Auditing Risk Culture

Emma Price, Director Enterprise Risk

Introduction

In these turbulent economic times, the role of risk management and internal audit is increasingly critical for many reasons. Chief amongst these is that these two functions provide a real opportunity for the organisation to eliminate ineffective business practices that are hindering the achievement of strategic objectives, and to identify opportunities for business process improvements that can translate into real bottom line value.

In 2010 the UK Corporate Governance Code, which replaced the earlier Combined Code, stated in Provision C.2.1 that "The board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so".[1] This updated the earlier 2008 version of the code which referred only to the effectiveness of internal controls, and did not include any specific reference to risk management. Prior to this, the Institute of Internal Auditors (IIA) had already clearly outlined the need for internal audit to provide objective assurance over the effectiveness of the risk framework, [2] and in 2008 Standard and Poor's had announced its intention to enhance its credit rating process for non-financial companies through an ERM review.

However, what is not specifically stated is that the risk framework is the sum of many parts, not only policy, process and procedure, but also the behaviours, beliefs and values – that is the culture – of the organisation as regards risks. Providing a review over the effectiveness of the company's risk management framework therefore requires a consideration of the less tangible elements of risk culture through the operation of the framework, as well as looking at the effectiveness of the process design.

This paper focuses on the challenge of auditing risk culture as part of the assurance of the risk framework effectiveness, and looks at how in tough times, tough questions need to be posed to identify areas of opportunity.

What is risk culture?

Risk culture rose in prominence following the global financial crisis. In its 2009 report, the Risk and Insurance Management Society stated that a key driver for the activity leading to the financial crisis was a "system-wide failure to embrace appropriate enterprise risk management behaviours"[3]. This view was supported by the Walker report into the corporate governance of UK banks in 2009 which stated that board Risk Committees are responsible for ensuring that a supportive risk culture is appropriately embedded so that all employees are alert to the wider impact on the whole

[1] The UK Corporate Governance Code, Financial Reporting Council, 2012, p18

[2] IIA Position Paper: The role of Internal Audit in Enterprise-Wide Risk Management. 2009

[3] RIMS, A Wake-up Call for Enterprise Risk Management. 2009, p4

organisation of their actions and decisions.[4] Following this, rating agencies such as Standard & Poor's have been looking at the rating of risk culture as part of a broader ERM assessment of financial and non-financial companies. This has the potential to impact access to capital and influences the cost of debt – and therefore has a real impact on the bottom line. More recently the Operational Risk Consortium (ORIC) conducted a new study on creating value from risk events,[5] which calls for firms to question their risk cultures and learn lessons from risk events in order to survive and prosper in the current times.

Yet despite the increased focus on risk culture, there is still a lack of understanding of what risk culture is and what it looks like. As a result, in 2012 the UK Institute of Risk Management released two guidance papers – one for boards and one for practitioners – on risk culture. Risk culture is defined by the IRM as "the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common purpose"[6]. This culture arises from the repeated behaviours of the group members, that is the external, observable risk related actions e.g. risk based decision making, risk communications etc. All organisations have a risk culture, the important question is whether or not the culture is supporting or undermining the success of the organisation in taking risks to achieve its objectives including the upholding of its reputation/ brand and financial stability.

Aside from the obvious benefit of supporting the organisation meet its objectives, a risk culture audit also brings benefits in terms of identifying and reinforcing desirable cultural traits and practices, and can therefore make a significant contribution to corporate performance and integrity. Looking at this from an alternative perspective, this means that the opportunity exists to eliminate actions and practices that may directly contribute to risks and issues arising in the future as seen through recent events such as those at HBOS and Barclays where the culture was described as "toxic".[7] A report into the UK mid-Staffordshire NHS Trust found that around 1,200 unnecessary patient deaths were caused to some degree by a prioritisation of financial performance over patient welfare imposed by senior management, and by a blame culture where employees at all levels were frightened to speak out.[8]

Ultimately it is the responsibility of the board to set, communicate and enforce a risk culture that consistently influences, directs and aligns with the strategy and objectives of the business, and therefore supports the embedding of the risk management framework. As part of this, key questions the board needs to ask itself include[9]:

- What is the current risk culture in our organisation and how do we improve risk management within that culture?
- How do we want to change that culture?

[4] A Review of Corporate Governance in UK Banks and other Financial Industry Entities, 2009, p92

[5] ORIC, Creating Value from Risk Events: leading practices in operational risk event reporting, analysis and investigation, learning and management'. 2013.

[6] IRM, Risk Culture Resources for Practitioners, 2012, P22

[7] Campbell, Operational Risk & Regulation, 15/5/13

[8] Report of the Mid Staffordshire NHS Foundation Trust Public Enquiry, February 2013

[9] IRM, Risk Culture Under the Microscope, Guidance for Boards. 2012, p9

- How do we move from where we are to where we want to be?

Internal audit has a key role in helping the board answer these questions by providing a picture of what the existing risk culture looks like in the organisation through the audit process, and facilitating at the senior management level the discussion on the desired future state. This does require a change in approach to consider and identify controls that focus on the 'soft' behavioural issues associated with culture, and may require a more considered approach to both the planning of the audit to ensure that the right elements are audited, and to the assessment and reporting aspects as behaviour cannot easily be rated using a traditional satisfactory/ unsatisfactory methodology. However, before looking at the audit approach in more detail, it is first useful to understand how a good risk culture can be defined.

What does a successful risk culture look like?

An effective risk culture enables and rewards individuals and groups for taking the right risks in an informed manner – and hence facilitates the achievement of organisational objectives. Indicators that the risk culture is successful (i.e. effective) include[10]:

1. A distinct and consistent tone from the top from the board and senior management in respect of risk taking and avoidance.
2. A commitment to ethical principles, reflected in a concern with the ethical profile of individuals and the application of ethics and the consideration of wider stakeholder positions in decision making.
3. A common acceptance through the organisation of the importance of the continuous management of risk, including clear accountability for and ownership of specific risks and risk areas.
4. Transparent and timely risk information flowing up and down the organisation with bad news rapidly communicated without fear of blame.
5. Encouragement of risk event reporting and whistle blowing, actively seeking to learn from mistakes and near misses.
6. No process or activity too large, complex or obscure for the risks to be readily understood.
7. Appropriate risk taking behaviours rewarded and encouraged and inappropriate behaviours challenged and sanctioned.
8. Risk management skills and knowledge valued, encouraged and developed, with a properly resourced risk management function and widespread membership of and support for professional bodies. Professional qualifications supported as well as technical training.
9. Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged.
10. Alignment of culture management with employee engagement and people strategy to ensure that people are supportive socially but also strongly focused on the task in hand.

[10] IRM, Risk Culture Under the Microscope, Guidance for Boards. 2012, p5

Using these indicators and beginning with the end in mind, the audit approach can then begin to be scoped and relevant controls identified.

Auditing risk culture

Before beginning any audit into risk culture, it is important to assess whether the organisation is ready to undertake such an initiative. Discussions should be held with the board and management about the objectives, benefits, implications and steps needed to implement risk culture auditing. Ideally a pilot area will be identified – possibly where management is particularly concerned about the potential findings - to test the defined methodology and to provide the opportunity to refine and improve if needed before rolling out further across the business.

In addition to gaining the buy in of the board and management, there is a need to involve key stakeholders in the process of planning, defining and potentially even conducting the audits. Some of the main evidence that may be required to support findings from the audit are likely to include existing indicators with an HR focus e.g. employee surveys and performance management and reward approaches and measures. As HR generally tend to be the owners of this type of information, it is vital that a collaborative agreement can be reached so that their specialist skills and knowledge can be used to help interpret the evidence and add value and insight to the audit. Similarly, other parts of the organisation such as Risk and Compliance are likely to hold data that can contribute to a comprehensive understanding of the behaviours underlying and impacting the implementation of the risk process.

As well as identifying and involving key stakeholders, a significant challenge in the audit of risk culture is defining the approach to be used – a mixture of art and science. The following steps are one way of developing the risk culture audit:

1. Select a risk culture model to audit against. The IRM Risk Culture Resources for Practitioners document is a good reference in terms of various methodologies and approaches that can be taken. The IRM's own risk culture model is however a sound starting point as it identifies eight key aspects of risk culture grouped into four themes – key indicators of the health of the risk culture aligned to the business model.

Table 1. Themes and aspects in the IRM Risk Culture Model

Themes	Aspect
Tone at the Top	Risk Leadership: clarity of direction • Senior management set clear and consistent expectations for managing risk • Leaders role model risk management thinking and actively discuss tolerance to risk issues
	Responding to bad news: welcoming disclosure • Senior management actively seek out information about risk events • Those that are open and honest about risks are recognised
Governance	Risk governance: taking accountability • Management are clear about their accountability for managing business risks

	• Role descriptions and targets include risk accountabilities
	Risk Transparency: risk information flowing • Timely communication of risk information across the organisation • Risk events are seen as an opportunity to learn
Competency	Risk resources: empowered risk function • The risk function has a defined remit and has the support of leaders • It is able to challenge how risks are managed
	Risk Competence: embedded risk skills • A structure of risk champions support those managing risks • Training programmes are in place for all staff
Decision making	Risk Decisions: informed risk decisions • Leaders seek out risk information in supporting decisions • The business's willingness to take on risks is understood and communicated
	Rewarding appropriate risk taking • Performance management linked to risk taking • Leaders are supportive of those actively seeking to understand and mange risks

2. Once a model has been selected to audit against, questions need to be determined to explore the organisation's behaviours around these areas. As the audit is focusing on culture rather than process, it is necessary to look for evidence to support any statements given which may not necessarily be documented as controls. Instead, evidence should concentrate on factors such as:

- meeting minutes which demonstrate the substance of risk discussions held, questions raised and 'pull' for risk data to inform decision making;
- evidence of risk events and incidents being used to facilitate learnings;
- reports showing the number of incidents/near misses reported;
- frequency with which risks are raised;
- reports showing the usage of risk systems;
- examples of leadership demonstrating the risk management values;
- performance objectives containing references to risk responsibilities;
- frequency and reach of risk communications and education;
- understanding of, agreement with and conduct of risk responsibilities;
- examples of action taken against those where risk behaviour was considered inappropriate or exemplary;
- the role of risk champions or specialists to support the business;
- the extent to which risk management is embedded within other business processes;
- the extent to which the various risk functions collaborate;
- employee surveys (e.g. satisfaction, understanding of key policies etc);
- budgets allocated for risk management activity;
- examples of improvements made to risk and control frameworks; and
- terminology used to discuss risk.

Whilst there may be documented controls around the required risk behaviours and values in the organisation, the majority of the evidence will come from documented actions as opposed to documented processes. If there is initially a lack of documentary evidence to support the question responses, a wider respondent group may be needed to verify statements made, and a list compiled of evidence that would be expected in future risk culture audits.

It is also important to be aware of any national biases that may be impacting the risk culture and effecting results of the audit if working across different geographic regions, as the perception of risk varies across cultures. This can vary from a high level of avoidance to fatalism to acceptance, and this bias can impact on how risk guidance is perceived and understood e.g. ‘avoiding surprises’ can be taken to mean that risks should be escalated, but could also be understood as unpleasant surprises should be hidden. An awareness of the primary approach to risk management by the local nationality is therefore of use when interpreting the audit results and tailoring recommendations.

3. As the risk culture model presupposes a continuous improvement approach where risk culture improves incrementally and performance is tracked over time, traditional scoring methods such as satisfactory/ unsatisfactory are not appropriate. Consideration should therefore be given to a maturity based scoring and reporting approach.

   There are a number of risk maturity approaches available in the public domain that can be used and modified in the first instance, or the organisation may decide to invest the time and skills in defining its own risk culture maturity approach. This should be done in conjunction with the Risk function that will be able to provide useful input into this process. In general, such approaches use a three, four or five point scale ranging through stages such as ‘Foundation’ through to ‘Optimised’ or using colour coding, with each stage being defined by a number of specific attributes. Again the IRM Culture guidance offers a practical diagnostic based on the eight factor maturity model discussed earlier. This uses a four point scale with colour coding to help identify the organisation’s current position as regards risk culture maturity.

Table 2. IRM Risk Culture Aspects Model

Issue	**9 to 10**	**6 to 8**	**3 to 5**	**1 to 2**
Tone at the Top - Risk Leadership	In addition to 'green', executive sponsor is very visible and leaders demonstrate their commitment on a sustained basis, show personal conviction in how they communicate and ask questions regarding business risks.	Leadership expectations are clearly expressed and consistently communicated. Direction is set and leaders create a 'Tone at the top' through reinforcement and challenge.	Leadership expectations on risk management are defined but inconsistently communicated and understood. Staff are not clear on overall direction.	It is not possible to describe a 'Tone at the top' or leadership expectations on how risks are managed.

Tone at the top - Dealing with Bad News	In addition to 'green', leaders see their ability to extract learning from good and poor risk management judgements as a key corporate competitive advantage. This is seen as part of the organisation's knowledge management process.	Leaders encourage the timely communication of material risk information. They challenge managers to divulge 'bad news' early to ensure it is acted upon in a timely manner.	The communication of 'bad news' is sporadic. Attempts are made to encourage early communication of risk information. It is recognised that this is important but processes are still to be formalised and embedded.	The organisation does not encourage the communication of information about potential negative events. Managers have concerns about communicating 'bad news' to leaders. Stories exist of the manager having been 'shot'.
Governance - Accountability & Governance	In addition to 'green', leaders act proactively on their accountabilities, seeking out and challenging risk strategies associated with key business risks under their nominal control.	Accountabilities for managing risks are clearly defined and widely understood. Accountability for risk management as a process is held by the risk function. Accountabilities are clearly mapped to manager's role descriptions and targets.	Accountabilities for managing risks are partly defined. Some key regulatory and compliance aspects are well defined. The risk management and reporting process is in place but not clearly defined or widely understood.	Accountabilities for managing risks are not consistently defined. It is not possible to be sure who is accountable for managing which risk. Risk management is ill-defined and ownership for the process is unclear.
Governance - Risk Transparency	In addition to 'green', leaders actively seek to learn from risk events. When appropriate risk decisions are taken, these are celebrated. More importantly, when risks crystallise, the organisation seeks to learn from these events. The key learning points are widely communicated.	Risk information is communicated up and down the organisation. The information provided is meaningful to leaders and appropriate to their needs. Risk information is actively used in decision making and levels of appropriate risk are clearly defined.	Risk information is effectively communicated on certain specific issues related to regulatory or compliance aspects. Communication of risk information tends to be one-way (bottom-up) with little feedback or leadership direction. It supports a 'tick box' approach.	Risk information is not transparent and is not readily communicated. Managers do not receive risk information on which to base their judgements. It is not possible to define the level of acceptable risk within the organisation.
Competency - Risk Resources	In addition to 'green', leaders recognise the risk function as a valuable facilitator of strategic thinking on business risk. Risk managers are sought out to support the business in evaluating key decisions.	The risk function has a clear role and remit endorsed by senior management. The function has the support and credibility to deliver these. The function has the skills and resources required to support an effective risk management culture.	The risk function's role is defined but it does not cover all aspects required for an effective governance process to be implemented. The risk function does not have the breadth and depth of skills to support all aspects required to develop an effective risk management culture.	The risk function does not have a clear role or remit. Governance activities are fluid and shared between a range of functions and role holders. Risk professionals are not seen as being strategic advisors. The risk function may be ill-equipped to support Governance arrangements.
Competency - Risk Skills	In addition to 'green', competency in risk awareness and risk management is seen as an entry-level requirement for senior management and this is widely recognised across the business.	Risk awareness is recognised as a key competency for managers across the organisation. Skill development is proactively encouraged and programmes are in place to develop and sustain competency.	Training and awareness programmes around risk management exist in parts of the organisation. These are implemented in a partial or soloed manner. The process is not fully developed or sustainable as part of a wider ERM framework.	Competency in risk management is not recognised as a key skill. Training and communication programmes are not conducted and address specific issues within the context of specialisms and 'silos' of risk.

Decision making - Informed Risk Decisions	In addition to 'green', leaders refuse to take major decisions without an explicit risk/ reward study. Risk-adjusted accounting practices are embedded in business planning.	Leaders actively seek risk information to inform their judgement on key business decisions. The willingness to take risk is understood and clearly communicated. The scale of risk and reward is balanced in decision making. The process for achieving this is visible and recorded.	Leaders seek risk information on an ad hoc basis to support decisions. The boundaries of acceptable risk are only defined with respect to specific issues. It is not clear how risk and reward are balanced although these are considered in decision making.	Business decisions are typically taken in isolation from explicit risk factors. The evaluation of risk and reward is done in an ad-hoc and intuitive manner.
Decision making - Rewarding Appropriate Risk Taking	In addition to 'green', leaders recognise that risk management competency is a key skill and this is used as a criteria in succession planning and leadership selection.	Leaders are supportive of those seeking to engage with the management of risks. Those that demonstrate a capability for evaluating risks and taking informed judgements are effectively rewarded. The Performance Management process is used to reward appropriate risk taking and to challenge inappropriate risk behaviours.	It is recognised that risk awareness and taking behaviours are valuable to the business. Steps have been taken to encourage these but these are not explicitly connected to Performance Management processes. Inappropriate behaviours typically go unchallenged.	Risk awareness and taking behaviours are not recognised as valued and are not explicitly rewarded.

The risk culture audit is best done in conjunction with the standard assessment of the effectiveness of the risk framework as it is difficult to divorce design and operational effectiveness from the implementation behaviour, but when put together, a comprehensive picture of the effectiveness of the overall risk framework should emerge.

Managing the outcomes

Having successfully navigated the intricacies of the audit, the next step to consider is what to do with the outcomes. This provides a key opportunity for Internal Audit and Risk to facilitate a discussion at senior management level concerning the gap between the current state, and the desired future state position for risk culture maturity. With the help of the diagnostic used for the audit, agreement needs to be gathered on the various levels of maturity required for the different aspects of the model. This must be done taking into consideration the overall purpose of the risk culture for the organisation, and what the overall risk strategy is. Once agreed, tangible actions can be defined to address the gap, and a clear benchmark set in terms of follow-up audits.

Summary

Internal Audit has a key role to play in evaluating the effectiveness of the risk framework not only from a process perspective in terms of compliance and alignment with leading standards, but also from a cultural perspective in terms of the underlying implementation behaviours. Developing and conducting a risk culture audit poses a challenge as it looks at areas outside the traditional scope of internal audit activity. As such, it may require the temporary use of additional specialist skills from across the business, and involve some clear articulation of why the audit should be conducted and the expected benefits to be achieved in order to achieve buy-in from stakeholders. However, if conducted successfully, the benefits of having a complete picture of the risk framework include:

- the opportunity to make risk management more relevant and effective for the organisation;
- demonstrating to stakeholders both internally and externally the value placed on risk management by the organisation; and
- reinforcing desirable cultural traits and practices that support the success of the organisation in taking risks to achieve its objectives.

For further detailed information on risk culture, see the two IRM guidance documents at http://www.theirm.org/publications/PUpublications.html