smith Report, 2003: 24, Paragraph 18 et. seq.), the Report makes the following observations:

[5] At this point the Smith Report inserts a footnote stating that 'The board may set-up other sub-committees to deal with the requirements of the Turnbull report on internal controls' (Smith Report, 2003: 11, Footnote 4).

[6] The 'unitary board structure' is in contrast with the more Germanic 'dual board structure' where the second board is a supervisory board (cf. Weimer and Pape, 1999; Jackson and Moerke, 2005; Dore, 2005; Mintz, 2005; Solomon, 2007). The unitary board structure is dominant in the UK, America and other Anglo-Saxon English-

> 'We believe that an audit committee separate from the board would be less effective than the conventional audit committee established as a sub-committee of the board.....Audit committee members are not, and are not intended to be, independent of the board. But they must be independent of the executive management.....We attach the utmost importance to the idea of audit committee independence within the unitary board structure.....Audit committees should take care not to duplicate the role of the executive or of the auditors. In all ordinary circumstances, an audit committee should seek to satisfy itself that the executive and the auditors (internal and external) are carrying out their roles properly and effectively, not to step in to do it themselves.....So there is a delicate balance to be stuck between a detached oversight role as the normal mode of operation and a willingness to become closely involved when things may be going wrong.' (Smith Report, 2003: 24 and 25, Paragraphs 19 to 24)

The Smith Report, along with a range of other Reports, played a major part in reshaping the 1998 Combined Code into a new Combined Code in 2003. The 2003 Code remains as the latest major set of requirements on private sector corporate governance even though there have been minor changes to this Code in 2006 and 2008[7]. The 2008 Combined Code requirements on internal control (C.2) and on audit committees and auditors (C.3) are identical with the 2003 and 2006 versions of the Codes. Requirement C.2.1 on internal control is not dissimilar to the 1998 Code but with an important, certainly for the codification argument of this paper, addition of the word 'systems' when mentioning risk management:

> 'The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.' (Combined Code, 2008: Main Principle C.2)
> 'The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management *systems.'* (Combined Code, 2008: Code Provision C.2.1 (emphasis added))

speaking countries. The unitary board model has also been implemented in the public services codes although, as Broadbent, Gallop and Laughlin (2009) argue, this creates all manner of problems in this context.

[7] A further substantive change in the Combined Code, to try to address some of the problems that the recent fiscal crisis has generated, is currently being developed and is at the time of writing currently out for consultation (Financial Reporting Council, 2009).

There are, however, considerable changes in relation to the audit committee and auditor code provisions in the 2003 Combined Code, the latest draft of which is in 2008 (Financial Reporting Council, 2008) relative to the 1998 version. Whilst the Main Principle (C.3) remains the same as the 1998 Main Principle, the two Code Provisions are now seven. The second Code Provision (C.3.2), on the main role and responsibilities of audit committees gives virtually exclusive responsibilities over the review of internal control and risk management systems to the audit committee:

> To review the company's internal financial controls and, unless expressly addressed by a separate board risk committee composed of independent directors, or by the board itself, to review the company's internal control and risk management systems.'
> (Combined Code, 2008: Code Provision C.3.2 Bullet Points 1& 2)

Recounting of this trajectory in governance arrangements provides evidence of the way risk management has gained prominence and how the various interventions have led to more 'standardised' (Power, 2007: 66) practices. Whilst the active involvement of audit committees in the effectiveness review in and of itself alone The very fact that audit committees are actively involved in the effectiveness review of internal control/risk management systems of itself does not lead inevitably to a particular standardised, codified and defendable form of these systems. However, when coupled with four other dynamics that Power (2007: 66 et seq) highlights the audit committee involvement does make what are widely referred to as 'enterprise risk management' (ERM) systems, both increasingly important but also more and more codified and standardised.

The first force is the internationalisation of this standardisation process and the way this influences national and organisational thinking. This is led, primarily, by the USA and

notably through the reports of the Committee on Sponsoring Organizations of the Treadway Commission (COSO) (COSO, 1998, 2004). To Power (2007: 76) the 'COSO framework for internal control .....was one of the first systematic conceptual frameworks and standards for internal control'. The 2004 COSO publication 'codifies the discrete elements or stages of an ideal-typical ERM process which owes much to cybernetic systems thinking' (Power, 2007: 77). It has become the international guide on how to design an ERM system. The wide adoption of its thinking in the UK and in most other countries has demonstrated the power of some ideas to be highly influential internationally.

The second force Power (2007: 82 et seq) highlights is the rise of Chief Risk Officers (CROs) whose job is to manage the ERM system. CROs now have 'strategic significance' (Power, 2007: 82) in most private sector organisations and 'must work hard to create representations of their own effectiveness and performance' (Power, 2007: 83). This leads, in the view of Power, inevitably to increasing pressure towards codification and transparency of the ERM so that CROs can show they have a clear role and their effectiveness and performance can be made transparent and evaluated.

The third force is the increasing importance of 'risk-based regulation' (cf. Black, 2005). As indicated above there has been a move from 'command and control' forms of regulation to an 'enforced self-regulation' model, but 'risk-based regulation' takes the regulatory process into new dimensions. To Black (2005: 514) '....risk-based regulation will both fuel and be fuelled by the current vogue for focusing on firms' internal controls in the successful operation of regulatory regimes.' Put simply if effective ERM systems are in place and functioning well then the view is that the regulators can reduce their regulatory pressures whether of a command and control or enforced self-regulatory form. This creates pressure on organisations

to demonstrate that their ERM system is indeed effective which, in turn, creates an inevitable further pressure, according to Power, on making sure these are codified, transparent and audited so the regulators can see clearly whether in their judgement they are effective. Needless to say this whole process creates significant risks for the regulators if in fact the organisations, despite the perception that the ERM system is effective, get into serious trouble. Given the banking sector across the world have been leading the way in this approach to ERM system design and regulation, with a resulting reduction in banking regulation, due to levels of questionable trust in the messages coming from the clearly codified and transparent ERM systems, it is certain to be a model that is likely to come under intense scrutiny in the future. That notwithstanding 'risk-based regulation' has been yet another force, to Power, in making the ERM systems more codified and transparent.

A fourth force, which has a very direct audit linkage, has been the emergence of 'business risk auditing' in the work of external auditing and the effects of this on internal audit and ERM design. As Knechel (2007: 386) makes clear the 1990s saw audit clients '...exerting tremendous pressure on auditors to reduce fees'. The solution was to move to a 'business risk' model for external auditing. Knechel (2007: 389) encapsulates the logic for this in the following way:

> '.....client risk management could provide a basis for refocusing the audit process and to help control costs that were increasingly under pressure.....Companies that had effective risk management processes in place were arguably of lower risk from an audit perspective and could be audited with fewer resources. Of even more potential importance, perceived gaps in risk management at a client could become fodder for management letter comments.....and might yield lucrative opportunities for spin-off non-audit services.'

Management letters are an important part of external audits in the private sector. They are private letters from the external auditors to boards of directors with reflections on areas,

following their audit, where improvements are deemed to be needed. Whilst these letters are indeed private and do not have to be followed it would be a foolish organisation that did not take the suggestions seriously and do something about whatever is raised before the next audit takes place. More generally the move to business risk auditing, taking aside the potential risks for auditors who are similarly vulnerable to those described about in relation to risk-based regulation, also creates pressure, according to Power, in making ERM systems more codified and transparent. There is a clear dynamic for this, since the more an organisation can demonstrate ERM system effectiveness to the auditors in the way *they* judge effectiveness then the less work they need to do and the less fees the organisation has to pay. If, however, the ERM system is not auditable in this way, any negative comments made in the management letter about this, will tend to make the ERM system more auditable in future years.

So taken together these governance changes and other forces coalesce to drive internal control and risk management to be codified, systematised and transparent in 'the Turnbullisation of organisational life' Power (2004: 24). Given all the other change agents it may be a little unfair to isolate the Turnbull Reports (1999, 2005) as the main driving force behind this systematisation and transparency process but they certainly played a major part.

The above developments have been focused primarily on private sector organisations but similar developments are apparent in the public services. The following section concentrates on HE to demonstrate this claim. But it is not just HE that is subject to this mirroring. As the introduction makes clear there are a number of generic codes that apply across the public sector as well as the voluntary ('third') sector. Space precludes a detailed explication of these

codes but they follow from and mirror the developments described above in relation to the private sector.

(iii)A Concluding Thought

In conclusion, this section has set out to do two things. First to show how internal control has become centrally important in the management of organisations and how this key concern has been '....turned inside out, made public, codified and standardised and repackaged as risk management' (Power, 2004: 28). Second, to demonstrate that this development occurs not just in private sector organisations but is apparent in *all* organisations. Whilst most of the developments have their origin in and are focussed on private sector organisations and are, arguably, more developed in this context, the public sector and voluntary ('third') sectors are pursuing mirror images of these developments. The following section explores this in more depth and detail in the specific context of HE.

Risk Management Systems in HE in England: An Analysis

Before exploring the nature of this 'mirroring' of private sector developments in HE in England[8] it is important to highlight a major distinctive difference in the regulatory arrangements in HE relative to those in the private sector. This relates to the key importance and role of the Higher Education Funding Council of England (HEFCE) in the regulation of HE, not just in England but in all regions of the UK, which have regional funding councils, the equivalent of which rarely exists in the private sector.

[8] Whilst the contents of this section have a particular focus on England much, if not most, of the developments described are applicable to other regions in the UK.

HEFCE has a regulatory role in HE that is unlike type of regulatory body in the private sector. In the private sector, committees, such as those chaired by Cadbury, Turnbull, Smith etc., are not regulatory institutions. Their reports feed into the design of the Combined Code on Corporate Governance for which the Financial Reporting Council (FRC) is responsible. The FRC is a permanent regulatory institution which has the responsibility and authority structure to ensure that all private sector organisations comply with the latest version of the Code. The only other similar regulatory institution in the private sector, in relation to governance requirements, is the Financial Services Authority (FSA) who provide additional governance regulation over specifically the financial services sub-sector of the private sector. This, however, is in addition to and certainly not in contradiction of the FRC's recommendation. The FRC remains the independent and only regulatory of governance requirements.

The FRC and FSA, however, differ in two important ways to HEFCE. First, the FRC and FSA have no financial resources to allocate on behalf of the owner shareholders of private sector organisations they represent. Second, whilst they act on behalf of owner shareholders they do not have direct accountable responsibility to these shareholders. HEFCE, on the other hand, has resources to allocate from the government of the day and is accountable for these resources and their use.

Where HEFCE and the FRC and FSA do have commonalities is in relation to the level of independence they have over their regulatory brief, even if the former is more constrained in its freedoms relative to the latter two regulatory bodies[9]. HEFCE, along with many similar

[9] The FRC is actually more independent than the FSA. The FSA was given statutory powers by the 2000 Financial and Markets Act. The FSA Board is appointed by HM Treasury and is accountable to Government

bodies in other areas in the public sector, is what is referred to as a 'Non-Departmental Public Body' (NDPB). HEFCE, as a NDPB, works:

> '.....within a policy framework set by the Secretary of State for Business, Innovation and Skills, but are not part of the Department of Business, Innovation and Skills (BIS). We have distinct statutory duties that are free from direct political control.'
>
> 'A non-departmental public body (NDPB) is an organisation that has a role in government processes, but which is not part of the Government or one of its departments. As a consequence, NDPBs work at arm's length from ministers, who are ultimately responsible for their effectiveness and efficiency.' (http://www.hefce.ac.uk/aboutus/history/)

NDPBs are therefore intermediary bodies between government and public sector organisations working within a 'policy framework' determined by Government with Government resources to be used to ensure such a framework is fulfilled. However, they are technically free of Government interference.

There are other differences between the private and public sectors, but, for now, the important point to stress is that, in the context of HE, HEFCE, as a NDPB, is the key regulatory body over HEIs[10]. The argument of this paper is that a key element in HEFCE's 'policy framework' specifically related to governance arrangements, in which it must work, and in its regulations over HEIs, 'mirrors' the private sector thinking, analysed in the previous section, which stresses the centrality of codified risk management and audit systems

---

through HM Treasury but remains independent from Government. The FRC, on the other hand, is the 'UK's independent regulator responsible for promoting confidence in corporate governance and reporting' (http://www.frc.org.uk/about/) with no direct links to Government although the latter still has the power to intervene in the workings of the FSA in the name of the 'public interest' (cf. Broadbent and Laughlin, 2005). HEFCE is closer to the FSA than the FRC in terms of Government links but differs from the FSA in terms of responsibility and authority to allocate substantial amounts of Government money.

[10] There are other NDPBs involved in particular aspects of the regulation and funding of HEIs. However, within the context of England, and also the UK more generally, few have more wide-ranging powers than HEFCE and, certainly, in terms of governance arrangements. It is for this reason that the focus in the following will concentrate on HEFCE.

and their accountability. The following explores this. The first sub-section clarifies the Government to HEFCE governance relationship and HEFCE's own governance processes to demonstrate the central importance that is given to risk management systems. The second sub-section explores similar themes in the governance relationship between HEFCE and HEIs and in the governance processes of HEIs.

(i)The Concentration on Risk Management Systems in Government Governance Requirements for and by HEFCE

Whilst specific and short term Government requirements of HEFCE are contained in an annual 'Grant Letter', the long term base for these requirements and the ongoing relationship between the two is specified in a Management Statement and in a Financial Memorandum. The current versions of these are dated June 2006 and remain in force. The Financial Memorandum (Department for Education and Science (DfES)[11], 2006a: Paragraph (P hereafter)1: 5) '....sets out in greater detail certain aspects of the financial framework within which HEFCE is required to operate'. However, the Management Statement '...sets out the broad framework within which the HEFCE will operate' (DfES, 2006b: P 1.1.2: 3). The Management Statement, therefore, provides the underlying framework for the Financial Memorandum, which is seen as a document that '....sets out in greater detail certain aspects of the financial provisions which the HEFCE shall observe' (DfES, 2006b: P 1.1.3: 4). The Management Statement, on the other hand, sets out:

> 'the NDPB's overall aims, objectives and targets in support of the sponsor Department's wider strategic aims and current Public Service Agreement;

[11] As indicated in the Introduction the DfES was the Department of Government responsible for HE in 2006. Since this time responsibility for HE has been shifted initially to the Department of Innovation, Universities and Skills (DIUS) and now to the Department of Business Innovation and Skills (DBIS). The 2006 Financial Memorandum and the Management Statement however remains in force at the time of writing (see http://www.hefce.ac.uk/aboutus/history/#statement).

> the rules and guidelines relevant to the exercise of the HEFCE's functions, duties and powers;
>
> the conditions under which any public funds are paid to the HEFCE;
>
> how the HEFCE is to be held to account for its performance.' (DfES, 2006b: P 1.1.2: 3)

Concentration, therefore, will be on the Management Statement in the following.

The Management Statement makes clear that it is technically not organisational units as such that are of key importance in relation to management responsibilities but rather an individual person called an 'Accounting Officer'. So it is made clear that:

> 'The Permanent Secretary, as the Department's principal Accounting Officer, is responsible for the overall organisation, management and staffing of the sponsor Department and for ensuring that there is a high standard of financial management in the Department as a whole' (DfES, 2006b: P 3.2.1: 7)

The importance of having an Accounting Officer (AO) for HEFCE, also applies to HEFCE itself:

> 'The principal Accounting Officer designates the Chief Executive of the HEFCE as the HEFCE's Accounting Officer, and may withdraw the accounting officer designation if he/she believes that the incumbent is no longer suitable for the role.' (DfES, 2006b: P 3.2.1: 7)

This peculiar personal responsibility of an individual rather than an organisation or institution is traceable to the 1866 Exchequer and Audit Departments Act and was reinforced again though the 2000 Government Resources and Accounts Act. AOs' responsibilities are considerable and, as will be discussed in more detail below, particularly concentrate on a responsibility to provide an 'account' of behaviour, a key part of which is a report on the 'effectiveness of internal control'. This mirrors the private sector thinking discussed in the previous section, but requires this of a particular individual rather than from the board (of directors). This is made clear in the draft letter of appointment for all AOs when

concentrating on their responsibility to produce 'resource accounts'. The only specific content point in relation to these 'resource accounts' reads:

> 'As part of the resource account you will be required to provide a statement on the effectiveness of your internal control systems (SIC). As risk sets the context for internal control it is important that the SIC process is firmly and clearly linked to the risk management process.' (http://www.hm-treasury.gov.uk/psr_governance_accountingofficers.htm)

The Management Statement clearly has a number of organisational requirements before getting to this key reporting responsibility of AOs, yet many of these responsibilities are largely a precursor to be able to provide the 'resource accounts', the important part of which is the report on the 'effectiveness of internal control'. Given its importance it is little wonder that AOs are cautious on the accuracy and legitimacy of the content of these 'resource accounts' and particularly so with regard to report on the 'effectiveness of internal control'. It is for this reason the 'resource accounts' need to be auditable and audited, and consequently codified and standardised, as will become apparent below.

Whilst stressing the central importance of the Secretary of State as the Accounting Officer, the Management Statement makes clear that there is a 'HEFCE Sponsorship and Governance Team' who shall 'advise the Secretary of State' (DfES, 2006b: P 3.3.2: 7). A key responsibility of the 'sponsoring team', in its 'support of the departmental Accounting Office' (DfES, 2006b: P 3.3.3: 8), is in relation to 'performance and risk management', namely to:

> '...monitor the HEFCE's activities on a continuing basis through an adequate and timely flow of information from the HEFCE on performance resource management and risk management, including early sight of any changes to the HEFCE's Statement on Internal Control as agreed in the annual year end timetable;
>
> ....address in a timely manner any significant problems arising in the HEFCE, whether financial or otherwise, making such interventions in the affairs of the HEFCE as the Department judges necessary;

> ....periodically carry out a risk assessment of the HEFCE's activities to inform the Department's oversight of the HEFCE; strengthen these arrangements if necessary; and amend the management statement accordingly. The risk assessment shall take into account the nature of HEFCE's activities; the public monies at stake; the body's corporate governance arrangements; its financial performance; internal and external auditors' reports, the openness of communications between the body and the Department; and any other relevant matters.' (DfES, 2006b: P 3.3.3: 8)

However, continuing the theme of giving responsibility to individuals, the Management Statement, even though it takes as given that HEFCE will be directed by a Board, similar to a private sector board of directors, gives particular attention to the role of the Chair of the HEFCE's Board. The Chair is 'appointed by the Secretary of State' (DfES, 2006b: P 3.4.1: 9) with an expectation that 'communications between the Board and the Secretary of State shall normally be through the Chairman' (DfES, 2006b: P 3.4.6: 10). According to the Management Statement, the 'Chairman has particular leadership responsibility' for:

> '.....ensuring that the Board develops a suitable strategy....ensuring that the Board, in reaching decisions, takes proper account of guidance provided by the Secretary of State or department.....promoting the efficient and effective use of grant funding, staff and other resources.....encouraging high standards of propriety....representing the views of the Board to the general public.....adhering to the corporate governance arrangements of the Council.' (DfES, 2006b: P 3.4.3: 9)

In relation to the final responsibility above, the Chairman must ensure that the Board '.....demonstrate high standards of corporate governance at all times, including by using the independent audit committee to help the Board to address the key financial and other risks facing the HEFCE' (DfES, 2006b: P 3.5.2: 10).

Apart from this continuing importance of individuals, the Board is of central importance, as is the case in the private sector, but so too is the role of internal and external audit and the Board's audit committee. This is made clear in a number of requirements in the Management

Statement. These link, in some cases, to a number of Government governance codes, the contents of which mirror private sector thinking. So, for instance, it is made clear that:

> 'The HEFCE shall establish and maintain arrangements for internal audit in accordance with the Treasury's Government Internal Audit Standards (GIAS).'
>
> 'The HEFCE shall set up an independent audit committee as a committee of its Board in accordance with the Cabinet Office's Guidance on Codes of Practice for Public Bodies and the Treasury's Audit Committee guidance.'
>
> 'The HEFCE shall arrange for periodic quality reviews of its internal audit in accordance with the GIAS.'
>
> 'The Department's Internal Audit Service shall also have a right of access to all documents prepared by the HEFCE internal auditor, including where the service is contracted out. The.... HEFCE's Head of Internal Audit's opinion on risk management, control and governance shall be forwarded as soon as possible to the sponsoring team who shall consult the Head of Internal Audit as appropriate.'
>
> 'In addition, the HEFCE shall.....notify any changes to internal audit's terms of reference, the audit committee's terms of reference or the HEFCE's Fraud Policy and Fraud Response Plan.'
>
> 'The Comptroller and Auditor General (C&AG) audits the HEFCE's annual accounts and lays them before Parliament, together with the HEFCE's annual report.'
>
> 'The C&AG has agreed to share with sponsor Departments information identified during the audit process and the audit report (together with any other outputs) at the end of the audit.'
>
> 'The C&AG may carry out examinations into the economy, efficiency and effectiveness with which the HEFCE has used its resources in discharging its functions.' (DfES, 2006b: P. 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 5.2.1, 5.2.3, 5.3.1: 16 – 18)

Yet, despite these extensive responsibilities of the Board, audit committees and audit more gernally, the responsibilities of the AO remain seemingly more extensive. So, for instance, it is made clear that:

> 'The Accounting Officer of the HEFCE is personally responsible for safeguarding the public funds for which he/she has charge; for ensuring propriety and regularity in the handling of those public funds; and for the day-to-day operations and management of the HEFCE.' (DfES, 2006b: P. 3.6.2: 12)

In recognition of these extensive responsibilities the Management Statement does allow some delegation of '...day-to-day administration of his/her Accounting Officer.....responsibilities to other employees in the HEFCE'. But is reminded '....however, he/she shall not assign absolutely to any other person any of the responsibilities set out in this document' (both quotes taken from DfES, 2006b: P. 3.8.1: 14).

The list of responsibilities for all AOs are contained in Paragraph 3.6.3 (DfES, 2006b: 14) under the titles of 'on planning and monitoring', 'on advising the board', 'on managing risk and resources', 'on accounting for the HEFCE's activities'. One of the key set of governance responsibilities are that the AO must:

> '.....ensure that a *system of risk management* is maintained to inform decisions on financial and operational planning and to assist in achieving objectives and targets.....ensure that adequate internal controls are maintained by the HEFCE, including effective measures against fraud and theft.....*sign a Statement on Internal Control regarding the HEFCE's system of internal control, for inclusion in the annual report and accounts.'* (DfES, 2006b: P. 3.6.3: 13 (emphasis added)

As indicated above it is the 'Statement on Internal Control' (SIC) that is of central importance to the AO's role. The difference is that in the private sector it is the Board, as a collective, that takes responsibility for the signing off of the SIC. In government departments and NDPBs it is the AO, *as an individual*, and not the Board, who has this responsibility.

The importance of the AO, not only in relation to signing the SIC, but more generally, however, is being questioned:

> 'The principle of clear Parliamentary accountability is not in question, but departments are now of a complexity little imagined over a century ago. As management becomes increasingly professional and departmental boards assume greater responsibilities, the question of whether accountability to Parliament is best served through an unchanged Accounting Officer role deserves continuing discussion.' (HM Treasury, 2005: Appendix A: P. A3: 17)

This remains unresolved at the time of writing but the indications are that, as will be made clearer below, the practices of HEFCE and advice from HEFCE and the Committee of University Chairmen (CUC) to HEIs is that HEFCE's Board and university councils in HEIs are to be seen as similar to boards of directors in the private sector, which de facto, rather than de jure, downplays the role of chief executives as AOs. Taking this aside, for now, the point to stress is that the de jure responsibilities of AOs, as currently stated in the Management Statement, are very extensive. The production of resource accounts, of which the SIC is a major element, provides the primary form of accountability. For these statements to have legitimacy requires extensive reliance on those who can supply suitable assurances as to the accuracy of the contents. AOs, therefore, like boards of directors in the private sector, rely heavily on other views, most notably on audit and the Board's audit committee. Audits and the audit committee equally have to be careful as to what they can say. Taken together the resulting resource accounts and particularly the SIC has a tendency to be codified and systematised to allow auditors to offer the verifiable assurances the AOs require.

These Management Statement requirements for HEFCE are clearly apparent in the actual practices of HEFCE as seen through their account of their governance arrangements. However, they are not entirely replicated, in that, as mentioned above, whilst the AO of HEFCE is still of central importance, the HEFCE Board has a more heightened role.

HEFCE's governance arrangements are contained in what is referred to as its 'accountability framework' (http://www.hefce.ac.uk/aboutus/accframe/[12]). This is because HEFCE are '.....accountable for the money we administer on the Government's behalf'. The centre point

[12] All quotes in this paragraph are taken from this web page.

of this accountability framework is 'HEFCE's approach to risk management' reinforcing, yet again, the importance of this concern as is the case in the private sector. Three elements feed into this central risk management concern, in the 'corporate governance framework', 'HEFCE's assurance framework' and the 'planning framework'. The following will concentrate on the first two of these frameworks to highlight HEFCE's compliance with the Management Statement from Government and the way this mirrors private sector thinking.

As already noted the role of the Board, as specified in the Management Statement, is not as prominent as is the role of the Chairman and the AO, yet, in HEFCE's corporate governance framework, the Board and Audit Committee have considerable importance. So in the Code of Best Practice (http://www.hefce.ac.uk/pubs/hefce/1997/m14_97.htm) (the Code hereafter) the role of the Chairman and Chief Executive is emphasised, yet the Board is given a much greater role than would seem to be required by the Management Statement. A flavour of this somewhat uncomfortable mix in responsibilities can be seen in various points in this Code:

> 'Communications between the Board and the Secretary of State will normally be through the Chairman, except where the Board has agreed that an individual member should act on its behalf.' (Paragraph 4 taken from (http://www.hefce.ac.uk/pubs/hefce/1997/m14_97.htm as with all the following)
>
> 'Day-to-day business between the Council and the DfES[13] will be conducted by the Chief Executive and other members of staff.' (Paragraph 5)
>
> 'The Chairman has particular responsibility, with the Chief Executive, for providing strategic leadership on matters such as..... a. Formulating the Board's strategy for discharging its statutory duties.' (Paragraph 7)
>
> 'Board members have corporate responsibility for ensuring that the Council[14] complies with any statutory or administrative requirements for the use of public funds.' (Paragraph 9)

[13] This code has not been updated at the time of writing to reflect the move of HE to the DBIS.

[14] The Code refers to HEFCE in short as the Council.

'Individual Board members should also be aware of their wider responsibilities as Board members. Like others who serve the public, they should follow the seven principles of public life set by the Committee on Standards in Public Life (the Nolan Committee).' (Paragraph 11)

'The Board is responsible for overseeing the production of a corporate plan. Preparing the corporate plan provides an opportunity for the Council to determine its key strategic objectives and targets.....' (Paragraph 20)

'Board members have a duty to ensure that public funds.....are properly safeguarded. They must ensure that at all times the Council conducts its operations as economically, efficiently and effectively as possible, with full regard to the relevant statutory provisions and to relevant guidance in Government accounting.' (Paragraph 23)

'The Chief Executive has responsibility, *under the Board*, for the overall organisation, management, and staffing of the Council and for its procedures in financial and other matters, including conduct and discipline.' (Paragraph 29) (emphasis added)

'The Chief Executive is the Council's designated accounting officer. He[15] is responsible to Parliament and the accounting officer of the DfES for the resources under his control. He has personal responsibility for....the public finances for which the Council is answerable; for keeping proper records; for prudent and economical administration; for avoiding waste and extravagance; and for the efficient and effective use of all the resources in the Council's charge. *The accounting officer has a responsibility to see that appropriate advice is tendered to the Board on all these matters*.' (Paragraph 30) (emphasis added)

'*The Board has a responsibility to monitor the performance of the Chief Executive and other senior staff*.' (Paragraph 37) (emphasis added)

Whilst the responsibilities and accountability of the Chairman of the Board and Chief Executive, as individuals, are important, as required by the Management Statement, the HEFCE Board, as a collective body, takes on a much wider significance. So, as indicated from the above quotes, it takes until paragraph 29 and 30 of the Code before the statutory responsibilities of the Chief Executive, as an AO, are clearly recognised. But Paragraph 37 reminds the holder of this officer that his (or her – see footnote 15) performance is subject to

[15] It is hoped that this reference to 'he' is not meant to imply that that this precludes a woman from becoming the Chief Executive of HEFCE sometime in the future, even though to date the office has been exclusively held by men.

the monitoring of the Board which makes the Board, as a collective group, rather more important than the chief executive as the AO. This significance of the Board, we would argue, is not traceable to the Management Statement but rather the wider legitimacy provided by the private sector thinking that this emphasis mirrors.

This more collective responsibility and mirroring of private sector thinking is also apparent in HEFCE's assurance framework, which includes the concentration on risk management systems and the extensive responsibilities given to the audit committee of the Board. The assurance framework makes clear from the outset that:

> 'The Board and the Chief Executive need to be confident that the systems, policies and people they have put in place are operating in a way that is effective, is focused on key risks and is driving the delivery of objectives. HEFCE's assurance framework sets out the sources of assurance that are available to provide this confidence.
>
> The disclosure requirements for Non-Departmental Public Bodies (NDPBs) such as HEFCE now include a Statement on Internal Control. This is a narrative statement that explains how the Council has applied the internal control principle. This should cover risk management and all controls, including governance, financial, operational and compliance controls.
>
> The Board accepts fully its responsibility to discharge these governance obligations, including the management of risk. In order to deliver its accountability responsibilities the Board has agreed a risk management policy that sets out its approach to risk management and the context for the system of internal control.' (Paragraphs 1 to 3 of HEFCE's Assurance Framework in http://www.hefce.ac.uk/AboutUs/riskman/[16]).

The Assurance Framework, therefore, concentrates on internal control and more specifically on risk management which:

> '..needs to allow for the effective assessment and exploitation of opportunities while also identifying what will prevent us from achieving our objectives, and ensuring we have in place *procedures to minimise, or manage, those risks* to a level we find acceptable. Risk management therefore involves a *planned and systematic approach* to the identification, assessment and mitigation of the risks which could hinder the achievement of strategic objectives.' (Paragraph 17 (emphasis added)

[16] Quotes in the following are also taken from this Assurance Framework.

The role of the Chief Executive is recognised but there is also a de facto recognition that the Board is ultimately responsible for the risk management systems' design, its effectiveness and the SIC. So it is made clear that:

> 'The Chief Executive is responsible (on behalf of the Board) for HEFCE's system of internal control and ensuring that the system is effective in managing risk.' (Paragraph 13)
>
> 'As Accounting Officer, the Chief Executive remains ultimately responsible for the organisation and its management of risk. He must: have a clear understanding of the Council's assessment of the risks that could prevent delivery of objectives.....ensure that the organisation has effective risk management and control processes.....be provided with assurance that the processes and the key strategic risks are being effectively managed.' (Paragraph 36)
>
> 'He will require these assurances in order to sign off the Statement on Internal Control. As part of this process the Chief Executive must undertake an annual review of the effectiveness of the system of internal control, which will enable the appropriate statement to be made in the Council annual report and accounts.' (Paragraph 37)
>
> '*The Board has a fundamental role in the management of risk. It will: receive an opinion from the Audit Committee that will include its review of the processes of risk management and internal control.....consider risk issues as they affect Board decisions....review key strategic risks that will be analysed annually alongside the strategic plan..... periodically review risks as part of the monitoring of the annual operating plan.*' (Paragraph 38) (emphasis added)

As with HEFCE's Governance Code the de jure role of the Chief Executive, as AO, in risk management is recognised but is consistently set within the context of the Board, which has ultimate responsibility for such matters. As is also clear from the above the role of the Audit Committee of the Board is of central importance to provide the assurances that are needed for the AO's, but in effect, the Board's SIC. The assurance framework, therefore, puts considerable emphasis on the work of the Audit Committee.

HEFCE's Audit Committee, as is the case in its equivalent in private sector organisations, has a unique role in relation to both the Board as well as the AO. As the terms of reference of the

Audit Committee (see http://www.hefce.ac.uk/aboutus/board/committees/audit.htm - all quotes in the following are from this webpage) indicate, constitutionally:

> 'The Audit Committee is a standing committee of the HEFCE Board. It advises both the Board and the Chief Executive as the Accounting Officer.' (Paragraph 4)

The more detailed purpose of the Audit Committee is to:

> '....advise and support the Board and the Accounting Officer by giving them independent assurance as to the effectiveness of the Council's internal control, corporate governance, and risk management. In particular, the committee will give a formal opinion to the Board on the audited accounts, including the Statement on Internal Control, before they are approved.....this.....extends to assurance to the Board about the internal control, corporate governance and risk management by institutions and related bodies receiving funding from HEFCE ('funded institutions')[17].' (Paragraph 1)

The duties of the Audit Committee follow from this purpose and are to:

> 'Consider the adequacy of corporate governance, risk management and internal control within the Council and funded institutions through reviewing: a.i. The mechanisms .....adopted by the management of HEFCE for the assessment and management of risks. a.ii. The planned activity of internal and external audit designed to...assess the systems operated by the Council and funded institutions to achieve effective internal control and risk management. a.iii. The annual results of internal and external audit activity..... a.iv. The adequacy of HEFCE management responses to issues identified by audit activity. a.v. Formal assurances given by HEFCE management relating to the corporate governance requirements for the organisation.....This includes receiving regular reports from directors on how they are managing risks in their areas of responsibility.' (Paragraph 3)

This allows the Audit Committee to 'advise the Board and the Accounting Officer' on the '....effectiveness of internal control, corporate governance and risk management in HEFCE and in the HE sector' (Paragraph 3.b.i). It also allows the Audit Committee to fulfil one of its major purposes (see above) to '.....give a formal opinion to the Board on the audited

[17] The internal control of HEFCE and, in fact, the success of HEFCE, is dependent on these funding institutions. As we have pointed out in the introduction, and as we discuss further below HEFCE '....are ultimately reliant on universities and colleges and other organizations to help us deliver our objectives.' (http://www.hefce.ac.uk/AboutUs/riskman/ Paragraph 31).

accounts, including the Statement on Internal Control, before they are approved' (Paragraph 1).

The resulting SIC is contained in the Annual Report and Accounts, the most recent of which is for 2008/09 (http://www.hefce.ac.uk/aboutus/accframe/ - all quotes below are taken from this SIC). The SIC starts with making clear that as Accounting Officer the Chief Executive has:

> '....responsibility for maintaining a sound system of internal control that supports the achievement of our strategic aims and objectives, while safeguarding the public funds and Council assets for which I am personally responsible, in accordance with the responsibilities assigned to me in the Treasury guidance 'Managing Public Money'. I also acknowledge my responsibilities in respect of the funds provided to the Council which are transmitted to higher and further education institutions and others for education, research and associated purposes.' (p.53)

HEFCE's AO, therefore, is speaking for and responsible for not just HEFCE, as an organisation, but all the 'funded institutions' who receive financial transfers from HEFCE. The SIC then goes on to make clear what the system of internal control is designed to:

> '....manage risk to a reasonable level rather than to eliminate all risk of failure to achieve policy, aims and objectives.' (p.53)

This leads to a statement that:

> 'The Council's approach to risk management is based on a *process* designed to identify the significant risks to achieving HEFCE's strategic aims and objectives, to evaluate the nature and extent of these risks, and to manage then effectively, efficiently and economically.....Central to this policy is the clear relationship between our strategic risks and the achievement of our strategic objectives' (p.53/54) (emphasis added)

This complex personal responsibility, however, is achieved through reliance on a range of others::

> 'While I am ultimately responsible for ensuring the system of internal control is effective in managing the Council's risks, I am supported in this process by my directors and senior management team.....'(p.53)

> ‘As Accounting Officer, I have responsibility for reviewing the effectiveness of the system of internal control. My review is informed by the work of the internal auditors and the executive managers within the Council who have responsibilities for the development of the internal control framework, and comments made by the external auditors in their management letter and other reports.....Our internal control is also subject to continual review and monitoring by the Deputy Chief Executive and directors. As part of the effectiveness review process I have sought assurance from them on these controls (via their assurance statements), and I then also review the key annual controls which inform this statement.’ (p.54/55)

The Audit Committee and the Board are centrally involved in the production of the final effectiveness review. So it is made clear that:

> ‘Each of the key annual controls (directors’ risk management statements, the production of the financial statements, the Assurance and Institutional Risk annual report and the Internal Audit annual report) have been considered by the Audit Committee with onward reports to the Board. I have discussed my effectiveness review with the Audit Committee and the Board and taken advice from them on its implications.’ (p.55)

The confidence this involvement of the Audit Committee and the Board gives the Chief Executive allows him, as AO, to conclude that in his report for 2008/09 there is no ‘....significant weakness in our internal controls which would warrant disclosure here’ (p.55).

This extensive involvement of others, notably the Audit Committee, and the need for a defendable effectiveness review, creates pressures towards codification and standardisation in the risk management system. This is clear from the identification and concentration on 23 strategic risks which are scored, monitored and assessed on a continuing basis. The process for this is described as follows:

> ‘Quarterly reports, which go to our Chief Executive’s Group and Board, provide a summary of the 23 strategic risk scores: they highlight the highest-scoring risks, explaining any movements in risk scores and provide a total risk score for the portfolio of risks to enable the overall movement in the risk portfolio to be managed over time. This quarterly monitoring system aims to identify new and changing risks, to confirm that controls are operating in respect of the key risks, and to evaluate the effectiveness

of those controls. The full risk register is reviewed as a whole as part of the annual update of the strategic plan.' (p.54)

As has been argued throughout this paper there seems to be an inevitable tendency to equate internal control with risk management and to make the resulting risk management into codified and standardised systems due to the necessity to make the annual report on effectiveness of these systems, transparent, auditable and audited. These same characteristics are apparent in the in the nature of internal control and risk management processes in Higher Education Institutions (HEIs).

(ii)The concentration on Risk Management Systems in Governance Requirements for and by HEIs

Governance requirements for HEIs, and the concentration and development of risk management systems, is an even closer replication of the private sector model described in the previous section. HEFCE, in this sense, is slightly more of an outlier, given its continuing reliance on the personal role and responsibility of the AO relative to HEFCE's Board. Even though HEIs are closer to the private sector in terms of the role and responsibilities of the Boards of Governors, a key difference with the private sector is that the risks of HEIs are also the risks of HEFCE due to the interdependence of the two. This interdependency affects HEFCE's regulatory involvement with HEIs as well as what HEFCE refer to as their 'risk appetite':

'In summary, HEFCE's risk appetite is reflected in our strategic objectives. We have considered our overall portfolio of risks to ensure, as far as possible, that the mix of risks remains tolerable and well balanced, even though the residual risks are relatively high. *This is partly because we are ultimately reliant on universities and colleges and other organizations to help us deliver our objectives.* The Council's framework for monitoring and reporting on the delivery of our strategic plan is designed to provide ongoing assurance, and/or highlight where further action is required.' (HEFCE's Assurance Framework http://www.hefce.ac.uk/AboutUs/riskman/) (emphasis added)

Because of this interdependency HEFCE needs certain risk-based assurances from HEIs so as to be able to be assured about the risks it is taking and to demonstrate through its own SIC that it is not taking too many risks with Government money. The way HEFCE does this is, not surprisingly, given the faith in risk management systems, is by finding out what is happening in HEIs, notably in terms of the way they are managing the risks they face. The analysis is intended to allow HEFCE to be in a better position to judge whether HEIs, in their view, are high or low risk and, therefore, whether they, in turn, can claim their own risk management systems are effective. This dynamic will be the primary focus of this sub-section.

The first impetus for the development of risk management systems in HEIs came with a 'circular letter' to all heads of HEIs in November 2000. In this, 'HEFCE's Accounts Direction to higher education institutions for 2000-01', the importance of risk management was presented as follows:

> 'The policy on corporate governance has been broadened to incorporate the need to operate systems of internal control, covering business, operational and compliance as well as financial control. This policy concentrates on a risk-based approach, with the aim of integrating corporate governance into the overall management process.' (HEFCE Circular Letter 24/00: 1)

With more than an eye to the private sector roots from where this thinking derives, Circular Letter 24/00 continues:

> 'The key principles of corporate governance are already being adopted by the higher education sector in order to reflect good practice. There are genuine business benefits to be gained from the risk based approach quite apart from the improvements in accountability and shareholder confidence.' (HEFCE Circular Letter 24/00: 1)

Effective risk management in Circular Letter 24/00 is very clearly linked to corporate governance and is portrayed as a 'process' that:

- ‘Covers all risks- governance, management, quality, reputational and financial, however it focuses on the most important risks
- Produces a balanced portfolio of risk exposure
- Is based on a clearly articulated policy and approach
- Requires regular monitoring and review, giving rise to action where appropriate
- Is integrated into normal business processes and aligned to the strategic objectives of the organisation
- Needs to be managed by an identified individual and involve the demonstrable commitment of senior governors, academics and officers.’

(HEFCE Circular Letter 24/00: 1)

This Circular Letter was very quickly followed up with a ‘briefing for governors and senior managers’ (HEFCE 2001/24) and ‘guide to good practice’ (HEFCE 2101/28) on risk management, the latter of which has been revised and updated (HEFCE 2005/11). To demonstrate the centrality of risk management to HEIs, the 2005 version of the good practice guide is of the view:

> ‘In the best-run organisations, risk management is synonymous with good management and good governance. It is not considered as a bolt-on to existing practices, or a separate exercise simply to meet regulatory requirements.’ (HEFCE 2005/11: 2, Executive Summary, Paragraph 5)

HEFCE, however, is not reliant on only these forms of advocacy for the importance and effectiveness of risk management systems but makes this a requirement through three major channels. First, through requiring that HEIs adopt the Committee of University Chairs (CUC) governance code of practice (CUC, 2004; 2009) where risk management is centre stage. Second, through the ‘financial memorandum’ (see HEFCE 2008/19 for the latest version), which specifies the basis for the financial relationship between HEFCE and HEIs, where risk management again is of central importance. Thirdly, and closely connected with the requirements of the financial memorandum, through the audit and accountability of HEIs in relation to the funds that HEFCE supplies (see HEFCE 2007/11 for an overview of the latest requirements and the Accountability and Audit Code of Practice in Annex B of HEFCE

2008/19) where HEFCE seeks certain assurances related to risk management practices to enable HEFCE to make a judgement as to whether any HEI is high or low risk. The following briefly looks at each of these three forms of requirements.

The CUC governance requirements are largely built on the private sector governance model analysed in the previous section giving particular major responsibilities to the governing body which has a majority of non-executive members. As is made clear from the outset of the Code:

> 'Every higher education institution shall be headed by an effective governing body, which is unambiguously and collectively responsible for overseeing the institution's activities, determining its future direction and fostering an environment in which the institution mission is achieved.....it shall take all final decisions on matters of fundamental concern to the institution.' (CUC, 2009: Part 1 Paragraph (P) 1: 13)

These extensive responsibilities are to be managed by a governing body that will have a '.....a majority of independent members, defined as both external and independent of the institution' (CUC, 2009: Part I, P 10: 14). In this connection, whilst the Head of Institution has a particular role granted by the financial memorandum, he or she is ultimately not as important as the governing body:

> 'The head of the institution is responsible for the executive management of the institution and its day-to-day direction. *The head of the institution must not seek to determine matters reserved for the governing body*.....The specific responsibilities...include...implementing the decisions of the governing body or ensuring that they are implemented through the relevant part of the institution's management structure.....and.....fulfilling the duty, as the officer designated by the governing body under the terms of the Funding Council's Financial Memorandum ('the designated officer') to alert the governing body if any actions or policy under consideration would be incompatible with the terms of the Financial Memorandum. If the governing body nevertheless decides to proceed, then the head of institution has a duty to inform either the chief executive of the relevant Funding Council or other appropriate officer.' (CUC, 2009: Part 11, P 2.14 and P2.15: 21) (emphasis added)

This makes the governing body the equivalent of the board of directors in private sector organisations but gives a particular statutory role to the head of institution, as a 'designated officer' which is not replicated in the private sector[18].

This replication of private sector thinking is clearly apparent in the risk management systems emphasis and the role of the audit committee in the effectiveness review and the SIC, which reports on the effectiveness of these systems. So, for instance, it is a requirement that:

> 'Institutions must adopt a risk-based approach to strategic planning.....HEIs are expected to identify and actively manage risks, having particular regard at governing body level to risks which could threaten the existence of the institution. An annual disclosure about risk management is required in audited financial statements..... Each institution's audit committee is required to provide advice to the governing body annually on risk management, control and governance in advance of the governing body approving the audited financial statements.' (CUC, 2009: Part 11, P 2.3.4, P 2.3.5, P 2.3.6: 25)

The role of audit and the audit committee in assessing the risk management systems is reinforced further in a number of ways such as:

> 'While the responsibility for devising, developing and maintaining control systems lies with management, *internal audit provides independent assurance about the adequacy and effectiveness of risk management, control and governance*.....The audit committee should be a small, authoritative body which has the necessary financial expertise and the time to examine the institution's risk management control under delegation from the governing body. It should not confine itself to financial systems but should examine risk management, control and governance independently, and report areas of concern to the governing body. *The committee must produce an annual report for the governing body, including its opinion on the adequacy and effectiveness of the HEI's risk management, control and governance arrangements for promoting economy, efficiency and effectiveness (value for money).*' (CUC, 2009: Part 11, P 3.9, P 3.10: 32) (emphasis added)

[18] It is the Chair of the Board of Directors, rather than Chief Executive, who has particular statutory responsibilities in the private sector. This is one of the reasons why the two positions are required to be held by different people. As an aside it was no wonder, therefore, there was much displeasure and unease when Sir Stuart Rose of Marks and Spencer extended his role as Chief Executive to also become Chairman of the Board of Directors. Since this time and following pressure to comply with the Combined Code of Corporate Governance Sir Stuart has finally agreed that by June 2010 a new Chief Executive will be appointed whilst he retains the Chairmanship of the Board.

So, in relation to risk management system design, effectiveness review of these systems and reporting on these systems, audit and the audit committee are of central importance as is the case in the private sector from which this thinking is derived.

Turning to the requirements contained in the Financial Memorandum (FM) the purpose of the FM is to address directly the interdependency problems in the relationships between HEFCE and HEIs. Thus it is made clear that:

> 'This Financial Memorandum sets out the formal relationship between HEFCE and the governing bodies of the institutions it funds. It reflects our responsibility to provide annual assurances to Parliament that.....our funds are being used for the purposes for which they were given....risk management, control and governance in the sector are effective.....value for money is being achieved.'
> (HEFCE 2008/19: Paragraph (P) 1: 2)

As this indicates one of the major 'assurances' HEFCE has to give to Parliament is in relation to the effectiveness of 'risk management, control and governance in the sector'. They are, therefore, very active in specifying how 'risk management, control and governance' are to be conducted in HEIs so that they are able to provide judgements on their effectiveness for the parliamentary assurances they need to make.

The centrality of the governing body is also apparent in this quote and is reinforced in various ways through the FM. So, for instance, it is made clear that:

> 'The governing body of an institution is collectively responsible for overseeing its activities, determining its future direction and fostering an environment in which its mission is achieved. Acting in accordance with the institution's own statutes and constitution (where appropriate), the governing body should ensure that the institution...has a robust and comprehensive system of risk management, control and corporate governance....has regular and adequate information to monitor performance and track the use of public funds.....plans and manages its activities to remain sustainable and financially viable....complies with the mandatory requirements relating to audit, set out in our audit and our annual accounts direction.....sends us.....the annual

> accountability returns which constitute the 'single conversation'[19].....other information we may reasonably request to understand the institution's risk status....has effective arrangements for the management and quality assurance of data submitted to.....HEFCE and other funding bodies (we reserve the right to use our own estimates of data where we have reason to believe institutional data are not fit for purpose).....considers our assessment of its risk and takes action to manage or mitigate the risks we identify.' (HEFCE 2008/19: P 13: 4)

The following will explore the audit and accountability implications of some of these summarised set of responsibilities but before looking at these it is worth noting that, as with the CUC governance guidelines, it is the governing body rather than the head of institution – called not the AO but the 'designated officer' – who is expected to undertake these requirements. It is even the governing body who appoints the 'designated officer' even though he or she has statutory responsibilities:

> 'The governing body will appoint the head of institution as the 'designated officer', who will advise the governing body (and HEFCE, if necessary) if the institution fails to comply with this memorandum. The designated officer and/or chair of the governing body may be required to appear before the Public Accounts Committee alongside the chief executive of HEFCE, as accounting officer, on matters related to grants to the institution.' (HEFCE 2008/19: P 14: 4)

The other point to note is the importance given in the FM to HEFCE's risk assessment of HEIs which provides an important context for understanding the importance of the accountability information that need to be supplied about HEIs. This starts within a general context of expectations in relation to good governance and management. As the FM makes clear:

> 'We expect institutions to have governance and management processes that can readily demonstrate to their public sector funders (including HEFCE) proper control over and accountability for, the use of public funds. The better these processes are, the easier it

[19] More will be said about what this below.

> will be for institutions to show that they are making proper use of public money.' (HEFCE 2008/19: P 27: 6)

To understand whether this is the case, accountability is of central importance with the amount of information to be supplied dependent on HEFCE's risk analysis of any HEI:

> 'Institutions should send us their accountability information on the specified dates in December each year. We will review this and give each institution a confidential formal assessment of its risk status. For those we consider to be 'not at high risk' – in our experience to date, the vast majority – there will be no need for further information or discussion of accountability until next year's return. Sometimes we will ask for more information to clarify uncertainties.
>
> When we assess an institution as 'at higher risk' we must respond appropriately, to protect the public interest. Our institutional engagement and support strategy .....describes the range of ways in which we might respond and help institutions resolve difficulties and manage risks. We will always discuss our concerns with the institution and take its views and actions into account, before we formally make an 'at higher risk' assessment. We will also try to reach agreement on what needs to be done. When we consider the institution to be no longer at higher risk, we will write to its governing body to confirm this.' (HEFCE 2008/19: P 30: 7)

Audit and accountability requirements which are focussed on the provision of required required reports at a single point of time in the year, referred to as the 'single conversation', is the subject of HEFCE 2007/11. However, it is the Accountability and Audit Code of Practice which is contained in Annex B of the FM (HEFCE 2008/19) which provides full details of HEFCE's requirements of HEIs. Annex B, however, follows from Annex A which spells out in more detail the 'mandatory requirements' of the FM and the Accountability and Audit Code of Practice, with which HEFCE will 'assess compliance'. The following will, therefore, concentrate on this Annex.

The key requirements in Annex A are largely related to the importance of risk management, audit and accountability. These are as follows:

'The governing body of each HEI must take reasonable steps to ensure that there are sound arrangements for risk management, control and governance, and for economy, efficiency and effectiveness (value for money) within the HEI.

Each HEI must have an effective audit committee which produces an annual report for the governing body and the designated officer.....The audit committee annual report must include the audit committee's opinion on the adequacy and effectiveness of the HEI's risk management, control and governance arrangements.

The audit committee of each HEI, advised where appropriate by its internal audit service, must satisfy itself that satisfactory arrangements are in place to promote economy, efficiency and effectiveness.

Each HEI must have an effective internal audit function, which reports regularly to the audit committee and at least annually to the governing body and the designated officer.

The work of the internal audit service must cover the whole of the risk management, control and governance arrangements of the HEI.

The head of the internal audit service must have direct access to the HEI's designated officer, the chair of the audit committee and, if necessary, the chair of governing body. Internal as well as external auditors must also have unrestricted access to information – including all records, assets, personnel and premises – and be authorised to obtain whatever information and explanations the head of the internal audit service or the external auditor considers necessary.

Subject to legislative constraints, the HEFCE assurance service must have unrestricted access to information.....which it considers necessary to fulfil its responsibilities. This includes access to any work of the internal and external auditors, or correspondence between internal and external auditors.

The following information must be provided..... a signed and approved set of financial statements.....a copy of the audit committee's annual report....a copy of the internal auditor's annual report.....a copy of the internal auditors' annual report.....the completed annual assurance return[20].....a copy of the external auditor's management letter and any management response.

The HEI's designated officer must report any material adverse change – such as a significant and immediate threat to the HEI's financial position, significant fraud or major accounting breakdown – without delay to all of the following: the chair of the HEI's audit committee...the chair of HEI's governing body.....the HEI's head of internal audit...the external auditor...the HEFCE chief executive.

The governing body must inform HEFCE's assurance service without delay of the removal or resignation of the external or internal auditors.' (HEFCE 2008/19: Annex A, P 4, P 5, P 7, P 8, P 9, P 10, P 13, P 15, P 16, P 17: 8-10)

[20] This is a simple form, whose design is specified in Annex E to the FM, which confirms a number of things not least compliance with the FM. It has to be completed by the designated officer. It is not the equivalent of the SIC provided by the Chief Executive of HEFCE as the accounting officer. This SIC is part of the financial statements. This will be developed further below.

Given the centrality of risk management and its effectiveness in these mandatory requirements this section ends with some brief comments on the contents of the Statement on Internal Control (SIC) whose main purpose is to clarify the nature of the internal control and risk management arrangements and the effectiveness review of these processes. The SIC provides an important empirical 'window' into HEI internal control and risk management arrangements and the way they are indeed codified, procedural systems. Space precludes a detailed empirical investigation into the actual nature of these systems in particular HEIs but the following gives a flavour of the insights that are likely to be forthcoming from such a study.

The SIC is not the Designated Officer's Assurance Statement. This is in marked contrast with HEFCE's SIC which is produced by the Chief Executive in a personal capacity as the Accounting Officer. The production of HEIs' SICs is a requirement but it needs to come from the governing body and not the 'designated officer'. According to HEFCE 2007/11 (Paragraph 20: 6) the financial statements need to:

> '....include a statement on internal control and/or a corporate governance statement. We believe this should incorporate or clearly reflect the Code of Governance published by the Committee of University Chairmen (CUC), which all institutions say they have adopted. This provides external assurance that the effectiveness of corporate governance is subject to regular review, and thus adds confidence to the accountability returns generated by institutions.'

This, not surprisingly, is much closer to the private sector equivalent of the SIC.

This dominant private sector emphasis leading to the codification and standardisation of these practice, resulting in them becoming procedural systems, is apparent in the SICs. Exploring

the SICs of all HEIs that are publicly available through the British Universities Finance Directors Group (BUFDG) financial statements service (http://www.bufdg.ac.uk/resources/statements/?a=cm) reinforces this claim.

All the reports and accounts on this website provide a Statement on Corporate Governance (SCG) and either a separate SIC or a SIC that is part of the SCG. All SIC's start off with two generic paragraphs about following HEFCE guidelines and providing caveats on the effectiveness assurances that can be given. These paragraphs read as follows but are taken from the University of Bath's SIC in the 2007/08 report and accounts:

> 'As the governing body of the University of Bath, the Council has responsibility for maintaining a sound system of internal control that supports the achievement of policies, aims and objectives, while safeguarding the public and other funds and assets for which it is responsible, in accordance with the responsibilities assigned to it in the Charter and Statutes and the Financial Memorandum with HEFCE.
>
> The system of internal control is designed to manage rather than eliminate the risks of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurances of effectiveness.'

What is apparent from the above is that what constitutes 'internal control' is that it is a risk management *system* whose effectiveness, and resulting assurance of effectiveness, cannot be 'absolute'.

Many SICs then go on to provide a generic description of the 'system of internal control that is in place. A typical example of this comes from Kingston Universities' SIC in their 2008/09 report and accounts:

> ‘The system of internal control is based on an ongoing process designed to identify the principal risks to the achievement of policies, aims and objectives, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically. This process has been in place during the year ended 31 July 2009 and up to date of approval of the financial statements, and accords with HEFCE guidance.’

Many SICS also provide further details on the nature of the risk management system, who are actively involved in its management and who make judgements about effectiveness. A typical rich example of this is apparent in the University of Cambridge’s SIC, as part of their 2007/08 report and accounts:

> ‘The Council’s Risk Steering Committee oversees risk management....The Audit Committee receives periodic reports from the internal auditors, which includes the internal auditors’ independent opinion on the adequacy and effectiveness of the Univesity’s system of internal control and risk management..... A system of indicators has been developed for the University’s key risks.... A robust risk prioritization methodology based on risk ranking and cost-benefit analysis has been established.... A University-wide risk register is maintained....key risks have been assigned to risk owners and reporting channels established.’ (Paragraphs 4 c, d,f, g, h and i)

Or take the SIC from Manchester Metropolitan University, included in the 2007/08 financial statements:

> ‘The Governing Body has...established a risk working group, made up of the Directorate, to oversee risk management.....The Audit Committee receives regular reports from the Head of Internal Audit, which includes Internal Audit’s independent opinion on the adequacy and effectiveness of the institution’s system of internal control, together with recommendations for improvement..... a system of key performance and risk indicators has been developed....an institution-wide risk register is maintained.....a robust risk prioritisation methodology based on risk ranking and cost benefit analysis has been established.’

The resulting risk management system is often managed by a defined group but in all cases the internal auditors are involved in one way or another and particularly in relation to the

effectiveness judgement. A not untypical model is apparent from the University of Portsmouth' SIC in their 2008/09 report and accounts:

> 'The Audit and Quality Committee has responsibility for overseeing the development and implementation of our Risk Management Policy.....The Audit and Quality Committee receives regular reports from our internal auditors, which include the internal auditor's independent opinion on the adequacy and effectiveness of the institution's system of internal control, together with recommendations for improvement.....A system of key performance and risk indictors has been developed and is reported to the Board at each meeting in the quarterly operating statements.'

This combination of codification and standardisation in risk management and the necessity to make these processes auditable, audited and defensible – to make them into procedural systems in other words - so apparent in these examples is replicated across the SICs of all HEIs.

Some Concluding Thoughts

This paper has a analysed three interconnected themes.

First, it has demonstrated how important internal control and risk management is to all organisations. Organisations are in existence to achieve certain objectives and to use different means for this achievement. The risk that well developed plans, both in terms of the ends to achieve and the means to achieve them can be disturbed through uncertainties that have not been predicted is of major concern to all organisations. Risk management processes, which try to make these uncertainties more apparent and controllable is a vital part of organisational life.

Second, that the design of risk management systems has been led by the private sector and, in effect, whatever has been a requirement for this sector, has been a mirrored requirement for organisations in the public and 'third' sectors. Like the generic 'new public management'

(Hood, 1991, 1996), which has permeated a range of specific changes in the managerial arrangements in the public and 'third' sectors over many years - making the title 'new' somewhat paradoxical - the development into areas such as risk management can be seen as yet another example of this trajectory. In all these cases the mirroring has always been one way – from the private sector to the public and 'third' sectors – very largely because of an underlying assumption that the private sector has lessons to teach the other sectors in our society.

Third, that this mirroring brings with it the problems that have arisen in the private sector with this systematisation of risk management concerns. The paper has used Power's (2004, 2007) critical analysis, which is primarily drawn from the private sector, to provide a critical edge to this analysis. His view that the '....private world of organisational internal control has been turned inside out, made public, codified and standardised and repackaged as risk management' (Power, 2004: 28) is a powerful and significant critique of what is happening in the private sector which is now replicated across the public and 'third' sector, and consequently HE, as the paper has demonstrated. There are various forces at work to make this systematisation inevitable and the paper has tried to articulate these in the context of HE. HE is a replication and is subject to the same critique.

We end this paper with developing this critique with Power's (2009) latest paper as a springboard for this analysis. Power (2004) talked of the 'risk management of everything' to register the fundamental influence risk management thinking has had for all aspects of organisational life where, in effect, everything to him was risky and needed to be managed if

ends were to be achieved. This remains true yet Power (2009) now talks of the 'risk management of nothing' to register the point that despite the immense amount of work that has occurred in the private sector, and now in other sectors, important risks and uncertainties are just *not* being managed. This 'depressing answer' is because:

> '.....growth of risk management from the mid-1990s onwards – the risk management of nearly everything – was less about managing risk as it is formally understood and more about creating organizational rhythms of accountability and auditable representations of due process. We have fallen prey to a legitimacy-driven style of risk management which has been extensively institutionalised and globalised, and important issues of 'risk appetite' have become lost in the procedural detail of organization-specific internal control, compliance and accounting systems.' (Power, 2009: 854)

The 'culprit' of this 'depressing answer' is with the power and significance of accounting and auditing:

> 'The problem goes much deeper: no less than an accounting style of knowing and a logic of auditability are responsible for restricting the development of a risk management which might have done a better job.' (Power, 2009: 854)[21]

Power's solution is to move away from these disciplines to other ways of looking at risk management, which provide less seeming certainty, less systematisation but more meaningful if rather less 'tidy' and assured analyses.

Why is this critique important for HE? First, it is important since HE, like all other organisations across all sectors, are replicating each other and that, whilst there is an attempt

[21] Michael Power, like the authors of this paper, are all professors of accounting. When the authors made similar points raised in this paper, in connection with a research project into schools, the audience of educationalists, commented in relation to the paper presented, that it was so good to hear such a critique coming from the 'belly of the beast'. It is the view of both Power and the authors of this paper that the academic profession of accounting and auditing has much to answer for what is happening in risk management. Yet at the same time it is recognised that society's anxieties to make uncertainties more certain, and the willingness of accounting and auditing to provide these assurances has allowed this thinking to have the influence it has managed to achieve.

at the 'risk management of everything', there is, in fact, a 'risk management of nothing' occurring. Yet there is a *belief* that the practices that are in place *are* managing the immense risks and uncertainties that HE faces. Second, unlike no other era has HE faced more uncertainties as to its future and the achievement of its objectives. The concern with risk management is fundamental to the survival of HE not just in England but throughout the UK and across the world. The trouble is that what is happening at the moment is little more than window dressing which might be good for accountants and auditors in HE and might even make HEFCE and HEI feel that they have the assurances that they need, but is failing to get to grips with the substantive issues about an uncertain future.

REFERENCES

Ayres, I. and Braithwaite, J. (1992) *Responsive Regulation*, New York: Oxford University Press

Basle Committee on Banking Supervision (BCBS) (1998) *Framework for the Evaluation of Internal Control*, Basle: Bank for International Settlements

Basle Committee on Banking Supervision (BCBS) (2001) *Consultative Document –Pillar 2 (Supervisory Review Process)* Basle: Bank for International Settlements

Beck, U. (1992) *Risk Society: Towards a New Modernity*, London: Sage

Beck, U. (2004) *A Critical Introduction to the Risk Society*, London: Pluto Press

Black, J. (2005) The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom, *Public Law*, Autumn, 512-548

Boyle, D. (2000) *The Tyranny of Numbers: Why Counting Can't Make Us Happy*, London: Harper Collins Publishers

Broadbent, J. and Laughlin, R. (2005) 'Accounting Concerns and Tensions in Accounting Standard Setting: The Case of Accounting for the Private Finance Initiative', *Accounting and Business Research*, 35(3): 207-222

Broadbent, J., Gill, J. and Laughlin, R. (2008) 'Identifying and Controlling Risk: The Problem of Uncertainty in the Private Finance Initiative in the UK's National Health Service', *Critical Perspectives on Accounting*, 19(1): 40-78

Cadbury Report (1992) *Report of the Committee on The Financial Aspects of Corporate Governance*, London: Gee Professional Publishing

Chartered Institute of Public Finance and Accounting and the Office of Public Management (CIPFA and OPM) (2004) *The Good Governance Standard for Public Services*, London: CIPFA and OPM

Committee on Sponsoring Organizations of the Treadway Commission (COSA) (1992) *Internal Control – Integrated Framework*, http://www.cosa.org/guidance.htm

Committee on Sponsoring Organizations of the Treadway Commission (COSA) (2004) *Enterprise Risk Management – Integrated Framework*, http://www.cosa.org/guidance.htm

Committee on Sponsoring Organizations of the Treadway Commission (COSA) (2009) *Guidance on Monitoring Internal Control Systems*, http://www.cosa.org/guidance.htm

Committee of University Chairmen (CUC) (2004) *Guide for Members of Higher Education Governing Bodies in the UK*, London: CUC

CUC (2009) *Guide for Members of Higher Education Governing Bodies in the UK*, London: CUC

Department for Education and Science (DfES) (2006a) *Financial Memorandum Between the DfES and HEFCE,* London: HMSO

Department for Education and Science (DfES) (2006b) *Revised Management Statement for HEFCE*, London: HMSO

Editorial (2000) Corporate Governance – The Subject Whose Time Has Come, *Corporate Governance: An International Review*, 8, 289-296

Financial Reporting Council (FRC) (1998) *The Combined Code of Corporate Governance*, London: Financial Reporting Council

FRC (2003) (Revised Versions in 2006 and 2006) *The Combined Code of Corporate Governance*, London: Financial Reporting Council

FRC (2009) *Consultation on the Proposed New Combined Code of Corporate Governance*, London: Financial Reporting Council

Froud, J. (2003) 'The Private Finance Initiative: Risk, Uncertainty and the State', *Accounting, Organizations and Society'*, 28(6): 567-589

Hampel Report (1998) *Final Report: Committee on Corporate Governance*, London: Gee Profession Publishing

Higher Education Funding Council of England (HEFCE) 2001/24, *Risk Management: A Briefing for Governors and Senior Managers*, February 2001

HEFCE 2001/28, *Risk Management – A Guide to Good Practice for Higher Education Institutions*, February 2001

HEFCE 2005/11, *Risk Management in Higher Education: A Guide to Good Practice*, January 2005

HEFCE 2007/11, *Accountability for Higher Education Institutions: New Arrangements from 2008*, January 2007

HEFCE 2008/19, *Model Financial Memorandum Between HEFCE and Institutions*, June 2008

HM Treasury (2005) *Corporate Governance in Central Government Departments: Code of Good Practice*, London: HMSO

Hood, C. (1991) A New Public Management for all Seasons?, *Public Administration*, 69 (1): 3-19

Hood, C. (1996) The 'New Public Management' in the 1980s: Variations on a Theme, *Accounting, Organizations and Society*, 20(2/3): 93-119

Hopwood, A.G. 'Editorial: Reflections and Projections – and Many, Many Thanks', *Accounting, Organizations and Society*, 34(8): 887-894

Hutter, B.M. (2001) 'Is Enforced Self-Regulation a Form of Risk Taking: The Case of Railway Health and Safety', *International Journal of the Sociology of Law*, 29(2): 379-400

Knechel, W.R. (2007) 'The Business Risk Audit: Origins, Obstacles and Opportunities', *Accounting, Organizations and Society*, 32(4/5): 383-408

Middlehurst, R. (2004) 'Changing Internal Governance: A Discussion of Leadership Roles and Management Structures in UK Universities', *Higher Education Quarterly*, 58(4): 258-279

National Council for Voluntary Organisations (NCVO) (2005) *Good Governance: A Code for the Voluntary and Community Sector*, London: NCVO, 2005

Power, M. (2004) *The Risk Management of Everything*, London: Demos

Power, M (2007) *Organized Uncertainty: Designing a World of Risk Management*, Oxford: Oxford University Press

Power, M. (2009) 'The Risk Management of Nothing', *Accounting, Organizations and Society*, 34(6/7): 849-855

Power, M., Scheytt, T., Soin, K. and Sahlin, K. (2009) 'Reputational Risk as a Logic of Organizing in Late Modernity', *Organization Studies*, 30(2/3): 301-324

Smith Report (2003) *Audit Committees Combined Code Guidance*, London: Financial Reporting Council

Spira, L and Page, M. (2003) 'Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit', *Accounting, Auditing and Accountability Journal*, 16(4): 640-661

Turnbull Report (1999) *Internal Control: Guidance for Directors on the Combined Code*, London: Financial Reporting Council

Turnbull Report (2005) *Revised Guidance for Directors on the Combined Code*, London: Financial Reporting Council