The EY Global Financial Services Institute brings together world-renowned thought leaders and practitioners from top-tier academic institutions, global financial services firms, public policy organizations and regulators to develop solutions to the most pertinent issues facing the financial services industry.

The Journal of Financial Perspectives aims to become the medium of choice for senior financial services executives from banking and capital markets, wealth and asset management and insurance, as well as academics and policymakers who wish to keep abreast of the latest ideas from some of the world’s foremost thought leaders in financial services. To achieve this objective, a board comprising leading academic scholars and respected financial executives has been established to solicit articles that not only make genuine contributions to the most important topics, but are also practical in their focus. The Journal will be published three times a year.

gfsi.ey.com

The articles, information and reports (the articles) contained within The Journal are generic and represent the views and opinions of their authors. The articles produced by authors external to EY do not necessarily represent the views or opinions of EYGM Limited nor any other member of the global EY organization. The articles produced by EY contain general commentary and do not contain tailored specific advice and should not be regarded as comprehensive or sufficient for making decisions, nor should be used in place of professional advice. Accordingly, neither EYGM Limited nor any other member of the global EY organization accepts responsibility for loss arising from any action taken or not taken by those receiving The Journal.
Editorial

Editor
Shahin Shojai
EY, U.A.E.

Advisory Editors
Dai Bedford
EY, U.K.
Shaun Crawford
EY, U.K.
Carmine DiSibio
EY, U.S.

Michael Lee
EY, U.S.
David Gittleson
EY, U.K.
Bill Schlich
EY, U.S.

Special Advisory Editors
H. Rodgin Cohen
Sullivan & Cromwell LLP
J. B. Mark Mobius
Franklin Templeton
John A. Fraser
UBS AG
Clare Woodman
Morgan Stanley

Editorial Board
Emilios Avgouleas
University of Edinburgh
Deborah J. Lucas
Massachusetts Institute of Technology
John Armour
University of Oxford
Massimo Massa
INSEAD
Tom Baker
University of Pennsylvania Law School
Patricia A. McCoy
University of Connecticut School of Law
Philip Booth
Cass Business School and IEA
Tim Morris
University of Oxford
José Manuel Campa
IESE Business School
John M. Mulvey
Princeton University
Kalok Chan
Hong Kong University of Science and Technology
Richard D. Phillips
Georgia State University
J. David Cummins
Temple University
Patrice Poncet
ESSEC Business School
Allen Ferrell
Harvard Law School
Michael R. Powers
Tsinghua University
Thierry Foucault
HEC Paris
Andreas Richter
Ludwig-Maximilians-Universitaet
Roland Füss
University of St. Gallen
Philip Rawlings
Queen Mary, University of London
Giampaolo Gabbi
SDA Bocconi
Roberta Romano
Yale Law School
Boris Groysberg
Harvard Business School
Hato Schmeiser
University of St. Gallen
Scott E. Harrington
The Wharton School
Peter Swan
University of New South Wales
Paul M. Healy
Harvard Business School
Paola Musile Tanzi
SDA Bocconi
Jun-Koo Kang
Nanyang Business School
Marno Verbeek
Erasmus University
Takao Kobayashi
Aoyama Gakuin University
Ingo Walter
New York University
Howard Kunreuther
The Wharton School
Bernard Yeung
National University of Singapore
Executive summaries

A brave new world? Making sense of practitioner and regulator perspectives on risk culture
by Simon Ashby, Associate Professor of Financial Services, Plymouth University, Michael Power, Professor of Accounting, London School of Economics and Tommaso Palermo, Lecturer in Accounting, London School of Economics

The risk culture of financial organizations is a popular area of focus at the current time, with regulators, advisory organizations, professional/trade institutes and financial organizations themselves all providing their view on the subject. However, despite the wealth of commentary there remain many unanswered questions, and to the extent that there is any consensus, there is a danger of overemphasizing certain elements. We provide a critical, but constructive, review of the practitioner literature on risk culture, the aim being to shed further light on some key questions. Specifically: what does risk culture do, can risk culture be modeled, is there a risk culture ideal (in terms of the elements of an appropriate risk culture) and can risk culture be regulated? We argue that there are no easy answers to these questions, and we also challenge some of the existing answers that have been provided. We suggest that to better answer these questions there is a need to look beneath the tip of the risk culture iceberg, focusing less on the more tangible and visible aspects of risk culture (incentives, risk management processes and procedures, etc.) and more on the human-social elements of organizations (such as communication networks and social relationships).
A brave new world?  
Making sense of practitioner and regulator perspectives on risk culture

Simon Ashby
Associate Professor of Financial Services, Plymouth University

Michael Power
Professor of Accounting, London School of Economics

Tommaso Palermo
Lecturer in Accounting, London School of Economics

Abstract
The risk culture of financial organizations is a popular area of focus at the current time, with regulators, advisory organizations, professional/trade institutes and financial organizations themselves all providing their view on the subject. However, despite the wealth of commentary there remain many unanswered questions, and to the extent that there is any consensus, there is a danger of overemphasizing certain elements. We provide a critical, but constructive, review of the practitioner literature on risk culture, the aim being to shed further light on some key questions. Specifically: what does risk culture do, can risk culture be modeled, is there a risk culture ideal (in terms of the elements of an appropriate risk culture) and can risk culture be regulated? We argue that there are no easy answers to these questions, and we also challenge some of the existing answers that have been provided. We suggest that to better answer these questions there is a need to look beneath the tip of the risk culture iceberg, focusing less on the more tangible and visible aspects of risk culture (incentives, risk management processes and procedures, etc.) and more on the human-social elements of organizations (such as communication networks and social relationships).
Introduction
Interest in risk culture has increased significantly in recent years. Where financial organizations and their regulators once spent their time and energy on quantifying risk and developing risk models for regulatory capital purposes, now they are diverting more of their attention to the “softer” topic of risk culture.

Events such as the financial crisis, as well as the more recent LIBOR, Payment Protection Insurance and “London Whale” scandals have played a key part in stimulating this growth in interest. In each case, a variety of post-mortems have identified “weaknesses” in risk culture as playing a key causal role. Moreover, regulators are looking to combat these weaknesses in risk culture via much more direct supervision, as exemplified by the recent Financial Stability Board (FSB) paper on risk culture [FSB (2014)].

All of this interest has generated a lot of “output”, especially on the part of advisory organizations, professional institutes and regulators. Risk culture, it would seem, is very much on trend. A review of this output reveals that there are areas where consensus is emerging, though whether this consensus is targeting the right issues/elements is another matter. However, there remain many unanswered questions and we are a long way from identifying the common elements (whether positive or negative) that may comprise an organization’s risk culture, or agreeing how to monitor and manage risk culture effectively - if indeed such utopian ideals really exist.

In what follows we provide a critical, but constructive, review of the growing regulatory and practitioner literature on risk culture. Identifying some of the key questions that have been explored in the literature and providing a more academic perspective based on our research project that investigated “Risk culture in financial organizations” [Power et al (2013)]. Our aim is to shed further light on the meaning and management of risk culture, while at the same time helping to avoid some blind and potentially destructive alleys.

Each of the questions outlined below relates to a key component in the discourse on risk culture. Notably, we explore questions on the role of risk culture, the elements of a “strong” risk culture and whether risk culture can actually be modelled or regulated. The answers to these questions are far from straightforward, and it is likely that they can
never be answered in full. Nevertheless, if we are to better understand risk culture, more considered answers to each of these questions are required. We end our paper with a brief conclusion and reflection on the future of risk culture in financial organizations.

**Question 1: What does risk culture actually do?**

Risk culture is often perceived as an enabler, helping to improve the effectiveness of risk management decisions and embed processes and procedures relating to governance, risk and compliance (GRC). Here, the focus is on controlling and limiting risk, risk culture being a mechanism for reinforcing more visible policies and procedures (enabling, embedding and controlling perspective), though in a few cases it is acknowledged that risk culture may support risk-taking, as well as control (the risk taking and control perspective).

A good example of the enabling, embedding and controlling perspective on risk culture comes from Protiviti (2012). In a survey of insurance firms Protiviti explains that risk culture is a “vital component” (p3) in the effectiveness of risk management processes and practices, helping employees to understand and accept that risk management is “part of everyone’s role and responsibility” (p3). Protiviti also stresses the importance of ‘aligning’ risk culture with an insurer’s risk management framework and practices.

Several of the larger audit/consulting firms (e.g., KPMG and PWC) share the enabling, embedding and controlling view. KPMG [Farrell and Hoon (2009)] emphasizes the behavioral and internal control aspects of risk culture, suggesting that it is a means to ensure that employees are “doing the right thing” and that they “understand risk and compliance rules,” leading them to make appropriate decisions. This is further developed in KPMG (2011), where risk culture forms the foundations for effective risk management — underpinning three more tangible pillars of effectiveness: risk identification and assessment, risk quantification/mitigation and risk monitoring/reporting.

Similarly PWC (2012) links risk culture to “effective and sustainable ERM,” suggesting that risk culture helps employees to understand the level of “acceptable” risk along with how risk information should influence their decisions. PWC further makes the claim that there are “studies” which show that a strong risk culture can lead to a reduction in loss events,
A brave new world? Making sense of practitioner and regulator perspectives on risk culture

along with better performance management; however, no evidence is provided to back up this claim. We are not aware of any such studies.

In comparison, EY [De Jonghe et al. (2013)] adopts a risk-taking and control perspective on risk culture. The authors argue that risk appetite and risk culture are closely related “reinforcing” mechanisms. The mechanism for this relationship is that an organization’s stated risk appetite should affect decision-making behaviors and hence risk culture; while an organization’s risk culture helps to determine whether its stated risk appetite is embedded and accepted. So in this respect risk appetite is seen to represent a more formal and tangible perspective on risk attitudes; risk culture a more informal and implicit one. The authors go on to suggest that a “strong” risk culture will allow organizations to achieve an appropriate balance between risk and return, while those with “weak” risk cultures will either take too little or too much risk – though excessive risk-taking is assumed to be the most common case.

Regulatory and professional organizations have also commented on the role of risk culture. An important example of the risk-taking and control perspective comes from the Institute of International Finance (IIF, 2009), which comments that: “A robust risk culture is a substantial determinant of whether a firm is able successfully to execute its chosen strategy within its defined risk appetite ... The risk appetite determined by the firm will be only as effective as the formal and informal network in which such appetite is disseminated as well as the way in which it shapes employees’ decision making. Having in place set processes and controls is not enough to give Boards and executives confidence that the risk appetite they set will be adhered to; they must ensure that all employees be aware of what risks they are taking, make the right decisions, and raise objections when necessary – the key attributes of a strong risk culture.” [IIF (2009), pAIII.1]

So here, as with EY, risk culture and risk appetite are seen as mutual reinforcing organizational features (risk appetite being a more visible manifestation of an organization’s risk culture). This point is reiterated in the IIF’s definition of risk culture: “Risk culture can be defined as the norms and traditions of behavior of individuals and of
groups within an organization that determine the way in which they identify, understand, discuss, and act on the risks the organization confronts and the risks it takes.” [IIF (2009), pAIII.2]

Less clear-cut is the work of the Institute of Risk Management [IRM (2012)]. At first, the IRM links risk culture to an organization’s ability to manage downside risks; however, later they explain that certain risk cultures may also stifle risk-taking. So, while their work arguably fits best with the risk-taking and control perspective, it also highlights a tension between risk-taking and control. Even within the IRM’s and EY’s work, risk management and risk culture are linked to reducing downside risk or at best, the downside elements of more speculative risks. It would seem that there is a persistent notion in parts of the practitioner community that risk is predominantly bad and should only be taken grudgingly to achieve strategic objectives. Risk culture, therefore, is predominantly consigned to a risk reduction role.

Regulatory views on the role of risk culture are much less ambiguous and are clearly aligned with the enabling, embedding and controlling perspective. This is especially evident in the work of the Basel Committee (see Question 4, below), which talks about a risk management culture, rather than a risk culture. The idea being that culture underpins processes and procedures for the management, and predominantly the reduction, of risk, including rigid structural control tools, such as the three lines of defense approach to risk governance.

Similarly, the FSB’s earlier work on risk culture very much emphasized the enabling, embedding and controlling perspective, the focus being on risk culture as a risk reduction/avoidance tool. The FSB’s original November 2013 consultation paper on the supervision of risk culture exemplifies this viewpoint (see especially the underlined statement): “A financial institution’s risk culture plays an important role in influencing the actions and decisions taken by individuals within the institution and in shaping the institution’s attitude toward its stakeholders, including its supervisors. A risk culture that promotes prudent risk-taking and discourages unrestrained profit maximization without due regard to risks supports an environment that is conducive to ensuring that emerging risks that will have a material impact on a financial institution, and any risk-taking activities
A brave new world? Making sense of practitioner and regulator perspectives on risk culture

beyond the institution's risk appetite, are recognized, assessed, escalated, and addressed in a timely manner.” [FSB (2013), p1]

This highly risk averse perspective creates the danger of a prudence drag, whereby risk culture is used to reduce risk-taking to such an extent that it may damage the long-term financial sustainability of financial organizations. While we accept that a financial organization's risk culture can help to provide an implicit constraint on what might be considered “bad” risk management behaviors, such as excessive risk-taking, or resistance to GRC-related processes and procedures, we do not accept that risk culture is only about control. Risk management is equally about effective risk-taking; financial organizations have to take risk in order to achieve a return and, in the light of events such as the financial crisis, it would seem wise to incorporate risk-taking within organized risk management activities. Therefore, it stands to reason that the role of a financial organization's risk culture is to support, in equal measure, both its risk-taking and control activities.

Our research on “Risk culture in financial organizations” supports this argument. While the organizations we visited recognized the controlling aspects of risk culture, many also accepted that risk culture can have a more strategic, risk-taking, role. The trick, of course, is to develop a culture that facilitates the “right” sort of risk taking (i.e., taking those risks that generate an expected level of return that is sufficient to offset any associated volatilities), while reducing those risks that may threaten the reputation, efficiency or financial viability of the organization.

That is not to say that these organizations placed no limits on risk-taking. Rather, they used their risk appetite frameworks to significant effect, in order to limit certain types of risk. However, within this limit framework they were also prepared to take risks, providing such risks were properly understood and generated appropriate levels of reward. This reflects the notion of core/value adding business risks versus non-core preventable or external risks [see Nocco and Stultz (2006); Kaplan and Mikes (2012)], where some of our participants did not see the risks directly associated with their primary business activities (e.g., insurance underwriting or credit provision) as being “risky” in the same sense as their
non-core risks – since taking these core business risks was an essential part of their mission and identity.

One participant took this point a little further, acknowledging the acceptability of risk taking in certain contexts: “people can play within the sandbox;” going on to state that senior management and the directors of the organization are the “guardians of the sandbox and the toys within it.”

We labeled such organization's “sandbox guardians” since, while they placed limits on risk within certain areas/activities, they also permitted and even encouraged risk taking in other areas – especially in relation to new strategic initiatives. Hence, protected sandbox environments were created to allow risk taking where appropriate and within a suitably monitored and protected environment.

In this vein, it is worth noting that the FSB removed all references to prudence in its final guidance on risk culture [FSB (2014)], which was in response to some negative feedback on the original 2013 paper (see Question 4 below). The FSB's revised work is certainly much closer to that shared by the “sandbox guardians” that we observed, however the tone remains highly procedural and governance orientated: “A sound risk culture consistently supports appropriate risk awareness, behaviors and judgments about risk-taking within a strong risk governance framework. A sound risk culture bolsters effective risk management, promotes sound risk-taking, and ensures that emerging risks or risk-taking activities beyond the institution's risk appetite are recognized, assessed, escalated and addressed in a timely manner.” [FSB (2014), p1]

This raises further questions about the central role of risk culture. While an organization's risk culture may well support the operation of formal risk management and risk governance processes, risk culture can also be used to support flexible and adaptive risk-taking, helping financial organizations to make risky decisions in complex environments with competing stakeholder expectations and to even deviate from the “rules” from time to time, especially in response to unfamiliar circumstances (e.g., to seize a new opportunity or respond to a crisis).
From an academic perspective the work of Weick and Sutcliffe (2007, Ch. 6) provides an interesting perspective on this last point. Weick and Sutcliffe argue that the role of culture from a risk perspective is to help promote a collective sense of the diverse/ changing nature of risk and uncertainty (i.e., “mindfulness” or big picture “situation awareness”), as well as to support collective and coordinated action in response to this dynamic environment. In such a context, rigid processes and procedures, including defined risk limits, may be more of a hindrance than a help. Instead, what may be more important is a flexible culture, which adjusts to sudden changes; in conjunction with a learning culture, where there is a preparedness to revise pre-existing assumptions and convert “lessons learned” into action.

**Question 2: Positivism and auditability, can risk culture be modeled?**

Nearly all advisory, professional and regulatory organizations adopt a modeling perspective, and identify a range of elements that can be used to assess and benchmark organizational risk cultures. These elements are then distilled into a smaller number of broader factor categories, which are often presented in graphical form (for example, using some form of “wheel” in which the various spokes are grouped according to the broader factor categories).

**Table 1** provides a summary of the factor categories that have been identified by organizations that have developed relatively formal “models” of risk culture.

From **Table 1**, it is clear that there are many differences between the proposed “models” of risk culture. However, some factor categories are more popular and common than others. One popular factor is leadership and “tone from the top” in particular, a concept borrowed from the mainstream literature on organizational culture and in particular Schein (2010). Also popular are categories relating to compensation and performance.

---

1. We understand that EY is developing a new model, but no public information is currently available. The new model includes four main factors: incentives, leadership, organization (governance structure and accountability) and “risk framework” (communication and risk appetite).
2. The IRM’s 4 categories of “tone at the top”, “decisions”, “governance” and “competency” are quite broad and cover more than 3-4 of the factors listed here. The same is also the case for the IIF (2009), PWC (2012) and Towers Watson [Davidson et al. (2012)].
3. Table 1 represents an updated version of the table found in Power et al. (2014).
management – the idea being that risk culture is reflected in the financial motivations of employees. Similarly, organizational structure and governance is a common category, as is risk communication and reporting. This further reinforces the notion of risk culture as a control tool – it being reflected in how employees are constrained in terms of their decision making (through monitoring, incentives, etc.).

What we also observe within the modeling perspective is a strong philosophical bias toward the measurement and auditability of risk culture, especially on the part of advisory organizations. Following the review of an organization's risk culture, using an advisory organization's model, it then follows that “gaps” are identified and actions/interventions planned and executed in order to close these “gaps”. It is also common for these advisory organization models to generate percentage risk scores for the identified risk culture factors, scores which may then be rated as “red”, “amber” or “green” (RAG). No significant public information is provided on the mechanisms used to generate these scores or the means by which RAG thresholds have been determined. However, we presume that the idea here is to help organizations to somehow quantify their risk culture and prioritize “weaknesses” that require action.

The modeling perspective reflects the persistent managerialist notion that “if it can't be measured, it can't be managed,” a quote often misapplied to the management guru Prof. Peter Drucker4 and even repeated in the IRM’s work to develop their Risk Culture Aspects Model TM [IRM (2012, p13)]. However, a fuller investigation of the works of management gurus, such as Drucker or Deming will reveal that they do not share the myopic notion that management requires measurement. Indeed, Deming explicitly warned against running a company on visible figures alone in his seven deadly diseases of management [Deming (1986)].

While we understand the desire to model and measure risk culture, we are concerned that there is too much emphasis on this in the current literature from advisory, professional and regulatory organizations. As we discovered from our own research, risk culture is an

4 See: http://thedx.druckerinstitute.com/2013/07/measurement-myopia/
A brave new world? Making sense of practitioner and regulator perspectives on risk culture

inherently pluralistic and fuzzy concept and attempts to model it in one specific way will provide a partial picture at best, possibly even a misleading one. That is not to say that some of the more visible elements of risk culture cannot be modeled (e.g., those that relate to processes, procedures or organizational structures and possibly even “tone”). However, these elements represent the tip of the cultural iceberg.

Many of the financial organizations that we visited had taken steps to assess their risk culture, with a view to identifying weaknesses in their risk cultures or even validate a notion amongst senior management that they had a strong risk culture. However, in many cases there was skepticism about the relatively generic risk culture models developed by advisory organizations.

Risk culture is something that can be very idiosyncratic and specific to a financial organization and, to date, attempts to model it in general terms have added little to our understanding of the concept. While advisory, professional and regulatory organizations have the advantage of a helicopter view – being able to examine multiple organizations and share practice – their attempts to model risk culture often remain at the level of abstract principles. What is needed is an approach that can reflect the plurality of the concept and the range of trade-offs that need to be considered when assessing and managing risk culture. We return to this point in our discussion of Question 3.

**Question 3: Is there an ideal risk culture?**

Building on the modeling perspective from Question 2, there is a popular view among advisory, professional and regulatory organizations that it is possible to differentiate between “strong” and “weak” risk cultures and that organizational risk cultures can be managed toward some kind of utopian ideal (the idealist perspective). Though, just as with the risk culture elements identified in Table 1, there is less consistency over the specific attributes of a strong risk culture.

What also strikes us, when reviewing the factors summarized in Table 1, is that many reflect generic good management behaviors and structures/processes, rather than anything that might be considered risk culture specific. A good example of this is the Risk Intelligent Culture framework proposed by Deloitte (2012). Deloitte’s work highlights...
various “enablers” (for example: leadership commitment, communication, measurement and reporting and program management) to help “strengthen” an organization’s risk culture and promote “continuous cultural improvement.” [Deloitte (2012, p4)]. So here there are close parallels with the managerial concept of “total quality management” (TQM) and the established philosophy of “continuous improvement.”

EY appear to share the idealist perspective, [notably: De Jonghe et al. (2013)]; however, they draw more from “good” GRC practices, particularly using the results from their own 2011 post financial crisis survey of risk governance practices [EY (2011)]. EY emphasizes the following elements of a strong risk culture: a consistent “tone from the top,” appropriate metrics that are monitored regularly, effective escalation processes and an “open” culture in which employees feel able to raise concerns, and the enforcement of process/limit breaches. Such a GRC orientation is also shared by Protiviti (2012) that uses survey evidence to highlight two key factors: non-executive challenge on a firm’s risk management activities and the frequency of board discussions on risk management.

Building on this GRC orientation of the idealist perspective KPMG [Farrel and Hoon (2009)] and McKinsey [Levy et al. (2010)] add further examples of effective GRC behaviors and structures/processes for good measure:

- Leaders/managers, which set a clear risk strategy and support their organizations’ risk management policies and procedures, so that their teams know that non-compliance will not be tolerated (again this implies risk culture as a risk reducing control mechanism)
- The clear and consistent communication of an organization’s values and ethical codes of conduct by management
- Incentives to behave appropriately and “do the right thing” from both a risk management and an ethical perspective
- Having a consistent process for considering risk when making decisions
- Recruiting the right staff – those who are compatible with the prevailing risk culture

Professional institutes and regulators further reinforce the idealist perspective. One influential piece of work is by the Institute of International Finance [IIF (2009)], which devotes a lot of attention to the attributes of a strong risk culture and further links these
attributes to how risky decisions are governed and controlled. These attributes of a strong culture include: employee incentives, an effective governance structure with clear accountabilities for risk and risk tolerance limits, escalation of risk issues and the “tone from the top.” Thus, despite providing a relatively positive definition of risk culture, much of the IIF’s work on the elements of a “strong” risk culture further reinforce the view that risk culture primarily exists to limit risk-taking, not to facilitate it.

In contrast, the IRM explains that a “successful” risk culture should reflect an organization’s stance on both risk-taking and control/governance [IRM (2012)]. However, the IRM still outlines 10 (why this continued obsession with “top 10s”?) relatively generic elements of a successful risk culture, elements that include: “tone from the top,” commitment to ethical principles, risk reporting, acceptance of the importance of risk management, and so on.

The idealist theme continues with the regulatory literature on risk culture. Although in their latest work the FSB acknowledges the complexity associated with risk culture, they also emphasize three foundational elements of a “sound” risk culture: risk governance, risk appetite and employee compensation [FSB (2014)]. The FSB then specifies a number of indicators of a sound risk culture, built around four categories: “tone from the top,” “accountability” for risk taking and control, “effective communication and challenge” of risks and decision-making and finally “incentives”. Again, the quest for a risk culture ideal is very much in evidence, as is the generic managerial/governance nature of the FSB’s attributes.

While we understand the desire to identify the ideal attributes of a “strong” or “sound” risk culture, our own research suggests that this is a complex area characterized by a high degree of plurality. In short, what may be a strong attribute for one financial organization might be a weakness for another. For example, we found that some of the organizations we visited exhibited more of an organic approach to managing their risk culture, while others adopted what we call an “engineered” approach. Those more organic firms tended to place much less emphasis on formal controls, for example, relying instead on less formal networks of social interaction. In the absence of any clear evidence, who is to say that one approach is better than the other? Tensions were also identified in our research in the
implementation of the increasingly centralized and “independent” risk oversight functions that many (such as the IIF and FSB) emphasize as important elements in developing a “strong” or “sound” risk culture. However, again we observed that too much centralization and independence can drive a wedge between the risk function and other business functions, preventing joined up decision-making. As one of our project participants observed on the issues of centralization and independence [Ashby et al. (2012, p15)]: “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.”

That does not mean to say that there may be no common attributes of a strong risk culture, especially if these attributes are presented at a sufficiently macro level. However, the current piecemeal approach, and a lack of evidence to support the claims made by different organizations (including regulators), means that it is impossible to verify the proposed attributes of a strong risk culture. Identifying the attributes of a strong/sound risk culture will require careful evidence-based research, using appropriate investigative techniques (e.g., ethnographic study). In our own work, for example, we identify a number of trade-offs that can be involved in achieving a suitable risk culture, as well as the dangers of risk culture drift - where financial organizations may fail to review and manage their risk cultures in a mindful way. However, our work only represents the first tentative steps toward the development of a grounded theoretical framework based on observed practices that are consistently proven to be effective.

**Question 4: Can risk culture be regulated?**

The growth in political and regulatory attention to risk culture began following the financial crisis, and there appears to be increasing consensus within the international regulatory community that risk culture can and should be subject to regulatory supervision (the regulatory perspective). This is especially striking given the community’s previously ambivalent stance on regulating risk management practices: “It is not the Committee’s intention to dictate the form or operational detail of banks’ risk management policies and practices.” [Basel (2006, p 2)]
In terms of regulating risk culture, the Basel Committee offered some initial thoughts in its 2009 Basel 2.5 reforms, which were developed further in guidance for internationally active banks and their supervisors on corporate governance [Basel (2010)] and operational risk management [Basel (2011)]. These two guidance documents have a strong focus on the more tangible and structural GRC aspects of risk culture, with the committee highlighting factors such as compensation policies (suggesting they should be long-term and linked to clear risk management objectives) and the role of risk culture in helping to cement the three lines of defense approach to governance (e.g., by helping decision-makers to understand and accept their roles and those of the other three lines). However, the Basel Committee did not completely ignore the more behavioral aspects of risk culture. Notably, in the governance guidance paper [Basel (2010)] the Committee calls for the development of corporate cultures that highlight and embed appropriate norms and incentives for professional and responsible behavior, linking this to the creation of an appropriate “tone from the top” and the setting of professional standards, values and incentives that promote integrity and clarify appropriate and inappropriate behaviors. This view was reiterated in the Committee’s operational risk paper [Basel (2011)], where “Principle 1” states that a bank’s “risk management culture” must embody professional and responsible behaviors (though they do also state that standards and incentives must be set to ensure that these behaviors are adopted). The paper also suggests a link between a bank’s risk management culture and ethical business practices – though this is not developed further.

However, the most significant international regulatory development on risk culture has come from the FSB, whose work we have already commented on at several points above. Although the FSB may not have direct rule-making powers, it has influence over the direction of both international and domestic regulatory regimes, and as such the FSB’s work represents a landmark shift in the regulation and supervision of risk culture. The FSB make it very clear that supervisory attention to risk culture is an important part of their mission to increase the intensity and effectiveness of supervision and act more preemptively in relation to activities and behaviors that supervisors believe may threaten the financial system [see FSB (2013, 2014)]. The FSB adds that supervisors are in a “unique position” [FSB (2014, p4)] to gain insights into the risk cultures of financial organizations, given their privileged access rights across the sector.
Closer to home, the E.U.’s recently published Capital Requirements Directive (CRD IV) includes a new regulatory requirement on risk culture, stating that: “Member States should introduce principles and standards to ensure effective oversight by the management body, promote a sound risk culture at all levels of credit institutions and investment firms ...” [DIRECTIVE 2013/36/EU, paragraph 54]

This statement enshrines in European law the importance of risk culture for banking and securities organizations, but provides no further explanatory detail. As is customary under the Lamfalussy process of European regulation further policy development is left to the European Banking Agency (which replaced the Committee of European Banking Supervisors) along with local regulatory agencies, such as the Prudential Regulatory Authority and the Financial Conduct Authority in the U.K. To date, little further regulation has been forthcoming, though that is not to say that local regulators are not talking about it, as indicated in the U.K., below.

Though international regulators may be looking to increase the level of regulatory and supervisory scrutiny over risk culture, many outside of this community have concerns about this development. This skepticism about regulation perspective is exemplified in some of the responses to the FSB’s consultation paper on risk culture, which both questions the ability of supervisors to assess risk culture effectively and, in some cases, suggests that risk culture supervision may do more harm than good.

A good example of this skepticism perspective comes from Paradigm Risk Consulting’s response to the FSB consultation paper on risk culture [Paradigm Risk (2014)]. Paradigm Risk suggests that regulators have climbed on the “risk culture bandwagon” (p5) and that the FSB’s approach is overly superficial and lacks an appropriate academic foundation. In this regard, they suggest that the risk culture indicators proposed by the FSB do not get sufficiently deep into the less visible human/social aspects of risk culture. They also warn

---

5 See: http://www.fsa.gov.uk/about/what/international/european/lamfalussy
6 For one key exception see CEBS (2010), which provides further European level guidance on risk culture in its high level principles for risk management. This includes the importance of creating a “strong, institution-wide, risk culture,” as well as an enterprise-wide risk function that covers all risks and is independent. So again there is a strong internal control theme.
of a nonlinear relationship between management action and risk culture (linking this to chaos theory), where formal attempts to manage risk culture through the use of risk culture indicators may promote an overly mechanistic checklist approach, which leads to ineffective and potentially counterproductive interventions. Paradigm Risk is particularly skeptical of supervisory efforts to intervene in risk culture: “The presumption of efficacy of supervisory intervention in relation to culture or ‘risk culture’ rests on the sequence of reliability of observation and diagnosis through to reporting and prescription for action in the firm and the absence of unintended consequences. Supervisors should regard intervention in relation to specific behaviors or cultural elements as a ‘nuclear option’.” [Paradigm Risk (2014, p19)]

They go on to state that: “The presumption that supervisors will know pretty quickly what is a firm’s culture is simply hubristic; the expectation that they will be able to prescribe an effective solution is more so. While specific behaviors are safer ground for intervention, firms are unlikely to respond to such intervention in the way the supervisor may desire; response internally is equally likely to be personalized and punitive as enlightened and effective.” [Paradigm Risk (2014, p19)]

Though less critical of the FSB’s proposals, HSBC makes it clear that it is for the board and senior managers to assess risk culture, not supervisors, who they believe may lose their objectivity if their constant assessment of risk culture means they get too close to the organizations they are supervising [HSBC (2014)]. HSBC also warns that the FSB’s proposed approach to risk culture supervision may result in supervisors becoming “shadow directors” (p4), who become too involved in decision-making. Likewise, the CRO Forum of European insurance company Chief Risk Officers [CRO Forum (2014)] state that supervisors should not supervise risk culture directly, but only consider it via an assessment of risk appetite. They also challenge the FSB’s original notion [FSB (2013)] that a sound culture should be a prudent one, explaining that financial organizations have to take risk to remain in business. They state that: “CRO Forum members strongly believe that risk culture, together with risk appetite, should not necessarily reflect a prudent approach, but fit the business purpose of the firm.” [CRO Forum (2014, p1)]

Finally, several respondents challenge the elements of a sound risk culture proposed by the FSB (although many others do agree with them). For example, the Global Federation of
Insurance Associations states: “Best practices for risk culture are highly specific to each company and will vary depending on the nature, scale and complexity of the risk exposure …. What is a best practice for one company may not be a best practice for another company and yet the same level of policyholder protection can still be achieved.” [GFIA (2014, p2)]

This view is also supported by the International Actuarial Association: ““Culture” is a much more complex and fluid notion than suggested in the paper, and this needs to be recognized more explicitly lest regulators end up with a very narrow view of this important factor.” [IAA (2014, p2)]

The International Actuarial Association also warns of some damaging consequences from the regulation and supervision of risk culture: “Forcing all institutions into a single culture will greatly increase systemic risk since if there is any flaw in the proscribed risk culture, the entire financial sector will be subject to risks that are taken or mismanaged because of that flaw. Variety of practice, not uniformity, is an important aspect of systemic resilience.” [IAA (2014, p4)]

“Willingness to document things for the supervisor is not, in and of itself, an indication of risk culture. Documentation needs to be sufficient to convey the intended risk culture in situations where that is not being well conveyed by interpersonal communications. Over documentation of a good risk culture may end up undermining that culture, making it seem more like a set of restrictive rules when, in fact, it is a process of empowering employees to make good risk decisions on behalf of the company.” [IAA (2014, p6)]

In terms of the U.K. regulation neither the PRA or the FCA (or the former FSA) has produced specific regulation on risk culture. However, both the PRA and FCA have indicated that culture and risk culture are areas they intend to consider when supervising firms (as supervisors have always done, albeit informally). More concerning is the link made between risk culture and prudence, with the PRA making clear that to meet its Principle of Safety and Soundness banks and insurers must have a culture that supports this
A brave new world? Making sense of practitioner and regulator perspectives on risk culture

The PRA also states that it expects banks and insurers to “minimize incentives for excessive risk taking” via: appropriate incentives; ensuring that responsibilities for risk management are considered as a central part of front line management and through risk and control functions that carry “real weight.”

The FCA is even less specific and prescriptive, but has laid out its position in a speech by Clive Adamson [Adamson (2013)]. Here, Adamson suggests that the FCA will not assess or legislate on culture directly, but that it will “join the dots” using a kind of meta-analysis of existing data and findings: “Our approach today is to draw conclusions about culture from what we observe about a firm – in other words, joining the dots rather than assessing culture directly. This can be through a range of different measures, such as how a firm responds to, and deals with, regulatory issues; what customers are actually experiencing when they buy a product or service from front-line staff; how a firm runs its product approval process and the considerations around these; the manner in which decisions are made or escalated; the behavior of that firm on certain markets and even the remuneration structures.” [Adamson (2013)]

As explained in Power et al. (2014), we find this joining the dots approach compelling and pragmatic. This approach reflects the plurality of risk culture practice and should help to minimize the potential for unintended consequences, through the absence of direct rules or guidance on risk culture. However, it is clear that such an approach will mean less regulatory certainty for financial organizations and require more judgment on the part of supervisors. To help detect the “hidden” clues about risk culture, supervisors will need to develop a disciplined approach to the gathering of field notes during the supervisory process, drawing on unfamiliar ethnographic skills. In our own activity as researchers, we reflected on how we were received and treated in the 14 different organizations where we were able to conduct interviews (e.g., whether we were offered refreshments, whether we were allowed to record interviews, the level of “small talk,” etc.). These and other dimensions of the way organizations are open to, and engage with, outsiders are potential indicators of their internal risk culture.

**Recommendations for senior managers and boards**

Given all these unanswered questions, it is difficult to be prescriptive about risk culture. However, that does not mean that it is impossible to provide any guidance for the senior
managers and boards of financial organizations. In particular, we would suggest that ignoring risk culture, and allowing your risk culture to drift, is not an option. Senior managers and boards must work to improve their awareness and understanding of their organization's risk culture, identifying areas where attitudes and behaviors (toward both risk taking and control) need to be challenged, as well as examining factors, such as the internal authority of the risk function, levels of interaction between “business facing” and “control” functions and how well management across the organization understand its appetite for risk.

Remember also that it is the senior managers/board who will understand an organization’s risk culture best. That does not mean advisory organizations, and possibly even regulators, have no role to play here, especially as they may have experience of a wider range of risk cultures. However, just because a particular risk culture works for one organization, does not mean that it will necessarily work for another. If any advisory organization that you talk to is unable to appreciate this then find one that does. Also, resist any attempts by regulators to mold your organization into a particular cultural stereotype (e.g., by forcing you to become excessively prudent).

Finally, on the management of risk culture, remember that it is neither easy nor wise to fundamentally change risk culture overnight, especially via large-scale, time-limited change projects. Except in extreme situations, the effective management of risk culture requires regular and often quite small-scale inputs to “nudge” an organization’s risk culture into the direction desired by senior managers/boards. We would also emphasize that while the management of risk culture may well involve making changes to tangible risk management processes, procedures and frameworks (risk appetite, risk reporting, risk assessment, etc.), it is the more human-social side of the equation that can have a deeper and more far reaching effect (e.g., by building effective relationships between business and risk functions, facilitating informal interaction between staff, challenging established perceptions about risk management, etc.).
Conclusions
The work by advisory, professional and regulatory organizations on risk culture makes an important contribution to our understanding of the concept and how it is both understood and managed within financial organizations. However, the advisory, professional and regulatory literature is characterized by a lack of consensus, coupled with a managerial orientation that is rooted in the belief that risk is “bad” and that risk culture is something that can be assessed and controlled in a highly structured way.

These mutually exclusive positions – vagueness over the nature and meaning of risk culture, coupled with a very structured and procedural approach to its management – do little to help progress the debate and may lead to stagnation in our understanding of risk culture.

Currently, there remain more questions than answers in the discourse on risk culture. While we are sure that there are more answers to be found, it is unlikely that these will be as black and white as some professional, advisory and regulatory organizations might like. Tangible risk management/governance structures and procedures represent the tip of the iceberg when understanding risk culture, which is much more about investigating the hidden clues that characterize how risk taking and control decisions are made within organizations, clues which are predominantly human-social, rather than structural or procedural. This refocusing on the more informal networks and relationships, which are an essential part of any organization’s risk-taking and control activities, will require a new set of skills for those concerned with the management and regulation/supervision of risk management. Whether the field of financial services is really prepared to embrace new forms of knowledge and practice remains to be seen.
References
CRO Forum, 2014, “CRO Forum response to consultative document on increasing the intensity and effectiveness of supervision from 18 November 2013,”
EY, 2013, “Remaking financial services: risk management five years after the crisis,” EYGM Limited, New York,
GFIA, 2014, “GFIA comments on FSB guidance on supervisory interaction with financial institutions on risk culture,” Global Federation of Insurance Associations
HSBC, 2014, “Consultative document - guidance on supervisory interaction with financial institutions on risk culture,” HSBC Holdings

A brave new world? Making sense of practitioner and regulator perspectives on risk culture
A brave new world? Making sense of practitioner and regulator perspectives on risk culture

KPMG, 2011, “Risk management a driver of enterprise value in the emerging environment,” KPMG International
Schein, E., 2010, Organizational culture and leadership, John Wiley and Sons, San Francisco
Weick, K., and K. Sutcliffe, 2007, Managing the unexpected: resilient performance in an age of uncertainty, John Wiley and Sons, San Francisco
Appendix

A brave new world? Making sense of practitioner and regulator perspectives on risk culture
APPENDIX: A brave new world? Making sense of practitioner and regulator perspectives on risk culture

Table 1: Summary of risk culture model factors by organization

<table>
<thead>
<tr>
<th>Factor categories</th>
<th>Deloitte</th>
<th>EY</th>
<th>FSB</th>
<th>IIF</th>
<th>IRM</th>
<th>KPMG</th>
<th>McKinsey</th>
<th>PWC</th>
<th>Towers Watson</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgement of risk (potential for over confidence, effective challenge)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication (regular risk reporting and escalation of risk issues)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compensation and performance management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Systems</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Leadership (&quot;tone from the top&quot;)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Relationships (between employees)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respect for risk (potential for gaming the system)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsiveness to risk (ability to react to risk issues)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk competencies (of employees)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk facilitation (status of risk function and ability to support business)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management processes and procedures</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk ownership (clear accountabilities)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy and budget (e.g., aggressive revenue targets, budget for risk function)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structure of organization and governance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited.
All Rights Reserved.
EYG No. CQ0146

ey.com

The articles, information and reports (the articles) contained within The Journal are generic and represent the views and opinions of their authors. The articles produced by authors external to EY do not necessarily represent the views or opinions of EYGM Limited nor any other member of the global EY organization. The articles produced by EY contain general commentary and do not contain tailored specific advice and should not be regarded as comprehensive or sufficient for making decisions, nor should be used in place of professional advice. Accordingly, neither EYGM Limited nor any other member of the global EY organization accepts responsibility for loss arising from any action taken or not taken by those receiving The Journal. The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

Accredited by the American Economic Association
ISSN 2049-8640