KPMG

Risk consulting

A regulatory perspective

kpmg.ie

Risk Culture: A regulatory perspective

Risk culture - why is it important?

Increasingly financial regulators have an expectation that financial institutions have a sound organizational culture. Reports on control failures in recent years, from individual issues such as the LIBOR scandal to broader industry reviews such as the Irish statutory reviews of the banking crisis, cite an inappropriate organizational culture or the absence of a risk culture as contributory factors.

In Ireland, the emphasis on organisation and risk culture as a means of mitigating risk is reflected in a focus by the Central Bank on culture as part of its normal supervisory activity. Indeed, the Central Bank has recently conducted themed inspections examining "behaviour and culture" at local banks, along with actively inspecting banks' compliance with the internal governance guidelines set out by the European Banking Authority in its GL44 paper.

The problem facing financial institutions across the various sectors is that "culture" is a nebulous concept, not to mention a subjective one, far removed from concrete regulatory issues such as solvency, credit risk modeling and risk weightings.

"Culture"[1] within an organization relates to its people, its performance, individual beliefs within the organization and its leadership. It encompasses **risk culture** which addresses the articulation, communication, measurement and management of risk. But it also separately takes into account **conduct risk**[2] which seeks to identify and address risk in product design, sales practices and behaviour which may have an impact on customers.

The financial crisis of recent years highlighted poor risk management practices and clear weaknesses in internal control structures, but it also highlighted deficiencies in many financial institutions' attitudes towards risk. An assessment of risk culture is thus a core component of the cultural awareness agenda. Any culture is a mixture of formal and informal practices so the question arises, how can risk culture be articulated and how can regulators assess it? Conversely, how can a financial institution embed a risk culture and how can it assure itself that its risk culture is adequate, for example are there metrics that can be used?

This article seeks to answer the questions. It examines the initiatives of regulatory agencies to create an awareness of risk culture and their approach to reviewing it. It looks at how financial institutions can embed a desired risk culture and the tools available to them, and looks at the unique role that the internal audit function, in particular, can play in facilitating the building of such a culture and assessing it.

[1] KPMG Ireland's Organisations' cultural assessment and transformation paper 2017
[2] KPMG Ireland's Conduct Risk paper 2017

How do regulators assess risk culture?

In this section, we will look in some detail at how the Financial Stability Board, the European Central Bank and the Central Bank assess risk culture and what the regulators' expectations are.

Financial Stability Board (FSB)

The FSB defines risk culture as **"an institution's norms, attitudes and behaviours related to risk awareness, risk taking and risk management, or the institution's risk culture."** The FSB sets out that risk culture shapes the values and beliefs which govern how individuals within an institution behave, how they perform their roles, how they take decisions, how they assess risk and do the ethical thing to ensure they operate in a safe and sound manner, and as such is bespoke to each organization.

From a supervisory perspective, the FSB's *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture - A Framework for Assessing Risk Culture* published in April 2014 is the seminal, reference document. The FSB states that a sound risk culture will support appropriate risk awareness, behaviour and judgments about risk taking. The FSB does not define a target risk culture but rather gives regulators guidance on how to identify the risk culture within an institution.

The FSB indicates that a sound risk culture is one that:

- has an appropriate risk/reward balance consistent with risk appetite when taking decisions
- has an effective control environment
- allows the quality of the risk models, data accuracy etc to be challenged
- ensures all risk breaches are followed up with proportionate disciplinary actions

European Central Bank (ECB)

The idea of an appropriate risk culture in banks is also a theme with the ECB and its approach is hugely informed by the FSB's framework paper. Risk culture also features prominently in its document *'SSM supervisory statement on governance and risk appetite'* published in June 2016, which states that expectations are that a strong risk appetite framework will help build a sound risk culture.

The ECB focuses on four main areas:

- Board and senior management: acting with integrity should be promoted from the very top level of management, core values should be defined and the organisation should develop an openness to challenge as well as a consistent tone throughout the bank
- Staff accountability: the bank must ensure staff are capable and it must be clear who is individually accountable for actions with respect to the bank's risk profile. There must be clear delineation of roles and responsibilities for the control functions versus the business lines;
- Communication: is the bank encouraging open communication and adequate challenge? This should be evidenced in board minutes. Is there evidence of adequate horizontal and vertical sharing of information? Do appropriate whistleblowing procedures exist without unfair reprisals on employees?
- Remuneration and incentives: do annual performance reviews, remuneration and career paths reflect an appreciation and active promotion of the bank's core values and risk culture?

Central Bank of Ireland (CBI)

Recently the Central Bank has been focusing on cultural awareness as part of its normal supervisory activity, including a consideration of an institution's risk culture through continuous assessment meetings, risk management and governance reviews and inspections. Again the Central Bank does not prescribe a target risk culture but rather seeks to influence it.

In June 2016, Ed Sibley, who is now the Central Bank's Director of Credit Institutions, referred to the cutting edge techniques of the Dutch regulator in assessing culture and indicated that the Central Bank , in its behaviour and culture inspections' of banks, would be seeking answers in relation to;

- What influence, positive or negative, do individual actions and group dynamics have on the financial performance, integrity and reputation of an institution?
- Which facilitating or restraining role does the institution's prevailing culture play?
- Which measures are necessary to mitigate the risks related to human behaviour as much as possible?

It is noteworthy that the Central Bank has also completed themed reviews of the risk function, including risk frameworks and risk culture of investment firms, fund service providers and stockbrokers, indicating that its interest in risk culture is not confined to the banking sector. The main finding from that review is that there is a divergence in the quality and effectiveness of risk frameworks.

In essence the risk culture allows regulators to assess the soft side of the risk management framework while the risk appetite framework provides the metrics and more quantitative evidence of the firm's approach to risk taking. Regulators are trying to ensure that risk culture is a driver of the strategy and not the other way round

How can financial institutions embed a risk culture in their organisations?

Most financial institutions are grappling with how best to articulate what type of risk culture they aspire to. As already mentioned there is no such thing as an optimal target risk culture that applies to every financial institution. Rather each financial institution has its own prevailing risk culture and its own target or aspirational state.

It is challenging for a firm to assess what is the prevailing risk culture and whether it is consistent with the organisation's risk appetite and what changes need to be made to ensure that risk appetite and culture are aligned. In addition any changes made should be to the very core of business operations and culture, otherwise there is a risk that changes are superficial and do not lead to sustainable and genuinely different behaviour.

Articulation of Risk – Risk Appetite Frameworks

Regulators have recognised the need to establish a structure a financial institution can use to define its own, individual, acceptable bounds for risk-taking. This has resulted in a greater focus on the need to establish clearly articulated risk appetite frameworks.

The FSB's Principles for an *Effective Risk Appetite Framework* set out four key elements:

- an effective risk appetite framework;
- an effective risk appetite statement;
- risk limits;
- defining the roles and responsibilities of the board and senior management in establishing the approved risk appetite statement.

The risk appetite statement, in particular, can be used as a tool to support conversations about risk within business units and is an important component of risk culture.

Assessing the existing state of risk culture

Once a financial institution has defined its desired risk culture, it should seek to understand and assess the existing risk culture. This can be done using a variety of measures including:

- Staff surveys;
- Management information leveraging existing data from various sources such as breaches of risk limits, trends in risk reporting, loss events, whistleblower reports, compliance breaches, exit interviews, complaints and internal audit findings;
- External reviews
- Insights from informal interactions with stakeholders

Risk Communications

Leadership is central to shaping both organisational and risk culture. The board of directors obviously contribute an important element of "tone from the top" in their oversight and governance role. Senior and middle management are seen as having an immediate and tangible impact on behaviours both through communication (what they say) and role modelling (what they do).

Any messages on risk emanating from directors should be consistent with those from senior management. It is important that these messages demonstrate a clear alignment between organisational purpose, stated values and actual behaviours.

Furthermore there needs to be a "speak-up" policy in place within the firm which encourages communication about, for example, breaches of risk limits,

Risk Training

Employees should be trained on expected risk management behaviour. They should also "sing from the same hymn sheet" and in this regard, developing and disseminating a glossary of commonly-used terms will assist in the use of a common risk language. This should ensure a more consistent implementation, application, monitoring and measurement of risk.

Risk measurement

It is widely recognized that culture is a vague concept and methods to measure it within a financial institutions are still at an early stage of development. That said, there are some clear principles that can be applied to risk measurement:

- The risk appetite statement should be used to develop risk indicators relevant to the organisation and as a yardstick to benchmark actual behaviour;
- Any indicators used to measure the risk culture should be aligned to desired outcomes and should be material to the business;
- Performance management and reward systems should discourage excessive risk-taking; and
- The Risk Committee and Audit Committee should comment on its assessment of risk culture to the board, notwithstanding the fact that balanced scorecards to measure risk culture are still at an early stage of development.

How do the control functions play a role in the development of a risk culture?

A strong culture is evident in a firm which can demonstrate the effectiveness of its compliance, risk and internal audit functions. The compliance and risk functions champion a robust risk culture while internal audit plays a role in its assessment.

Compliance has a critical role in driving culture, especially by leading by example and "doing the right thing" on a day to day basis. Compliance should carry real weight within the firm, breathe life into compliance culture day to day and mitigate against the risk of non-compliance.

The risk function is clearly tasked with the operational aspects of risk management, but in so doing it plays a pivotal role in the development of the firm's risk culture. The risk function, along with the Risk Committee, are key to driving the risk culture agenda and awareness through their actions and behaviour.

Internal audit has a crucial role in assessing and highlighting the importance of risk culture within a firm. The unique perspective that it has on the organisation places it in an ideal position to support an on-going assessment of the prevailing risk culture.

From an internal audit perspective, there is an opportunity to provide the board of directors with a view as to whether measures to improve risk culture are proving to be effective, across all levels within the organisation. This can be done in two ways.

Firstly, by considering risk culture as part of every audit engagement and perhaps using this to provide thematic reporting on culture to the Audit Committee. Some internal audit functions have introduced a dual rating for audit reports. This first rating is applied to the control environment but the second relates to management awareness or attitude towards risk.

Or secondly through individual audit assignments, which take into account considerations such as:

- the initial engagement with internal audit: at the opening audit meeting does management demonstrate an awareness of the risk in its environment; do they actively seek to improve the control environment; are they open in relation to concerns or known blind spots; do they demonstrate awareness of corporate values?
- interactions throughout the assignment: - are these open, engaged, not defensive, co-operative?
- response to findings: typically organisations allow management to include comments in written reports in response to audit findings, the tone and content of these responses can be telling.
- dealing with open audit findings: a key risk culture metric can be how management deal with open audit findings i.e. are they closed within specified time frames; are they prioritized; are there instances of recurrence of the same issue; are there consistent requests for extensions to timeframes for closure of findings?
- a key indicator for internal audit can also be the output of detailed Root Cause Analysis of audit findings. For example, using the "5 whys" technique to understand if behaviour led to a control failure can be a prime indicator of deficient risk culture - did the control fail due to a choice to contravene policy or procedures or a lack of awareness or lack of training?

Individual audit assignments specifically focused on risk culture may be informed by (i) whistleblowing events (ii) HR grievances (iii) exit interviews (iv) breaches of firm policies (v) reviews of incentives schemes (vi) assessment of programmes to raise risk awareness and obviously assessments of how embedded the risk appetite is. However, this can be largely theoretical and the challenges for internal audit can include:

- the difficultly of reporting findings, which are subjective in nature;
- internal audit staff having the appropriate skillset on matters of culture and behaviours; and
- the development of appropriate management information and key performance indicators.

Finally, in respect of management information and key performance indicators, internal audit is in a unique position to gather data that can inform a firmwide database of metrics to assess data. It is essential that any internal audit assessment is underpinned by appropriate metrics and that a database of these is built up over time to afford a reasonable assessment. Additionally, it is difficult to accurately assess risk culture at a point in time. It needs to be considered over a time horizon and a trajectory i.e. is internal audit seeing an improvement in risk culture based on reliable quantitative metrics?

Creating and embedding risk culture – the foundations

An organisation with a strong risk culture is one where the board, management and employees all clearly understand what risks are acceptable and what risks should be minimised or avoided.

The risk culture informs core values, mission statements and a corporate vision that is clearly articulated and disseminated throughout the organisation. The behaviour and attitudes required must be understood at all levels within the organisation.

There needs to be a formal programme to embed awareness of the values (through training and communication) to ensure that it filters throughout the organisation. There should be no confusion as to where the limits and tolerances lie.

Communication is encouraged regarding risk accumulation and risk measurement. The desired culture is enforced through behaviour from management and directors as well as the use of incentives and sanctions.

Strengthening roles and responsibilities throughout the organisation in respect of risk management and enhancing the communication and training around risk has a significant impact on embedding a strong risk culture. All individuals must be accountable for their actions and initiatives should be put in place which consistently reinforce the desired behaviour.

There is a recognition now that culture is integral to everything and that governance is no longer simply appointing non-executive directors to the board and producing good board packs. Regulators are developing a more intrusive and encompassing definition of governance and risk culture is part of the widening of this definition.

Ultimately, boards will also need to embrace this concept and ensure that the correct tone from the top is set. Risk and compliance functions, along with senior and middle management, will need to drive this agenda to ensure that it meets supervisory expectations and that the risk culture is deemed adequate and supportive with internal audit playing a role in continuous assessment.

Contacts

Gillian Kelly
Partner,
Risk Consulting

T. +353 1 410 1120
E. gillian.kelly@kpmg.ie

Patrick Farrell
Partner,
Risk Consulting

T. +353 1 700 4029
E. patrick.farrell@kpmg.ie

Ciaran Rogers
Director,
Regulatory

T. +353 1 700 4238
E. ciaran.rogers@kpmg.ie

Claire Heeley
Director,
Risk Consulting

T. +353 1 700 4080
E. claire.heeley@kpmg.ie

kpmg.ie/regulatory

Produced by: KPMG's Creative Services. Publication Date: July 2017. (2770)