centre for analysis
of risk and regulation

Risk culture in financial organisations:

An interim report

Simon Ashby, Tommaso Palermo and Michael Power

November 2012

Contents

Acknowledgements

We are grateful to the following organisations for their financial support: Economic and Social Research Council (ESRC); The Chartered Insurance Institute (CII); The Chartered Institute of Management Accountants (CIMA); and the Lighthill Risk Network. We would particularly like to thank the many individuals and organisations who have participated to date in this study. For reasons of confidentiality they are not named. We also thank the Knowledge Transfer Network for Financial Services, specifically Dickie Whittaker and Chris Sier for their support, Hollie Seechurn for her research assistance, and Yvonne Guthrie for copyediting. Finally we acknowledge our respective institutions, the London School of Economics and Political Science and Plymouth University, for their additional financial contributions to the project.

Executive Summary

It is widely recognised that problems with *organisational culture* played a major role in the financial crisis which crystallised in the late 2000s. '*Risk culture'* in particular has become an object of focus and discussion by regulators and other bodies, yet there is no consensus on exactly what it is or how it might be managed. This research study, funded from a mix of public and private sources, seeks to enhance the practical understanding of risk culture. We regard it as highly likely that organisations can be characterised by more than one risk culture. We also propose a 'bandwidth' model of risk culture to suggest that there is no ideal, and that it can be understood in terms of the formal and informal *processes* by which organisations manage risk taking and control within limits of various kinds, including incentivisation limits. This interim report describes our initial findings and ideas based on deskwork and in-depth interviews with senior risk staff at nine major financial organisations. Future work will expand the interview base and conduct surveys to assess typical 'stress points' in organisational risk cultures. Our findings to date are grouped around four main themes.

- First, in contrast to public debates which emphasise values and the need to change mindsets, we learned of risk culture workstreams with more of an emphasis on improving *oversight structures* and *information flows*, including performance metrics for risk and good compliance.

- Second, from our discussions it also appeared that critical issues in risk culture were being played out in the space between what are called *first and second lines of defence*, suggesting that this distinction, which many take for granted, may not be helpful in advancing the debate about risk culture.

- Third, improving risk culture was also seen by CROs as a matter of improving the *organisational footprint of the risk management function*. This was more than just rolling out ERM systems but involved expanding the reach of informal risk processes, information sharing and escalation, and representation on key committees.

- Fourth, we also heard concerns about a familiar issue – the role of *documentation*. The argument was that some documentary and evidentiary demands were creating the wrong kind of risk culture. We intend to follow up further on this.

1. Risk Culture: background

Much of the commentary and analysis about the actions of financial organisations, from the global financial crisis to events such as product mis-selling, rogue trading and the recent LIBOR scandal, share a common and fundamental focus. It is argued that these problems arose because of weaknesses in the *cultures* of banks and other financial institutions (BOFIs). Yet, despite near universal agreement that this problem is at the centre of things, relatively little has been done by practitioners, regulators or academics, to explore how the cultures of BOFIs impact on risk taking and control decisions. This is beginning to change and advisory firms have created a number of service lines and survey instruments which seek to make risk culture visible and manageable. Professional institutes have also developed guidance. Yet the subject remains an 'elephant in the room', of which many are aware, but few have the capacity to tackle to any degree of depth and clarity.

In the wake of the global financial crisis, calls to address the culture of the banking sector have been accompanied by a distinct lack of detail on the specifics. For example, in October 2010, Marcus Agius, chairman of Barclays, stated:

> "…the leaders of industry must collectively procure a visible and substantive change in the culture of our institutions, so as fundamentally to convince the world once again that they are businesses which can be relied on." (FT.com, 2010a)

Similarly, in a series of speeches in 2010, the Financial Services Authority (FSA) indicated its commitment to improving the regulatory oversight of the culture of the UK financial services sector, and banking in particular (Sants, 2010a&b). This commitment was reiterated by Martin Wheatley in relation to the forthcoming Financial Conduct Authority (Wheatley, 2012). However, as the FSA Chairman Lord Turner has explained (FT.com, 2010b): "We simply do not know if we have the tools to change the banking culture."

Episodes such as the recent LIBOR scandal and apparent Payment Protection Insurance (PPI) mis-selling have reiterated the importance of culture and highlighted the very slow pace of change. Commenting in October 2012 Stephen Hester, the CEO of RBS stated, in an almost identical statement to Marcus Agius two years previously:

> "Banks must undergo a wholesale change in their culture and refocus their behaviour on meeting the needs of customers to restore trust in the industry." (Reuters, 2012)

One particularly important aspect of this culture change and concomitant restoration of trust relates to the development of more appropriate *risk cultures* within banks and, for that matter, other financial institutions such as insurers, who are not immune to crises and scandals of their own (some insurers have been implicated as agents of PPI mis-selling, for example). Influential organisations such as the Institute of International Finance (IIF) have even gone as far as to state that the:

> "…development of a 'risk culture' throughout the firm is perhaps the most fundamental tool for effective risk management." (IIF 2008)

Despite this apparent consensus on the importance of 'risk culture' (see also: Ashby, 2011; Independent Audit, 2011), there is little agreement on what 'risk culture' is and how it might be managed. We do not imagine that this situation is due to a lack of interest, especially amongst the consulting community. Indeed, the internet is full of advice on how BOFIs can assess and manage their risk cultures and there are some interesting efforts to develop diagnostic tools (see Appendix I). Professional risk institutes are also contributing to the debate, e.g. the October 2012 launch of the Institute of Risk Management's guidance on risk culture (IRM, 2012).

A feature of much of the practice-orientated work is the assumption that risk cultures can and should be measured and categorised. From this it seems to follow that there are some ideal elements of an *effective* risk culture, to which all organisations should strive (e.g. IIF, 2009). In short, we observe a desire to quantify risk culture, reducing it in some cases to a kind of basic personality profile which is then used to analysis the collective risk attitudes and risk management behaviours of an organisation's decision makers.

While we respect these efforts, we also feel that they necessarily overlook much of the richness of the concept of risk culture. Not only is risk a multi-dimensional concept (Haimes, 2009) but, as with any kind of profiling, certain organisations will fit the simplified profiles that are provided, but many others will not. This issue is likely to be especially acute in the financial services sector, where there is a wide variety of organisations (large-small, domestic-international, proprietary-mutual, etc.) working in a range of markets (retail, commercial, investment, insurance, etc.). Equally, while the academic literature on culture is very large and has influenced some of the consulting products noted above, risk culture has largely been ignored (Bozeman & Kingsley, 1998, and Power, 2007: 175-8 are notable rarities).

Our approach, as academics to the already crowded discussion, is contained in this interim report on our project which we intend to complete in mid-2013. It can be described as a 'bottom-up' approach which seeks in the first instance to understand how a sample of BOFIs think about and address risk culture, and especially how they make it actionable. We elaborate on this approach in the next section and then offer our preliminary results and thinking.

2. Risk Culture: our approach

There are many definitions of 'risk culture' (see Appendix I) and we do not wish to add to this list. The different definitions have some common elements, namely a focus on the habits and routines which are relevant to risk taking and its mitigation. What makes risk culture such a fascinating and challenging topic to research is the fact that many, though not all, of these habits and routines are not readily visible, even to organisational participants themselves let alone researchers. Yet it is this problem of visibility, of making risk culture visible, that is at the heart of current regulatory and organisational focus.

It is a fact that the term 'risk culture' per se has gained increasing attention in the recent years. While the quotes in the previous section suggest anecdotal evidence of greater institutional attention, Figure 1 provides a more systematic analysis of the emergence of the term 'risk culture' using: a resource for access to global news in English (*Nexis*, including results related to the banking sector only); and the websites of 28 professional bodies and consultancy firms (*practice* search).

Results confirm what we would naturally expect, namely an expansion in the use of the term in the last 10 years.

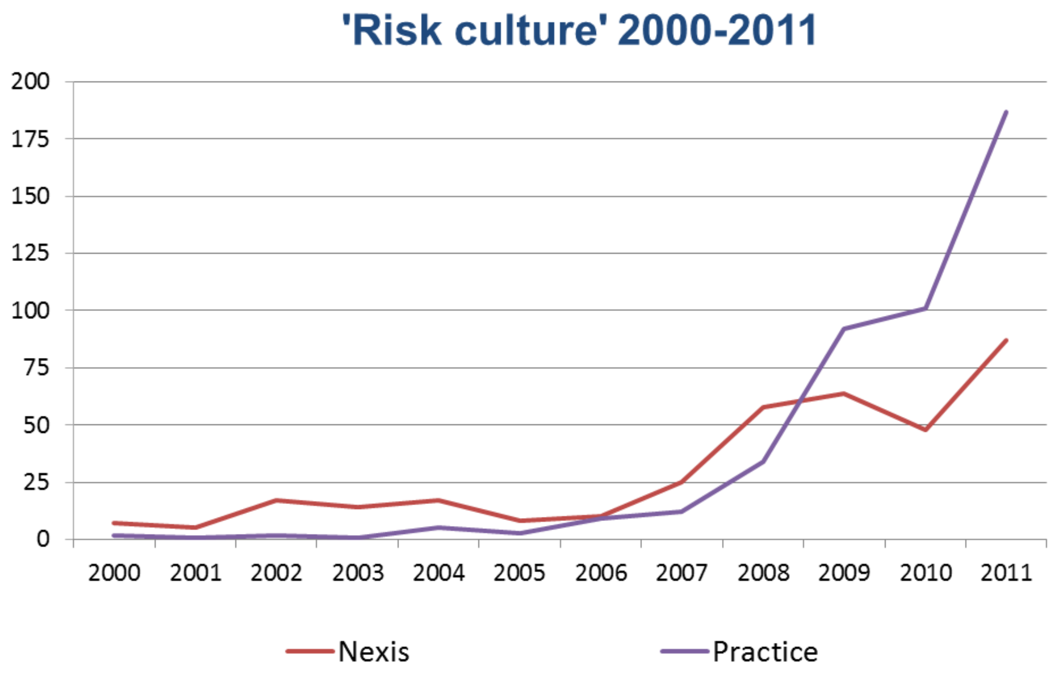

Figure 1

At the outset, we should say that 'risk culture in financial organisations' is not a special and unique issue. It may seem that way to those working in financial services, and there are certainly some unique features of financial services which we must take into account. But problems of 'risk culture' have many similarities with other change programmes which have been seen in corporate life, such as total quality management (TQM), Continuous Improvement programmes, and 'safety culture' in the offshore oil industry and in aviation. In all these cases, just as in the case of 'risk culture' in financial organisations, the focus has come about as a consequence of disappointments with existing practice, of threats of competition, and of outright disasters. Furthermore, 'risk culture' itself is not a recent concept despite the attention it is now receiving. The term can be traced back to the 1980s and the Piper Alpha disaster, but scholars such as Barry Turner, author of *Man-Made Disasters* (1978), were exploring related issues before that. Accountants will trace contemporary concerns with risk culture back to the idea of the 'control environment' which is at least as old as COSO (1992) and reaches even further back to auditors' distinction between transaction controls and *general* controls.

This project intends to increase our understanding of 'risk culture' and effect a knowledge transfer from academia to business by focusing on the 'drivers' (e.g., attitudes to information complexity, rate of expansion in operations) which influence the risk taking and control activities of BOFIs. The intention is not to presume what a 'good' or 'bad' risk culture looks like but to investigate the often competing aspects of organisational culture which can drive both risk taking and its mitigation.

We believe that a necessary step to achieve this goal is to start empirically by examining how organisations think about 'risk culture', what reasons lead them to an increased preoccupation with 'risk culture', and what are the concrete workstreams and change programmes put in place to make 'risk culture' a visible and manageable issue in the organisation. This mid-project report addresses mainly these latter issues – how organisations think and act on risk culture - based on our preliminary interview findings in nine BOFIs and additional interviews with relevant actors in the field (see Appendix II for more details on the methods). We do not impose on participant organisations our own definition and understanding of risk culture. On the contrary, we are primarily interested in how financial organisations define risk culture for themselves and develop actionable workstreams to manage it.

If we have any prior assumptions, they are minimal and modest. They can be described as follows:

- 'Risk culture' is not a static thing but a continuous process, or processes, which repeats and renews itself but may be subject to shocks.
- Risk culture will be a mixture of formal and informal processes (as noted in recent IRM guidance). The former are easy to observe; the latter are harder to observe since they involve a myriad of small behaviours and habits which in aggregate constitute the state of risk culture at any one point in time.
- Finally, we do not assume that either an organisation has a single risk culture or that a risk culture may not be trans-organisational. Conceptually we would prefer to speak of 'risk cultures' which may be unevenly distributed within organisations (e.g. retail as compared with investment banking) or the financial industry as a whole (e.g. insurers as compared with banks).

These assumptions lead to an approach to risk culture that emphasises the notions of 'bandwidth' and 'limits' (see Figure 2). Trade-offs between risk control and risk-taking activities are at the heart of our (tentative) conceptual model[1]. The basic and simple idea

[1] Note that similar trade-offs can be traced in other literatures, such as management control (Simons, 1995) and safety culture (Reason, 1997).

is that both too much control and too little control can lead to mediocrity or lost opportunity (risk of bankruptcy) and catastrophe or value destruction respectively (risk of catastrophe). Reckless organisations operate beyond their authorised bandwidth limits, while precautionary organisations operate beyond their control propensity (i.e. the level of control hinders the achievement of business objectives). The risk culture debate is primarily motivated by the former, whereas we think that it applies equally to the latter and the problem of excessive risk aversion.

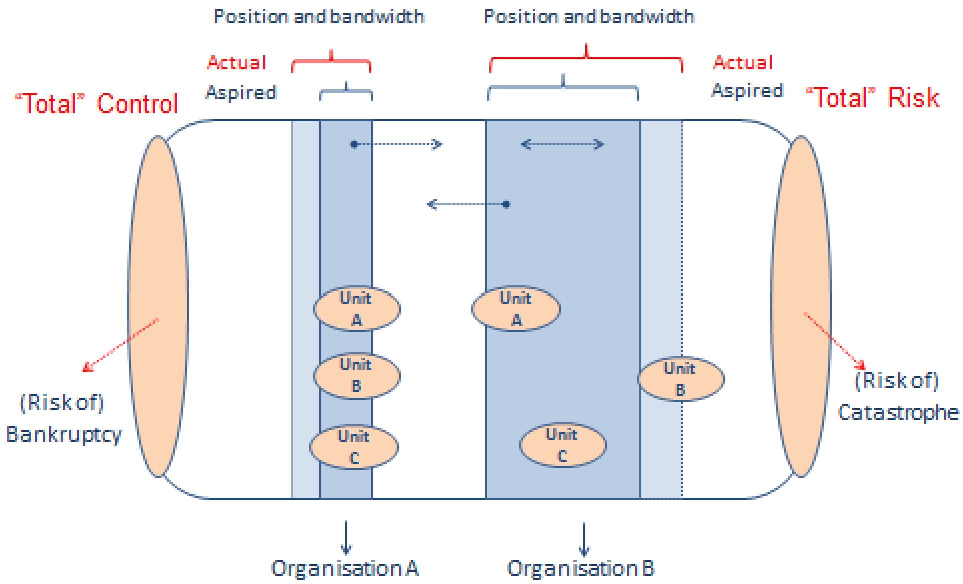

Figure 2: Tentative conceptual model of risk culture

The model suggests that risk culture may be dependent on clarity about the desired/actual net risk position of an organisation. In the example in the figure, in both organisation A and organisation B there is a gap between the aspired and actual position in terms of risk control/risk taking. Importantly, we believe that what happens at both the aggregate organisational level and in specific settings matters. Indeed, it may be more useful for practitioners to focus on the latter as '*stress points*' in risk cultures (e.g. hiring and promotion; performance planning and rewards; relations with regulators; new product development), where conflicts and tensions arise, rather than imagine that risk cultures matter equally in all parts of the organisation. We also recognise that in some organisations there may be greater homogeneity between different *organisational units* (e.g. organisation A in the figure) than in others (e.g. organisation B). Specific areas and hot spots may drive a business outside its prescribed 'safe' zone (e.g. unit B is leading organisation B towards the 'total' risk area). It follows from Figure 2 that risk culture requires clarity about, and commitment to the enforcement of, risk appetite or tolerance.

To summarise, in a short period of time the discourse of risk culture has grown dramatically (Figure 1) and a number of advisory and policy initiatives have taken place or are underway (Appendix I). Our research seeks to make a further contribution to practitioner and academic understanding in this crowded space. We begin in this interim report by addressing the way BOFIs think about risk culture. In future work we hope to identify organisational stress points where risk culture is both most visible and most tested.

Our methodological approach is described in detail at Appendix II. We have conducted interviews with risk leaders in nine organisations to date, and have analysed the public disclosure documents of these firms. We have also surveyed some of the existing literature. Our preliminary findings are based on our data collection to date and should be understood in the context of a small sample. Future work will extend the database of the project to include surveys of professional body memberships and also key actors within some of our participating organisations.

3. Risk Culture: preliminary findings and ideas

The initial interviews with senior risk leaders in participant organisations reveal an abundance of experimentation in the form of risk culture workstreams and change programmes. A number of interviewees agreed that risk culture is the most invisible and most important issue which fails to get enough attention in good times. Risk culture workstreams are often related to ambitions to change banking sector reputation. One interview complained about how one hears very often that banks have not changed their behaviours yet he has observed significant changes over the last three or four years.

Our inquiries were at the level of senior personnel in the risk functions of the participating organisations. We felt that this was an important place to start but we recognise that it limits the extent to which we can draw any general conclusions. Bearing in mind these limitations, the following strands of results represent valuable input to develop further our understanding of risk culture. A number of common themes struck us in our enquiries. These are detailed in four separate sections, although the themes discussed in each section seem to be highly interdependent.

3.1. Information and organisational structure

The failure to connect up disparate sources of risk information is a dominant diagnosis in the analysis of disasters and accidents (Turner, 1978), and we were struck by the centrality of this theme in many organisations. This demonstrates that risk culture is seen not only or primarily as an ethical issue or as having to do with incentives. Our data suggests that it also has as much, if not more, to do with management practice and information structures.

Among our sample, there was an emphasis on *risk centralisation* coupled to enhanced oversight capability. In one organisation this centralisation created 'tighter control over big earners' who were made to understand that their own rewards were dependent on the lower risk-return activities elsewhere in the group. In this setting centralisation was also coupled to a programme to develop more of a group mentality at the level of the business. At a number of other organisations centralisation was closely linked to *structural change* in the form of new, small groups to oversee silos, support the board and provide risk oversight perceived as previously missing or inadequate. Such groups would be more forward looking and less granular in their operations as compared with, for example, daily liquidity or compliance regulation. Although these units were in their early days of operation and the process was not without friction, they were seen by their proponents as very important for risk culture. As one interviewee put it, the mistake of the regulator in the past was to focus too much on 'risk management' and not enough on 'risk oversight'.

We take the suggestion here to be that a form of *risk oversight*, which operates in a different way to both first and second line risk management, is a defining feature of improving consistency in risk management for these organisations. The setting of limits and boundaries via clear authorities for first line activity, and the monitoring of these limits, was a universal aspiration in all our organisations. This suggests that the problem of risk culture may be as much about recovering clarity and enforcement capacity over organisational activities as it is about changing mindsets. Notably, we did not detect a romantic longing for a more solidaristic and communal organisation, something which is implicit in some consulting templates for risk culture.

Another key aspect of the new emphasis on centralisation involves *information*. In part this is reflected in efforts to drive risk ownership into the front line of business even more than at present. One organisation is explicitly building an approach where rewards and promotional prospects are attached to compliance across a range of activities. Such an approach depends on finding metrics with desired behavioural impact. Understandably, organisations regard these metrics as proprietorial, but we noted a difference between those who were looking to develop the use of their existing suites of compliance and risk data for this purpose, and those using and adapting the tools suggested by external advisers.

A closely related theme is the issue of the *aggregation* of risk data. Problems with other financial organisations, such as UBS, revealed considerable informational fragmentation and a failure to consolidate risk information, even at the simple level of counting types of assets and commitments. This was confirmed to us during an interview at the Bank of England. This is both an information issue and an organisation issue; it was suggested that how often the quality of risk data aggregation is reviewed is a good 'dip-test' of the state of organisational risk culture. Monitoring and hygiene work of this kind is not glamorous but may be regarded as the foundation of organisational risk culture. One of our interviewees made a similar point in relation to keeping Business Continuity Plans (BCP) up to date. More generally, the maintenance of risk infrastructure in the form of policies, standards and authorities was seen as essential.

Finally, all organisations were concerned to break down silos and encourage risk *information sharing*. In one organisation, this took the form of an open system with the idea of repositioning risk reporting and moving it away from the extreme of 'whistleblowing' and transforming it into internal knowledge sharing via a data repository. This journey to openness would be achieved by organisation-wide training programmes. Interestingly, one organisation monitored the take-up of risk training courses by non-risk people within the organisation, regarding this as a measure of risk culture.

Box 1: Risk culture, information and structure

The problem of risk culture may be as much about recovering clarity and enforcement capacity over organisational activities and information sharing as it is about changing mindsets. Risk information infrastructure, diffusion and use are a core feature of perceived 'good' risk culture by organisations.

3.2. Connecting first and second lines of defence

From our initial interviews, we concluded that key issues are played out at the interface between what are called the first and second lines of defence. Several interviewees admitted that there were significant challenges in operationalising this interface.

An ever present issue in maintaining risk culture is the structural position of risk functions within the organisation as a whole. One commonly identified issue was that of risk functions being *captured* by business units and this shows some of the difficulties of embedding risk directors within the front line. Regulators also play a role in this issue by having concerns about lack of role clarity of embedded risk functions. As a result, there is a proliferation of what one interviewee called 'dotted line reporting' to cope with role dualities.

A second issue, connected with the earlier discussion about information sharing and communication, concerns the reporting of risk issues by first line. A perceived challenge is to avoid punitive actions that may prevent managers from openly raising issues of concern. The potential problem emerges quite clearly from the words of one interviewee:

> "One of the things that helps greatly with the flow of information through the organisation is how it's reacted to when it gets to the next level. So being able to report risks openly and honestly without getting your head bitten off from the second that's done is crucial […] For example, if I told you something that might be happening you do not want your directors on your back saying 'What have you told them? Why?' So managing the flow of information through an organisation to ensure key stakeholders are properly engaged is quite important […] to avoid the wrong reaction happening."

Our preliminary view from these discussions is that role tensions and ambiguities of this kind are inherent in risk culture and organisations will deal with them in different ways. We had the impression that the distinction between first and second lines of defence was highly institutionalised in practitioner thinking but also unhelpful in addressing some of these more fuzzy issues. Rather than forcing key organisational actors into a binary system, the policy issue may be to have greater awareness and management of potential conflicts of interest and risks of capture. This seems more in line with the operating reality of organisations, particularly those with a large group structure.

Indeed, two interviewees suggested that regulators operate with an old model of the CRO/CEO relationship, while their organisation had created a new oversight officer, in addition to a CRO in the traditional sense, to strengthen 'risk oversight' over 'risk management'. We are not yet in a position to judge the success of this innovation but it raises an important question as to whether and how risk cultures would be judged by others, such as regulators, to be deficient if they adopt non-traditional roles and structure.

> **Box 2: Lines of defence and organisational innovations**
>
> *The present debate about risk culture appears to be characterised by efforts to strengthen roles that are already highly institutionalised and recognised by regulators. Therefore, the question is whether innovative organisational solutions, with a potential to enhance risk culture(s), may be welcomed or not by regulators and investors.*

3.3. The organisational footprint of the risk management function

Risk functions have traditionally been less powerful in many financial organisations, partly for credibility reasons and partly because of benign economic conditions. For example, despite longstanding efforts to launch ERM in insurers, underwriters and actuarial support have traditionally been at the centre of organisational risk thinking, with risk management confined to operations.

This 'old' world has certainly been transformed, and was changing prior to the financial crisis. We learned of many different efforts to expand the footprint of risk management within organisations. An obvious first step in this respect has been to obtain membership in key committees. One interviewee noted that regrettably there had been no risk member in one key senior-level committee. This view was reinforced by another interviewee who noted that traditional committee structures tend to segment risk thinking whereas 'good' risk management is implicated in every committee and not just a 'risk' committee:

> "You go to a management meeting and you talk about management issues and then you go to a risk committee and you talk about risk issues. And sometimes you talk about the same issues in both but people get very confused and I don't know … I don't know how right it is but I really think you should be talking about risk when you talk about your management issues because it kind of feels to me again culturally that's where we are."

Several interviewees acknowledged the communications challenge involved in increasing the footprint of risk management. In part this was 'making sure that debates happen' and being clear about the alignment of risk and performance. Risk functions which waste senior management time lose credibility very quickly. As put by one interviewee:

> "I have a two-hour slot with the Group Executive every month. I chose to cancel last month's because I didn't think I had enough of significance and urgency to utilise their time. It's a two-way street, I get the time I ask for but you need to recognise that as much as I know I've got that slot, I'm not just going to come in and talk to you unless I've got material things to talk to you about. To keep their engagement and trust they need to know that I won't unnecessarily waste their time."

At one organisation, we heard of efforts to animate risk conversations within the organisation using performance-focused language that did not use the 'risk' word. Similarly, one other recognised the need for the risk function to invest heavily in relationships with the front line and help them to take more responsibility. But it was not just a question of the front line. One CRO regarded IT and technology as one of the most challenging specialisms in the organisation with major challenges for the risk function. A number of organisations pointed to recruitment practices and pre-employment screening as an essential pillar of building the 'right' kind of risk culture.

Bearing in mind the limits of interviewing mainly senior risk managers, we were struck by two strands of our results. First, risk culture at the organisation level was not articulated and discussed primarily in ethical and reputational terms about proper behaviour - it had a much more operational feel to it. This is understandable as organisations have naturally responded to the risk culture challenge by dealing with what is visible and potentially manageable. Second, ERM was conspicuous by its absence in our discussions. Indeed, only one interviewee mentioned explicitly their ERM process in relation to the risk culture discussion. This suggests that the relationship between risk culture workstreams and existing ERM systems may not be as straightforward as might be imagined. We need to do further work on this issue, but it may be that ERM operates with traditional risk categories and business units; in contrast risk culture has more to do with linking formal and informal aspects of organisations.

Box 3: Risk culture and risk management

Observed risk culture workstreams dealt primarily with what is visible and potentially manageable, while formal ERM systems were generally absent from risk culture discussions. Therefore, the relation between risk culture workstreams and existing ERM systems may not be as straightforward as might be imagined.

3.4. Documentation versus behavioural change

Several interviewees noted that risk culture poses some unique problems of documentation. Indeed, this is hardly surprising given that it is both invisible and important as noted above. In one organisation they were comfortable that the risk culture was good, but this was 'hard to demonstrate' especially for committees which tended to be highly 'action- oriented'. One CRO confirmed that the organisation was 'not good at writing things down and on process and formality.'

In another organisation, it was argued that Solvency 2 documentation requirements were substantively affecting underwriting decisions, i.e. making underwriters more risk-averse. From this point of view a big question in our study going forward is whether regulation is affecting risk cultures in unintended ways. Different attitudes towards regulators' requests emerged from the initial interviewees. One interviewee put it rather bluntly:

> "It's bureaucracy gone mad and is destroying the culture we have. The pressure on individuals is phenomenal and has a negative impact on morale. They don't blame the company but just looking at what was being asked of them it was very clear it has limited real value to us or the regulator."

The CRO in another organisation, instead, suggested an ambition to align with regulators' expectations. Paraphrasing the interviewee's words, developing resistance is unlikely to be a fruitful strategy, although the business needs to recognise that compliance with regulatory requirements has a cost in terms of time and resources. Yet another CRO said the financial regulator was a given and if one didn't like it, then one should go to work in a different industry sector.

Documentation issues were also important in the use of tools and surveys. A number of respondents said that they used staff surveys, both general satisfaction surveys and specific risk attitude surveys (this is not surprising considering the increasing availability of risk culture toolkits – see Appendix I). One said that such exercises could be fun, with feedback sessions being enjoyable. However, he also noted that generating clear and valuable actions from such exercises was difficult.

We think that the potential value of such surveys might be in the process rather than the actionable outcome, since the academic literature suggests that increases in interaction may be associated with more effective risk cultures and capabilities to manage risk (Simons, 1999). However, this is just a speculation and an issue for further investigation.

Box 4: 'Writing things down'

Risk culture poses some unique problems of documentation, as organisations increasingly need to be good at 'writing things down'. This poses a challenge in terms of maintaining a good relationship with regulators and making the best use of risk culture toolkits that stimulate valuable discussion and informal interaction.

4. What we hope to do

The account given above describes our preliminary findings based on a small set of interviews with key organisational actors. The conclusions and observations should be understood in the context of these limitations. However, this early process has shaped where we will take the project in the next months and we welcome views on how we should do this. Specifically we would like to look further into:

- *How are risk culture tools actually used?* There are a number of products in the consulting marketplace in addition to in-house change programmes.
- *What collaborative networks exist?* In the aviation industry we know that there is a lot of information sharing between engineers in different companies. We might expect collaboration to exist for operational risk matters in the financial industry but market and credit risk issues would be likely to be highly proprietorial.
- *What are the effects of regulation on risk culture?* Is regulation making organisations more risk averse and more averse to the risk of regulatory censure? Is it having further unintended consequences around how organisations manage their risks? For example, does regulation increase attention to risk measurability?
- *How do the first and second lines interact?* From the academic literature we know that interaction is an important feature of risk management, particularly under stressed conditions. So a culture which encourages and sustains interaction could be said to be a good risk culture. This might also help us to address the question of when is the *embeddedness of risk management good or bad?*
- *What are the pressure points in risk culture?* We intend that our survey instruments, follow-up focus groups and further interviews will provide some answers to this question.

Appendix I: Selected 'risk culture' definitions and toolkits

Table 1 below provides a range of selected definitions of risk culture from the practice and academic literature.

	Selected definitions	Source
Practice literature	the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management.	Basel Committee (2011)
	…the general awareness, attitude and behaviour of its employees and appointed representatives to risk and the management of risk within the organisation.	FSA (2006)
	…the norms and traditions of behavior of individuals and of groups within an organisation that determine the way in which they identify, understand, discuss, and act on the risks the organisation confronts and the risks it takes.	IIF (2009)
	…the values, beliefs, knowledge and understanding about risk shared by a group of people with a common purpose, in particular the employees of an organisation or of teams or groups within an organisation.	IRM (2012)
	…the system of values and behaviors present throughout an organisation that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits.	KPMG (2010)
	...the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss, and act on the organisation's current and future risks. It is the last line of defence in grave situations.	McKinsey (2010)
	…organisational behaviours and processes that enable the identification, assessment and management of risks relative to objectives ranging from compliance to operational, financial and strategic.	PWC (2009)
	…the norms and traditions of behavior of individuals and groups within an organisation that determine the way in which they identify, understand, discuss and act on the risks the organisation confronts and takes.	Towers Watson (2011)
Academic literature	The organisation's propensity to take risks as perceived by the managers in the organisation.	Boseman and Kingsley 1998
	A risk culture is based on particular beliefs and assumptions. These can be clustered according to specific cultural tenets, namely risk, integrity, governance and leadership, decision-making, empowerment, teamwork, responsibility and adaptability… These tools are expressed in everyday workplace practices via attitudes and behaviours and, when they are expressed by leaders, they serve as powerful (human) culture embedding mechanisms.	O'Donovan (2011)

Table 1: Selected definitions

Each of these definitions are different, but there is a common thread that runs through almost all of them (except IRM, 2012) – that risk culture relates to the behaviour of the people within an organisation in relation to risk management. Behaviour influences both the effectiveness of an organisation's risk management processes and, as reflected in some of these decisions, the nature of its risk taking and control decisions (e.g. IIF, 2009; KPMG 2010).

Significantly, none of the above practitioner definitions reflect the culture-as-process orientation of Schein's popular definition of organisational culture as:

> "…a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration, which has worked well enough to be considered valid and, therefore, taught to new members as the correct way to perceive, think and feel in relation to those problems." (Schein, 2010: 18)

Instead the practitioner definitions tend to explain risk culture by reference to discrete dimensions, through which the behaviours of decision makers are affected. It could be argued that this approach helps to simplify the concept of risk culture, making it more tractable for measurement and management. Not surprisingly, the measurement of risk culture is the focus of recent practice survey studies (see Table 2), and there are many guidance and toolkits to measure and manage the 'risk culture' of an organisation (see Table 3).

Source	Title
Deloitte (2011)	Global Financial Services Risk - Management Survey
Deloitte (2011)	Global risk management survey
E&Y (2011)	Making strides in financial services risk management
EIU (2009)	Beyond box-ticking - A new era for risk governance
IRM (2011)	Risk management embedding and risk culture - survey
KPMG (2009)	Never again? Risk management in banking beyond the credit crisis
KPMG (2010)	Risk Management - A Driver of Enterprise Value in the Emerging Environment
Marsh (2012)	Risk management benchmarking survey results

Table 2: Selected surveys including questions on 'risk culture'

Source	Title	Notes
Deloitte (2009)	Solvency II and SST - Beyond quantitative models	Road map for Solvency II, including a risk culture item
Deloitte (2010)	Insurance Learning-on-the-Go	Risk and solvency assessment, including a risk culture framework
Deloitte (2010)	Remuneration policies in the financial sector	Providing a risk culture framework
Deloitte (2011)	Human capital advisory services	Toolkit to include risk culture in performance assessment and reward
Deloitte (2011)	Risk and Regulatory Review - The risk return proposition	Toolkit on "how to make a strong risk culture your competitive advantage"
E&Y (2011)	Growth in uncertain times - The need for dynamic risk management	5 steps to "understand and drive the right risk culture"
IRM (2011)	Risk guidance paper appetite & tolerance	Risk culture diagnostic within risk appetite guidance document
IRM (2012)	Risk culture - Resources for Practitioners	IRM risk culture framework
KPMG (2008)	Understanding and articulating risk appetite	Framework on risk appetite including a risk culture item
McKinsey (2010)	Taking control of organizational culture	Risk culture framework and risk culture diagnostic approach
PWC (2007)	The risk culture survey	Risk diagnostic tool - Key attributes and key indicators of effective Risk management
PWC (2011)	Building effective risk cultures at financial institutions	A framework where "risk culture forms one of the underlying foundations for managing risk"

Table 3: Selected guidance/toolkits on 'risk culture'

Appendix II: Methods

We aim for collective knowledge production – working together with CROs and other relevant actors to arrive at a shared view of the cultural factors that drive risk taking and control within BOFIs. To this end, the research combines qualitative and survey methods. At the current stage, we explored the theme with initial interviews in nine organisations. These latter provide a breadth of perspective on the financial services sector, ranging from large providers of various types of financial services (e.g. insurance, investment and retail banking) operating on a global scale to much smaller organisations operating locally in the UK. A total of fifteen individuals have been interviewed, of which ten hold a senior position in the risk management area of the organisation (e.g. CRO or deputy CRO). Furthermore, we have enriched our understanding of the field with two additional interviews with relevant regulatory actors.

We have also developed a short survey instrument to capture different aspects of risk-taking and risk control activities, which would be administered within participant organisations by cooperating CROs. The main purpose will be to enable further discussion based on the survey's results by means of feedback sessions and focus groups.

An extended version of the survey has also been developed and will be administered within the membership of the Chartered Insurance Institute. This survey will enable us to obtain extensive data from across a significant sample of individuals working in the financial services sector.

Overall, our research activities are informed by an (ongoing) review of the literature and desk research of pertinent publicly available documents

Appendix III: Selective bibliography

Ashby, S. (2011) Picking up the pieces: Risk management in a post crisis world. London: Financial Services Knowledge Transfer Network.

Bozeman, B., Kingsley, G. (1998) "Risk culture in public and private organizations". Public Administration Review 58(2), 109-18.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (1992), Internal Control – Integrated Framework. AICPA, New York, NY.

FT.com (2010a) "Bad actions stick archbishop tells city". Financial Times, 4th October 2010.

FT.com (2010b) "Cultural change is key to bank reform". Financial Times, 25th March 2010.

Haimes, Y. (2009) "On the complex definition of risk: A systems-based approach". Risk Analysis 29(12), 1647-165.

Independent Audit (2011) It's all about behaviour: How boards are tackling behaviour and ethics. London.

IIF (2008) Financial services industry response to the market turmoil of 2007–2008. Washington DC: Institute of International Finance.

IIF (2009) Risk culture. Washington DC: Institute of International Finance.

IRM (2012) Risk culture: Guidance from the Institute of Risk Management. London: Institute of Risk Management.

Levy, C., Lamarre, E., Twining, J. (2010) "Taking control of organizational risk culture". McKinsey Working Papers on Risk 16 (February), 1-11.

Power (2007) Organized uncertainty: Designing a world of risk management. Oxford: Oxford University Press.

PwC (2009) The risk culture survey. London: PricewaterhouseCoopers.

Reason, J. (1997) Managing the risks of organizational accidents. Ashgate publishing Limited.

Reuters (2012) "CEO says banks need culture change to regain trust". 1st October 2012.

Schein, E. (2010) Organizational Culture and Leadership. San Francisco: John Wiley & Sons.

Simons, R. (1999) "How risky is your company?" Harvard Business Review 77 (May-June), 85-94.

Simons, R. (1995) Levers of control: How managers use innovative control systems to drive strategic renewal. Boston, MA: Harvard Business School Press.

Sants, H. (2010a) "Do regulators have a role to play in judging culture and ethics?" Speech to Chartered Institute of Securities and Investments Conference, London, UK.

Sants, H. (2010b) "Can culture be regulated?" Speech to Mansion House Conference on values and trust, London, UK.

Turner, B. (1978) Man-Made disasters. London: Wykeham Publications.

Wheatley, M. (2012) "The incentivisation of sales staff – Are consumers getting a fair deal?" FSA speech, 5th September 2012.

Appendix IV: The research team

Principal Investigator

Michael Power is Professor of Accounting and Director of the Centre for the Analysis of Risk and Regulation (CARR) at the London School of Economics. He is a Fellow of the Institute of Chartered Accountants in England and Wales (ICAEW), an Associate member of the UK Chartered Institute of Taxation and an Honorary Fellow of the Institute of Risk Management. Since May 2005 he has been a non-executive Director of St James's Place plc where he is chair of the risk committee. In 2009 he was awarded an honorary doctorate in Economics by the University of St Gallen, Switzerland. His research and teaching focuses on regulation, accounting, auditing, internal control and risk management. His major work, *The Audit Society: Rituals of Verification* (Oxford 1997) has been translated into Italian, Japanese and French. *Organized Uncertainty: Designing a World of Risk Management* (Oxford 2007) has been translated into Japanese. He has given evidence to both the UK Treasury Committee and the House of Lords Economic affairs committee regarding the role of auditors.
Email: m.k.power@lse.ac.uk

Simon Ashby is Associate Professor in Financial Services at the Plymouth Business School and Head of the Accounting and Finance Discipline Group. Prior to this he was a Lecturer in Risk Management at Sheffield Hallam University and the University of Nottingham, a regulator (writing policy on risk management at the UK Financial Services Authority), and a practicing risk manager in a number of large and small banks. Simon has a PhD in corporate risk management and has published many academic papers in respected journals (e.g. British Journal of Industrial Relations, Geneva Papers, Safety Science, Risk, Decision and Policy), book chapters, professional articles and industry reports in the fields of risk management and financial services. This recently included a major study into the causes of the financial crisis and the risk management lessons that need to be learned (*Picking up the Pieces: Risk Management in a PostCrisis World*). Simon remains actively involved in the financial services sector and is a Fellow and the Chairman-Elect of the Institute of Operational Risk.
Email: simon.ashby@plymouth.ac.uk

Tommaso Palermo is a postdoctoral fellow at the London School of Economics – Department of Accounting. Tommaso has a PhD in Management, Economics and Industrial Engineering (Politecnico di Milano, Italy). His research and teaching focuses on the roles and uses of management control systems, the relation between risk management and performance management, and management accounting innovations in the public sector.
Email: t.palermo@lse.ac.uk

**Centre for Analysis
of Risk and Regulation**

The London School of Economics and Political Science
Houghton Street
London WC2A 2AE

tel: +44 (0)20 7955 6577
fax: +44 (0)20 7955 7420
email: risk@lse.ac.uk

lse.ac.uk/CARR