CRO Forum – A Guide to Defining, Embedding and Managing Risk Culture

September 2017

CRO FORUM

A Guide to Defining, Embedding and Managing Risk Culture

September 2017

Executive Summary

The purpose of this paper is to provide a practical guide to Risk professionals in defining, establishing, embedding and managing risk culture. In seeking to achieve this, it examines the behaviours that characterise a sound risk culture in the context of the insurance industry, and recognises the importance of a well-managed risk culture in achieving organizational objectives.

This paper examines:

- the ownership role of the Board in setting the risk culture;
- the supporting role of the Chief Risk Officer (CRO) and Risk Function in assessing and measuring; and
- the role of Executive Management, and the other lines of defence, in operating and embedding the desired risk culture.

Assessing the appropriateness of risk culture is high on the regulatory agenda. Whether it is performing risk management and governance reviews or reviews of capital, investment, and operational risks etc., regulators will be looking at behaviours, how decisions are made, how they are communicated, how this is reflective of a firm's risk management framework, and how actions are implemented on the ground.

In most instances, financial service organizations which have been subject to extensive regulation have developed a risk culture that is driven by both their own ambitions as well as those that meet regulatory expectations, e.g., fit and proper testing, remuneration, etc. These regulatory requirements are important for standard setting across the industry and to ensure a level playing field but they are no substitute for a local program.

Firms that develop their own informed opinion of their current risk culture, an assessment of their desired risk culture, and the means by which to achieve a desired state will be better positioned to have rounded conversations with their regulators and enduring cultures. However, without a steer and demonstrable support from the top, an organization is unlikely to arrive at a well-understood, credible, or sound one, let alone one adopted and owned by the middle and front line employees. Indeed, the perpetuation of an unformed risk culture is potentially an obstacle to innovation where the balance of risk taking mind-sets and speed of execution rely on the entire organization having a common understanding of how to apply firm wide risk disciplines to transformative change, particularly in a digital age.

This paper concludes that there is no one "right" risk culture that applies to all organizations and that a firm may have distinct risk cultures across its different businesses and geographies. Further, changing and embedding risk culture is a continuous process that will require constant management attention.

The paper draws from the experience of the CRO Forum member CROs who provided examples of practices, challenges, indicators of positive and negative behaviour, and methods to drive a positive risk culture. As an assessment of the firm's risk culture has more qualitative aspects, guidance is also included to support the CRO's efforts in framing an approach for that assessment.

Contents

1. The Importance of Risk Culture in Achieving Organizational Objectives

1.1 Risk culture defined

The term 'risk culture' is the nomenclature used to capture the way an organization – regardless of location in the world, industry, or legal structure i.e. public, private, not-for-profit – demonstrates through its actions and accepted behaviours its shared beliefs, values, and understanding of how it regards and manages risk in the course of achieving its business objectives. Risk culture is a sub-set or complement to organizational culture.

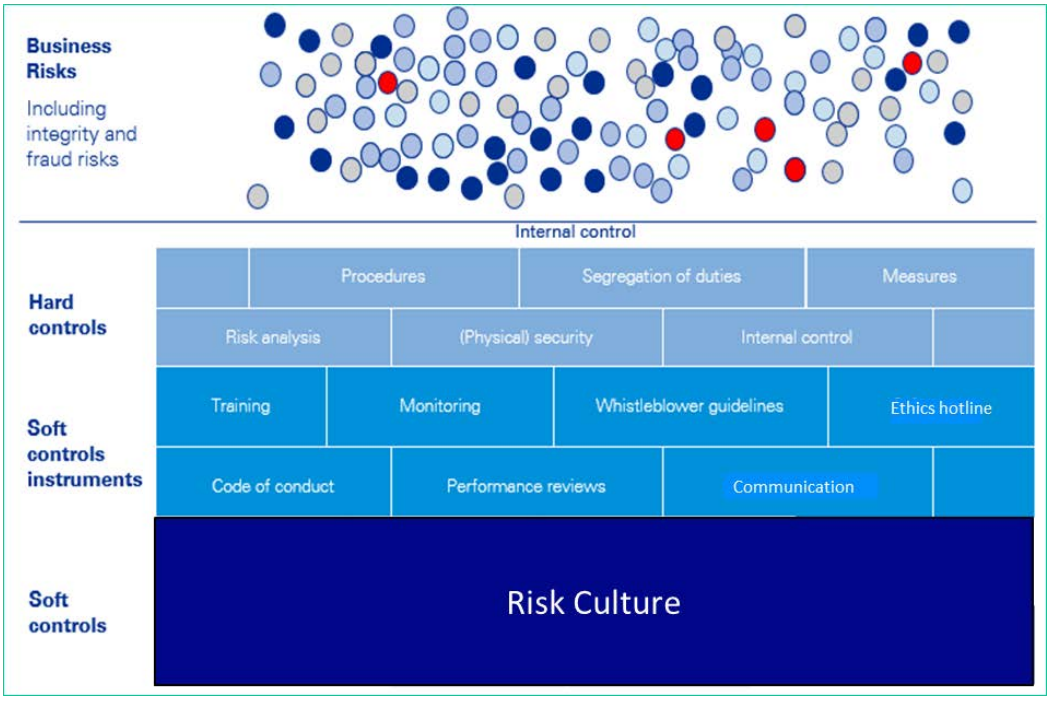
Organizations routinely define their purpose (why they exist); vision (what is the end goal); mission (what needs to be done to achieve the end goal); and strategy (the plan to achieve the goal). These are generally tangible objectives and outcomes. Often, an organization's articulated business culture can be found in its Code of Conduct. Having a written "culture", is not evidence that the targeted culture is embedded or actually experienced by employees and other stakeholders.

An organization's experienced culture can be described from the consistent, observable patterns of a firm's behaviour. This raises the question of whether structures, processes, and incentives drive the formation of culture, or whether culture is the expression of the behavioural output responding to structures, processes, and incentives. Regardless of 'which comes first?', culture evolves over time as it is affected by a wide range of internal and external factors and responses to those factors. The factors usually associated with a good business culture such as integrity, transparency, openness to communicating risks and opportunities, respect, accountability, customer and employee focus, and learning from mistakes, are also markers of a sound risk culture.

1.2 Established approach to shaping risk culture

The established approach for developing the internal control environment (see Figure 1) is through "hard control practices" and "soft control instruments" that are designed to complement the hard controls. Together they form a basis for providing evidence of a risk culture. Unfortunately, without demonstrable executive support, the evidence results from a tick-box exercise and may have limited relationship to the realities of daily behaviours in the firm.

Figure 1:



Source: M. Kaptein, Professor Business Ethics at Erasmus University, Feb 10th, 2017

Sometimes, it takes a crisis or need to respond to an external stimulus to act as the catalyst for implementing cultural change. Often a crisis will open a business to be receptive to making changes even where behaviours are already well ingrained.

A poor risk culture can persist for some time without detection, or immediate damage. Typically, it will be when a poor risk culture is combined with adverse market conditions and/or other stresses that there is greater potential for a build-up of unbalanced and ill-considered decisions to result in significantly adverse, and potentially crippling, financial outcomes' (Australian Prudential Regulatory Authority - APRA, 2016).

Then again, sometimes, a forward thinking firm can decide to define and drive clear organizational and risk culture standards because it makes good business sense.

Case Study: CRO Forum Member - Being Proactive, a Shared Effort

Through its existing practices of reviewing risks and regulatory developments in its various geographical locations, a CROF member notices that regulators in different parts of the world were asking questions about risk culture – how it was defined, measured and expressed within the local entity. Specifically, the regulators were interested in knowing not only whether a risk culture was articulated but whether it made a difference to decisions, strategy, employee behaviour, and customer engagement. In the firm's headquarters, the CRO and Executive management decided to assess proactively the current risk culture and determine a desired "to be" state. The firm began by benchmarking the journeys of other financial services firms and looked outside the sector as well. The Board, the CRO and Executive Management are actively engaged in reviewing and shaping the expression of risk culture from the centre and exploring how it is to be embedded worldwide.

1.3 Why do good people do bad things

The "fundamental attribution error" is a common cognitive bias in social psychology. It means that people have a tendency to explain someone's behaviour assuming it is an expression of the individual's internal personality or disposition and underestimate the influence of external factors, such as situational influences and pressures.

In any organization there will be numerous cognitive biases at play. Not acknowledging and addressing these biases will enable "Group Think" which can result in unchallenged, poor quality decision making due to unquestioning conformity. Tools to avoid the biases include pre-emptive setting of measures for success and failure (e.g. 'go-no-go' decision parameters), cognitive bias training, a conscious effort to measure feedback at defined stages against the measures of success, and, oversight from independent Non-Executive Directors to challenge the outcome.

In a whitepaper published by Mindgym, "The Only Way Is Ethics – why good people do bad things and how to stop us"[1], six broad reasons are outlined on why people who otherwise think themselves as "good" do "bad" things:

1. everyone else is doing it — actions are already seemingly justified;
2. it's not fair — feeling excluded;
3. tired and emotional — physical and mental exhaustion weaken integrity;
4. slippery slope — small transgressions lead to a person engaging in more serious transgressions;

[1] https://uk.themindgym.com/resources/the-only-way-is-ethics-2/

5. loyalty wins — an overdone strength that can turn to collusion—loyalty can smother fairness;
6. severe consequences — the goal matters above all else (Volkswagen, Wells Fargo, Enron, Tesco).

A recent case showing the effect of the threat of severe consequences is described below:

Case Study: Wells Fargo – Do what it takes or risk the consequences

Driven by its sales culture, the Community Bank's sales practices led to major financial and reputational damage. The bank's performance management system created pressure on employees to sell unwanted or unneeded products to customers and to open unauthorized accounts. Corporate control functions were constrained by the decentralized organizational structure and a culture of deference to business units. Substantial fines and penalties have been paid as a result of regulatory investigations. In response, the bank has eliminated sales goals and reformed incentive compensation. Centralization of control functions are being accelerated and a new Office of Ethics, Oversight and Integrity has been established with regular reporting to the Board.

Source: https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/presentations/2017/board-report.pdf

Given the right conditions, employees feeling "psychologically safe" to speak out, can make risk mitigation suggestions, put forward opportunities and do the right thing. This known safety can help to grow a business and enhance its reputation. The route to creating an ethical company is to manage the conditions and encourage reporting without inhibitions.

Case Study: Openness and psychological safety to face into issues yields reputational gains

Built at a cost of £18m, The Millennium Bridge in London was opened by the Queen on 10 June 2000. The 320 metre Bridge was closed almost immediately due to the fact that it developed a worrying "wobble". Rather than abandoning the project, the bridge's engineers (Arup) immediately reacted and started to search for a solution, which they successfully implemented just over a year later. As a result of learning from the problem and staying with the project, Arup's reputation was actually enhanced, and a number of other bridges were improved as a result of the findings. Their culture is stated as being one of constant creativity and learning, approaching everything as an opportunity to learn and improve.

Source: http://news.bbc.co.uk/hi/english/static/in_depth/uk/2000/millennium_bridge/default.stm)

2. The Role of the Board, CRO, and Management

2.1 Tone from the top

Risk culture is most effective when it is fully integrated into the business and inseparable from organizational culture – essentially they are co-dependent – one does not exist without the other.

Board and executive sponsorship is critical to influencing, and directing a strong risk culture. This can be achieved by reinforcing the importance of visibly relating risk culture back to the organization's purpose in decision-making and actions. Building a sound risk culture takes time. Consistent demonstration of what sound risk culture looks and feels like needs time to filter down from senior management to direct reports and across the business.

There is unanimity that tone from the top is crucial to setting organizational culture, but the mechanisms regarding what the Board and senior management can do in practice is more ambiguous. Regardless of Board structure, a single-tier board (unitary model) commonly, but not exclusively, found in countries influenced by the Anglo-Saxon style of corporate governance, or a two-tier board (dual model), consisting of a management board and a supervisory board more common to continental

Europe[2], the central message on risk culture responsibility is the same - boards, independent of management, have the responsibility for the effectiveness of risk culture and risk management systems. Boards have the authority to define, drive and change risk culture[3]. This matter is not the sole domain of the CRO just because the word "risk" is in the term.

Case Study: Risk Culture cannot be the sole responsibility of the CRO

One of Australia's largest banks announced losses in 2004 of AUD$360 million due to unauthorised foreign currency trading activities by four employees who incurred and deceptively concealed the losses. The bank had in place risk limits and supervision to prevent trading desks ever reaching positions of this magnitude. However, the risk management policies and procedures proved ineffective. Why? The trader's behaviour was heavily influenced by the "culture of profit-driven morality" which had primacy over any written risk disciplines or procedures.

This scandal identified the missing link between risk culture ownership and embedding within the management of risk-taking activities in the bank's trading area and highlighted the scant regard given to risk management systems as a way of doing business.

Boards are now seeking to define a more assertive culture oversight role. This renewed focus reflects a greater recognition that aberrant corporate culture can be the root of significant organizational and reputational risk harming multiple stakeholders such as customers/policyholders, employees and shareholders.

The Corporate Governance report published by the Business, Energy and Industrial Strategy Committee in April 2017 (following the major corporate governance failings at BHS and Sports Direct) states that:

'One of the key roles for the Board includes establishing the culture, values and ethics of the company. It is important that the Board sets the correct 'tone from the top'. The directors should lead by example and ensure that good standards of behaviour permeate throughout all levels of the organization. This will help prevent misconduct, unethical practices and support the delivery of long-term success'.

2.2 The Board's role

The Board, (unitary or multi-tiered) must take the lead in risk culture formation and management for the firm. Ostensibly, the Board has the required level of independence, the ability to challenge senior management, and the ability to direct management to take action as appropriate.

As the Board will not have deep insight into the everyday pressures employees face, they will need to empower the CRO and the Risk Function to gather management information on the firm's "as-is" risk culture and present back to the Board with a suggested desired "to-be" risk culture state.

In addition, the Board, in its role of approving the company's strategy, can reinforce the importance of risk considerations and issue management as an integral part of the corporate strategy discussions and decisions.

[2] In Germany, the BaFin has minimal standards for governance – the so called "MaGo" from 25 January 2017 – the responsibility for risk culture is assigned to the Board of Management. This includes both implementation and further development of risk culture (see: MaGo, chapter 6, Nr. 21). Given the fact, that the overall responsibility stays with the whole Board of Management, a Supervisory Board has the right to be informed, following the binding internal rules and procedures, just like for any other topic - but not necessarily tied or specific to risk culture.

[3] In Germany, the responsibility for the effectiveness of risk culture and the risk management system rests with the Board of Management (see: MaGo, chapter 10, § 1, Nr. 155). This means, that there is a link between risk culture and the risk management system. Being in charge of running and overseeing these frameworks, the CRO / Risk Management Function has a role, but there is no definitive list of concrete tasks.

2.3 The CRO and Risk Function role

A risk culture development program has three components where the CRO and Risk Function can be the "eyes and ears" of the Board, and work in close cooperation with the Board to:

- assess the current state of the firm – find tools, measures and indicators to help with this;
- set the "to-be" risk culture – define the ambition;
- manage the outcome feedback with reporting, action plans and monitoring.

In conducting the first two steps the CRO should consider the pros and cons of using internal and external resources when advising the Board. The use of internal expertise allows for greater corporate memory and institutional knowledge transfer. It can provide a better informed nuanced assessment of the organization and is more likely to obtain employee engagement. However, an insider may be reluctant to provide negative feedback given their ongoing need to maintain a working relationship with all areas of business. External expertise allows for a potentially more objective and detached approach and enables management to respond in a positive, supportive manner to a knowledgeable outsider who can draw on industry comparisons. In a 'shoot the messenger' culture, internal or external experts might not be tolerated if the opinion is negative, as the firm may not yet be receptive to critical feedback from either an insider or outsider, which is why a balance of the two is sometimes preferable.

Case Study: Relying on other business partners to assess the organizational culture

To provide an assessment of the organization's culture the CRO may be able to leverage other business partners to contribute to that discussion. These business partners may have objective and measurable information to share, and they may also contribute observational and anecdotal information. Other corporate functions that can be leveraged include: Legal, Compliance, Internal Audit, Human Resources. Business functions include: Sales, Marketing and Operations.

2.4 Risk presence throughout the Three Lines of Defence

Segregation of duties, or the "three lines of defence" governance framework, is deeply embedded in the risk language; however there is often a tension in how this separation is lived. On the one hand, the risk function is expected to be an independent body, existing apart from and giving an outsider's judgement on business decisions, but on the other hand, to be involved as a "business partner" enabling strategic business initiatives to be undertaken in a risk aware way. The risk function itself needs to decide how close it should get to the business while still retaining an independent view; a decision that is likely to be determined by the organizational culture of the institution itself.

Case study: CRO Forum Member multiple roles for a risk function to reinforce risk culture

Risk professionals will take on different roles in various situations which help to reinforce the understanding that Risk wears multiple hats in supporting the business in achieving its objectives.

The concept of 'different risk hats' has been developed as an aide-memoire. The "hats" recognise that at times risk managers '*coach*' - demonstrating deep understanding of the business and building collaborative relationships, at times '*operate as experts*' - offering technical expertise to manage risk, at times act as a '*steward*' - passionate about getting to the bottom of things, and, at times '*a challenger*' - able to influence, challenge and negotiate whilst not afraid of difficult situations.

The evidence of how embedded risk awareness and considerations are across the lines of defence can be seen through the behaviours exhibited in decision making and collaborative but "critical friend" interactions between first and second lines.

2.5 Organizational culture and risk culture become indivisible

For risk culture to be widely adopted it needs to be seen as relevant across the breadth of the firm. Business leaders must believe and act on it as a key component in the firms' success.

Case study: Dell: a culture that integrates ethics, risk and compliance into daily decision making

Dell believes acting ethically in all it does is good business and important to customers, suppliers and strategic partners. As a result, critical programs have been developed to address key risks across the enterprise. These programs operate under the oversight of the Dell Global Risk and Compliance Council (GRCC), which includes members of the Dell Executive Leadership Team and strategic functional heads such as Ethics, Audit and Accounting. This Council ensures both top-level leadership support and appropriate resources are available for Dell's risk and compliance programs, and that ethical decision-making informs strategic decision-making at the company.

When the first line uses Risk Culture to describe how they operate, form judgements, make decisions, and participate in effecting the firm's strategic objectives, it moves beyond something programmatic and becomes part of the firm's identity. The following case provides an example where the Board, CRO, Risk Function, Management, all lines of defence worked with new CEOs to transform the business and embed an acknowledged firm-wide risk culture in-to daily operations. Risk culture has become intertwined and inseparable from organizational culture.

Case Study: CRO Forum Member Tone from the Top and Actions from the Middle

In the last 20 years the CRO Forum member had four different CEOs, each of which played a major role in determining and shaping the business culture. In two cases, the business was considered to be in good health. The new CEOs used this as an opportunity to scale back and de-emphasise the importance of having an effective risk culture by marginalising risk and control disciplines and the associated operating costs - the implied message was the management of risk added little value. The other two CEOs joined following major crises and recognised the need for significant cultural change. With the support of the executive team, external consultants, internal change experts, project managers, internal audit, and the risk team large scale and rapid cultural change occurred. One of the foundational changes was the need for a strong and effective risk culture underpinning and facilitating the achievement of the firm's objectives. The degree of engagement with risk experts enabled a complete transformation of the risk and control environment. The openness and transparency about the business setting high standards and identifying and remediating control weaknesses resulted in over 1000 control gaps having been closed in the last two years.

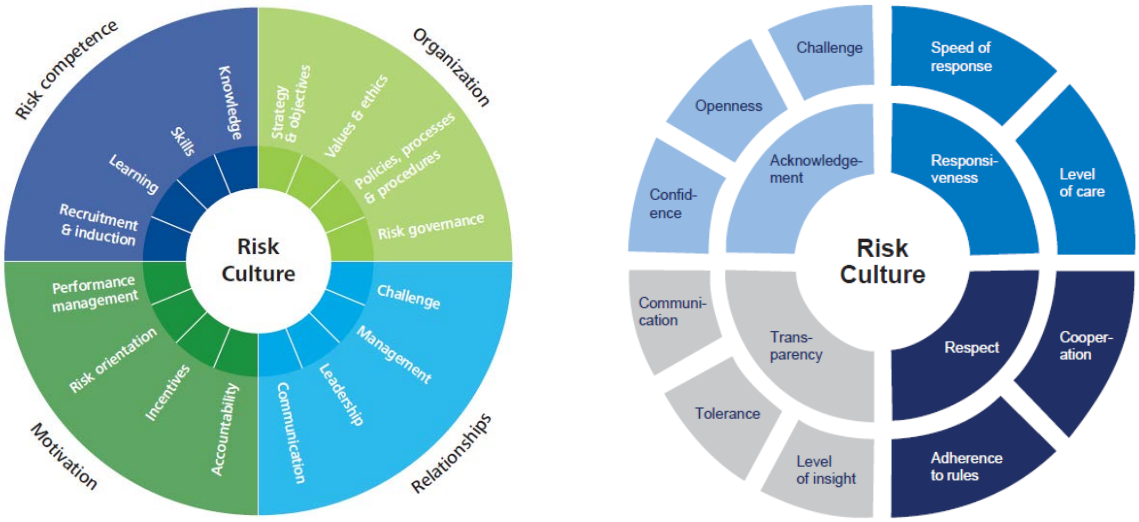
3. Developing a Risk Culture Framework

3.1 Identifying, measuring, assessing and monitoring risk culture

Identification

Examples of holistic risk culture frameworks from two consultancies are shown below. Others are listed in the references section, page 18. These require the identification of risk culture characteristics appropriate to the firm, and areas that can be measured and assessed.

Figure 2:



Source: Deloitte (2012) 'Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report'
Source: McKinsey (2015) 'Managing the People Side of Risk: Risk Culture Transformation'

Measuring and Assessing

There are a range of tools to assess current and on-going organizational risk culture, including surveys conducted across various segments of a firm, structured interviews with selected staff, root cause analysis around risk incidents, and evidence-based assessments.

There is no single metric or standardised combination of metrics, to evaluate a firm's risk culture. At the end of the process of information gathering and analysis, the best realistic outcome is an informed opinion based on agreed metrics and a qualitative interpretation of the data.

'Culture is "everywhere and nowhere". You can't take institutional culture down from a shelf and seek to change it in some mechanical way, [it is] an outcome more than an input' (Andrew Bailey, Chief Executive – Financial Conduct Authority, UK, 2017).

Whilst measuring risk culture is challenging, there are numerous metrics that, with further analysis and oversight, could be used to aid in forming an opinion about the risk culture within the organization. The challenge is to assess these matters on a *spectrum* in order to select the current and targeted balance.

An assessment of behaviour using the vice-to-virtue-to-vice spectrum (see section 3.3) will allow for insights to be shared with senior management and the Board. Some behaviour may not be easily measureable let alone apparent, and may be more anecdotal. Areas for vigilance (below) may emerge and help management to direct action plans to remedy:

- Siloes of thinking and behaviour where departments within the firm fail to involve their peers in other functions;

- Unwillingness to share information on a timely basis, or seek departmental success to the possible detriment of the firm overall, e.g. getting a product to market on time but leaving significant IT issues that will need to be addressed by another function;
- Unwillingness to talk internally about corporate mistakes – absence of a learning culture;
- Tolerance of minor policy/regulatory/code of ethics breaches by star employees;
- Hierarchical attitudes and insights of internal subject matter expert employees not actively sought out, or a reliance on third party consultants as an indicator of an underlying cultural reticence to challenge;
- Lack of access to information, or hoarding of information (the "knowledge is power" mind-set), in particular a lack of sharing with the control functions;
- An organizational culture where the control functions are openly challenged or diminished by senior business leaders and there is a strong negative, almost kneejerk response, to instances where oversight is required;
- Blaming Risk to deflect attention away from contributing factors regardless of the fact base;
- Lack of knowledge, staff not being aware of company risk management, compliance and ethical expectations either due to poor training or employee inductions;
- Staff turnover and retention rate, not just "how many" but "who".

Monitoring and Reporting

Types of quantitative Key Risk Indicators (KRIs) to inform both positive and negative risk culture trends include:

- Fines/regulatory breaches
- Breaches of the code of conduct or ethics
- Employee internal training completion rates, including senior persons
- Customer complaint (type and volume) and follow-up processes, including resolution rates
- Management response to Internal Audit recommendations; the percentage of actions closed within agreed-timelines
- Frequency and size of financial reporting corrections
- Volume of policy breaches
- Proportion of employees who were assigned a risk management type goal as part of their annual appraisal and who met these goals.

Quantitative KRIs are typically supported by qualitative indicators, as shown in the whistleblowing example below:

- Are reporting lines on whistleblowing independent of management?
- Does management have a good process for investigating individual reports?
- Does management conduct trend analysis?
- Is there timely follow-up?
- Are reporters assured anonymity? Do the reporters stay within the company or leave?
- Is there training to prevent retaliation?
- Is there clear reporting to the Board with details and metrics that demonstrate a transparent process?

3.2 Information sources to assess the current state of risk culture

There are a numerous sources of information to assess the current risk culture state. The key challenge is to triangulate the disparate sources of information to uncover pockets of concern. E.g.:

- Social media commentary (as assessed by Communications);
- Feedback from suppliers / distributors who have experience dealing with employees and see behaviour (as assessed by Procurement);

- Quality of regulatory relationship(s) - attitude to regulators and the regulators' attitude to the firm (as assessed by Legal or Compliance);
- Employee survey results, including open text boxes (as assessed by HR);
- The internal grapevine (various inputs);
- Comments from frontline staff who are closer to the culture and witness it daily (various inputs),
- Employee exit comments / opinions (as assessed by HR);
- Statements by rating agencies, investors and their observations of management actions (as assessed by Investor Relations).

Case Study: CRO Forum Member Getting a read on the state of the risk culture

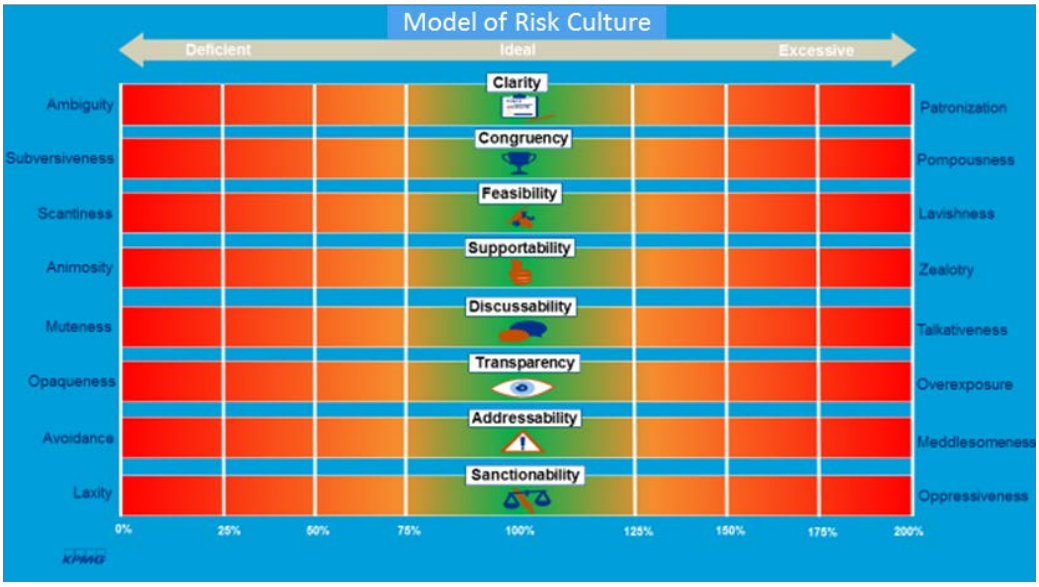
A firm used its regular staff survey to derive a risk culture index. Risk had collaborated with HR and included a few risk culture questions in the wider staff survey (about 5 out of 70 questions); for example whether employees feel able to speak out without fear of consequences. On reflection and reviewing the survey results, it realised that a number of other questions were also indicative of risk culture. It therefore consulted with risk leaders to finalise the selection and weighting of questions for a risk culture index. The external provider of the questionnaire then applied the index to the survey results and produced granular risk index results, which were moderated for variances in general engagement reported from different teams and territories. The results were then used to adjust the targeting of risk and control assurance work.

3.3 Assessing the organization on the vice-to-virtue-to-vice spectrum

Aristotle's doctrine of the mean states that a virtue is the mean state between two vices: a deficient and an excessive one. The Corporate Ethical Virtues Model, as developed by Muel Kaptein[4], defines the mean and the corresponding deficient vice for seven virtues and explores why organizations characterized by these excessive vices increase the likelihood that their employees will behave unethically.

For example, if the virtuous state is clarity, the one extreme would be ambiguity and the other extreme would be patronization, whereby employees feel that management is communicating to them in a demeaning or patronizing fashion. A patronizing environment can be just as damaging to one where there is a lack of clarity (see Figure 3).

Figure 3:



[4] Kaptein, M. (2017). When organizations are too good: Applying Aristotle's doctrine of the mean to the corporate ethical virtues model. *Business Ethics: A European Review*.

Many hard and soft levers (from Figure 1) can also be assessed on the *vice-to-virtue-to-vice spectrum* and ideally the Risk Function is able to assess what is the desired balance for the organization. For example, if the Risk Function is measuring whistle-blower matters, an absence of any reports may indicate a culture where employees feel unsafe to report or to speak, do not trust the process, or are completely disengaged. High volumes of reports could be indicative of major problems. The "virtuous" point may be somewhere in the middle where employees feel able to report, but the volume is moderate. Although the presence and use of whistleblowing is a hard lever, it is the indication of psychological safety that employees are able to speak out and are comfortable in the way management responds and handles whistle-blowers that matters. This understanding may provide more insights to risk culture than data on the number and substance of the whistleblowing matters themselves.

4. Risk Culture Management

4.1 Defining hard and soft levers

Policies, processes and controls that a firm uses to manage its business are known as 'Hard levers'. 'Soft levers' which support hard levers may be less readily observable, but tend to be the levers that deliver more reliable and enduring risk culture outcomes.

Examples of Hard Levers	*Examples of Soft Levers*
• Strategy, policies and company values (codes of conduct) that are clear and broadly communicated; • Risk Appetite statements that are understood and acted upon by the relevant stakeholders; • Clear organizational structure: governance processes for decision making; escalation processes, limits, tolerances; evidence that these elements are working as intended; • Control frameworks: ERM, SOX, Internal Controls; evidence that controls are working as intended; • Post-event root cause memo assessing the underlying cause is prepared and discussed; • Remuneration Frameworks encourage the right behaviour and discourage undesired behaviour.	• Tone at the top – behaviour and decision making from the leadership is consistent with the message being communicated; • Corporate communications that are consistent – same message being delivered regardless of whether "the microphone is on"; • Career pathing and promotion that reflects shared values and accountability; • Coaching and mentoring behaviour by senior employees demonstrating a commitment to the organization; • Openness to lessons learned discussions and continuous improvement giving employees a voice/freedom to speak and feel safe to "do the right thing".

4.2 Formal processes vs. informal networks in business decisions

Well-structured formal processes such as segregation of duties are a central aspect of risk management, in that they assure a hard and visible control over major business decisions. Formal processes involve things like inclusion of risk personnel in key decision making bodies, inclusion of the risk function in vetting loops for major business decisions, and formal approval of risk guidelines in decision-making Boards. These processes have the additional benefit of putting risk topics "front of mind" for the first line as well as senior management.

There are caveats to the formal approach:

- relying exclusively on formal processes may create a false sense of security that there is a presence of risk culture; and

- creating a library of prescriptive rules and procedures may mean that compliance becomes a "tick the box" exercise and the spirit and behaviours that the procedures were trying to instil are ignored. An excess of policies and procedures can actually harm an organization's risk culture as employees may feel that they are good corporate citizens by obeying the rules, but, their actions may contravene the desired intention.

This danger of becoming too formulaic and prescriptive was also described by the UK House of Commons Business, Energy, and Industrial Strategy Committee on Corporate governance published in April 2017:

> *"Good company culture does not lend itself to easy measurement and cannot be enforced via a tick box exercise. Instead, the central tenets of good corporate governance should be embedded in the culture of all companies, so that it permeates activity at every level and in every sphere"*[5]

On the opposite side of formal processes are the informal ones – known as networks through which knowledge and information flows. Understanding and reporting on the effectiveness of informal networks is crucial to understanding risk culture. For example, when the risk team is seen as a trusted advisor or critical friend, their point of view is sought out at the beginning of the process, as part of the way the firm operates. Robust debate often happens behind the scenes with a final decision reflecting all concerns. The absence of informal effective networks could be seen as a cause for concern about the willingness and ability to communicate risk issues or the respect and regard of risk disciplines in executing business decisions.

Characteristics of both approaches which enable the embedding of risk culture are outlined below:

Formal Processes	Informal Networks
• Segregation of duties • Formal inclusion of risk personnel in key decision making bodies • Formal inclusion of risk function in vetting for major business decisions and planning • Formal approval of risk guidelines in decision making Boards	• Risk personnel formerly in first line functions • 1st line personnel with previous second or third line experience • Risk personnel with a specific deep expertise • Cross functional projects including 2nd and 3rd line

Ideally a risk mind-set is present at the outset of any business consideration, with potential positive and negative outcomes defined in advance. This is easier said than done, as to some extent all decisions are influenced by shared experiences and biases within the organization.

4.3 Sub cultures within large groups

Perspectives of risk will differ at regional / divisional levels from a group or headquarter level. Additionally, local attitudes and business practices may differ dramatically based on culture, geography and language. As the Irish writer George Bernard Shaw famously said: "England and America are two countries divided by a common language."

Risks can diversify away or be compounded when aggregated to a group level. At a business unit level, local adherence to a group-led risk mandate and culture may lead to one set of conclusions very different from that of a group lens. Whilst this can be reflected quantitatively through risk limits, the more qualitative assessments of local management may not be applicable and could be negatively influenced by fears on the effect on their own business. Indeed, business units that know they are not

[5] Source: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmbeis/702/70205.htm#_idTextAnchor012

material from a group perspective may find it harder to view risk in the same way – the parent is seen as the lender of last resort, since default would be too damaging to reputation. Risk is reduced to compliance or limits, and it becomes harder to embed a cultural overlay—this situation will change as smaller business units mature and reach scale, provided they are supported to effect change.

The CRO could advise the Board about the limitations of any program that is centrally managed—the Board can either accept these limitations or encourage the development of local/regional risk cultures that reflect local approaches for certain matters, with strict adherence to group standards for other matters. Openly challenging management may not be possible in the local culture, but a good whistle-blower program will allow matters to be escalated.

4.4 Risk culture evolution

Implementing organizational change can happen in both 'engineered' and 'organic' ways.

Engineered changes are ones that can be implemented short term, for example a change in governance structure, or a change in financial incentives. Short term changes are easier to implement where there are clearly understood incentive structures, e.g. bonus incentives meeting clearly defined objectives and scorecards that include risk behaviours.

Organic changes which address less tangible outcomes may be harder to design and implement, and take longer to materialise. The organic approaches are self-driven. As early as the recruitment stage the human resources department plays an important role in reinforcing the desired risk culture by hiring people more likely to foster the culture. Other organic reinforcing approaches include: deliberate collaboration between various lines of defence; company recognition or awards of the right behaviours; non-monetary incentives, including career advancement and performance evaluation commentary, and exposure to management.

To encourage a high level of competency, development and risk understanding across the firm, some companies rotate talent that has been identified as 'management potential' through positions in to second or third line roles. Such actions indicate the firm is "invested" in the individuals and their potential. These are the changes that reinforce the organizational messages that employees are valued and typically get the most buy in and are most likely to hold long term.

Case Study: CRO Forum Member – Risk Culture Evolution

Internal and external resources used to develop and embed risk culture in three phases.

- ~ 12 months: Diagnosis of the as-is state using external consultants and collaboration with internal resources to validate direction. The articulation of, and mobilisation around, the desired state risk culture began. First line customer facing colleagues were appointed as risk champions. A complete refresh of the risk policy suite and the establishment of Line 1 ownership of risk/ control design and testing, reporting and action remediation. The appointment of Line 2 technical experts to assure the effectiveness of the Line 1 controls.
- ~ 24 months: Embedding hard controls through the strengthening of governance, reporting and the establishment of new control review forums to oversee the closure of policy and control gaps.
- Post phase 2: Enduring sustainability where the risk team place reliance on the maturity of the risk culture to partner with the business and oversee pruning of low value controls because demonstrated behaviours are embedded and incentives ensure the continuity of the behaviours.

5. Understanding the experience of the risk culture

Consistencies in the messaging and behaviours of middle and senior management are used by employees to work out what to do, how to do what they do and show others – through their own behaviour – how they have interpreted the 'rules'.

Questions to ask when considering the level of embedding include:

- Is the company purpose and strategy clear?
- Is there clarity on the desired cultural outcomes supporting the strategy?
- Are company values, expected behaviours and attitudes understood and rewarded?
- Are risk management incidents diagnosed in an open and transparent way assessing motivations, process and outcomes that enable others to learn lessons?
- Are risk appetites clear? Do experts have access to the big picture information they need to make informed decisions within those appetites?
- Is the company encouraging and fostering an environment where diverse thought, challenge and debate are commended?
- Is there an ongoing education and communications programme tailored to the different roles within your organization?
- Does management actively take appropriate action to deal with parts of the organization that disregard the established risk culture?
- Is management regularly sharing good and bad stories which reinforce the attitudes and behaviours that will drive your desired cultural outcomes?

5.1 Communication of risk culture

Everyone has a role to play to ensure that communication about risk culture, and expectations from employees, remain aligned to the business objectives. Risk communications can occur through various methods:

- CEO statements and town halls;
- Forums that share lessons learned, mistakes, and the right motivation;
- Consistent statement and actions through middle management;
- Alignment of rewards and compensation system with risk policies, procedures, and risk appetite statements;
- Disseminated communications through teach-ins, e-learning, “meet the risk team”, etc.;
- Escalation mechanisms to ensure that risk dialogues occur.

The relevance of these communications can best be tested by asking: Would the content of these communications have prevented bad behaviour from emerging or continuing? Would they survive the application of testing them against past corporate failure enough to have made the difference and serve the intended purpose?

An example from one of the CRO Forum members below describes the way that firm ensures that cultural lessons are learned across the functions:

Case Study: CRO Forum Member Risk Tales

Each quarter, three summarised studies of actual situations, chains of events and behaviours leading to failures in Risk Management (*“Risk Tales”)* from both within the insurance industry and beyond are shared internally with the entire Group. The aim of these Risk Tales is not to criticise the shortcomings of other companies, but to develop risk culture across all departments and levels of the company, to educate staff on risk management principles by identifying lessons learnt from past failures and to demonstrate the application of Enterprise Risk Management in real life contexts.

Example: A recently released Risk Tale details the bankruptcy of an international airline due to the realisation of a number of market and strategic risks. The company failed to envisage a scenario of rising fuel costs and were also unaware of upcoming regulatory changes that soon allowed a number of low cost competitors to enter the industry. Another contributing factor to the airline’s demise was a poorly handled acquisition involving incompatible corporate cultures. The CRO Forum Member then describes its practices in these areas including; hedging against market risks, monitoring legal and supervisory developments which could impact the Group and, following high internal standards for acquisition integration.

5.2 Performance management

Management is always faced with the challenges and trade-offs from balancing short term targets such as share price or quarterly sales and long term targets such as building a sustainable business. A compensation scheme that acknowledges the tensions between business goals, and the means and methods used to achieve those goals, will allow for risk culture to be included in the performance assessment.

Amongst the levers that make risk aware behaviours and outcomes very personal to employees, few are as potent as the effect of formalised risk modifiers (up or down) to group bonus pools, individual bonus awards and ultimately, career progressions. Board level remuneration committees using the input from Group CROs into their respective Board Risk Committees will be able to use actual events and decisions taken within an award period to apply and reinforce messages and measures concerning risk aware behaviour when agreeing bonus pools and management awards. In addition to knowing and understanding the effect of hard measures on the awarded bonuses, teams and individuals will be able to see the direct link of award modifications made (up or down) because of risk driven behaviours – a situation that creates the opportunity to reinforce risk aware values and behaviours.

Case Study: CRO Forum Member Balanced Scorecards and Remuneration Risk Modifiers

Annual objectives are set using a balanced scorecard approach--hard metrics on financial performance, and softer measures covering outcomes demonstrating alignment to firm values. Progress and adjustments are then tracked throughout the year. At the end of the year, Business Unit CROs write an independent assessment to their Group CRO to assist the Board Risk Committee in making a recommendation to the Board Remuneration Committee on whether adjustments should be made to Business Unit's and Head Office bonus pools based on their view that risk considerations and risk management disciplines were fully taken into account during the year. The assessment input from Business Unit CROs covers the following areas:

- context on the risk environment;
- assessment of business unit performance against risk appetite (including risk limits, policies, and the overall effectiveness of risk management and internal controls);
- actions taken to mitigate risks or improve controls;
- the degree to which the metrics and other mechanisms available for assessing and adjusting performance are appropriate in the context of risk appetite;
- highlights of any risk issues or incidents that have arisen during the performance year;
- any matters that should be considered in the determination of remuneration outcomes; and
- exceptional behaviours and judgements, both good and bad.

6. Developments

New roles are emerging to assist firms and risk functions in embedding and managing the complexity of risk culture. Ethics departments working alongside compliance, focus on spreading and enforcing sound risk culture, by emphasising behavioural rather than legal issues. Such a department could have helped avoid certain crises in the automobile industry (when software was developed with the sole purpose of cheating regulation, or decisions were made to maintain the production of certain pieces in a pure cost/benefit consideration at the expense of bodily injury and reputational losses). However, ethical considerations could prove difficult owing to the ambiguity behind morality, as this depends on such things as the country and industry culture.

Case study: "Psychologists and Compliance Officers"

At the Association of Compliance Officers in Ireland (ACOI) in January 2017, the Central Bank of Ireland (CBI) Director of Insurance Supervision, noted that the CBI has an in house organizational psychologist working with it to enhance their supervisory approach. It was noted that the psychologists' work has focused on how to identify key influencers of culture in the organizations it supervises, whether cultures are effective or ineffective and how to aggregate information to form a holistic view of a company at a point in time.

It was also noted that ultimately a sound culture of risk requires engagement from the industry itself – the senior management teams of companies, the Board members and compliance officers. As key function holders and leaders in the organization, it requires their on-going drive, persistence and support. Compliance officers have a responsibility to influence this culture across their organization. Not just one of compliance, but one of thinking how we can do things better. Increased regulation in the area of risk culture means that it is something that companies and their compliance officers will have to be more involved in.

7. Conclusion

The key to building a "good risk culture" is first to understand and articulate the cultural outcomes that will drive the right performance and support the delivery of an organization's strategy. It needs to be recognised that this "good" risk culture is actually the aggregate view of many sub-cultures which relate to different business activities.

Seeing risk culture as simply a governance check - focussing on inputs, checklists and frameworks, and trying to implement one way of working or thinking will be a drain on company resources risking company performance and opportunities. There is unlikely to be a single right way for one person to behave, so what matters is that groups of people constructively challenge each other and check that the overall behaviour is what is desired.

There will inevitably be some risks which require strict controls within any organization. However, knowing the desired cultural outcomes expected allows organizations to adapt more easily and supports greater resilience as different views and perspectives come together in pursuit of a common outcome. It entrusts the experts of an organization to "do the right thing" in the interests of the defined common goal.

There is more than one good culture. What works well in one area may be toxic to another, so having a "one size fits all" approach carries a great risk. Fundamentally, the attitude and behaviour of the Board, management, and all lines of defence is what determines whether the soft and hard levers will achieve a desired outcome, and therefore it is crucial to get buy-in across the organization.

Finally, embedding risk culture is not a one-time project or change programme. It's a way of life. An ongoing process of education and story-telling which changes not only behaviours but the underlying mind-sets that drives employees' thinking, decision making and behaviour. Without an ongoing dialogue, which enables employees to test and refine their understanding of what "good" looks like, culture, and risk culture as a subset of it, gets stale and fails to keep pace with the dynamic environment companies operate in.

REFERENCES

Articles and other references including industry bodies

http://www.gallup.com/businessjournal/163130/employee-engagement-drives-growth.aspx

https://www.centralbank.ie/news/article/remarks-by-director-insurance-supervision-sylvia-cronin-at-the-association-of-compliance-officers-in-ireland

http://www.corpcounsel.com/id=1202783481218/Advising-the-Cultural-Revolution-in-the-Boardroom?slreturn=20170319095852

https://globenewswire.com/news-release/2017/03/28/945857/0/en/NACD-to-Explore-the-Board-s-Role-in-Overseeing-Organisational-Culture.html

http://www.journalofaccountancy.com/news/2017/apr/habits-of-top-risk-managers-201716479.html

https://www.nytimes.com/2017/02/22/technology/uber-workplace-culture.html?_r=0

https://www.forbes.com/sites/rajeevpeshawaria/2017/02/28/uber-bare-four-steps-to-avoiding-a-corporate-culture-disaster/#255d62536119

http://www.strategic-risk-global.com/future-of-risk-management-new-risk-culture/1408089.article

https://www.centralbank.ie/news/article/remarks-by-director-of-markets-supervision-gareth-murphy-at-the-launch-of-the-duff-phelps-global-regulatory-outlook

http://www.lse.ac.uk/accounting/CARR/pdf/Final-Risk-Culture-Report.pdf

The Institute of Risk Management: https://www.theirm.org/media/885907/Risk_Culture_A5_WEB15_Oct_2012.pdf

Financial Reporting Council: https://www.frc.org.uk/getattachment/3851b9c5-92d3-4695-aeb2-87c9052dc8c1/Corporate-Culture-and-the-Role-of-Boards-Report-of-Observations.pdf

Consultancies

Mindgym: https://uk.themindgym.com/

Deloitte: https://www2.deloitte.com/lu/en/pages/risk/articles/cultivating-risk-intelligent-culture.html

KPMG:https://home.kpmg.com/uk/en/home/insights/2017/04/how-to-create-a-robust-risk-culture.html

EY:http://www.ey.com/Publication/vwLUAssets/Risk_culture_-_How_can_you_create_a_sound_risk_culture/$FILE/EY-risk-culture-model-brochure.pdf

PwC:https://www.pwc.com/us/en/risk-assurance/risk-in-review-study/survey-findings-risk-culture.html

McKinsey:http://www.mckinsey.com/business-functions/risk/our-insights/taking-control-of-organizational-risk-culture.
https://books.google.co.uk/books?id=U1oYbmA7zCYC&pg=PA50&dq=McKinsey+Risk+Culture&hl=en&sa=X&ved=0ahUKEwi-kb7U05XWAhWnIcAKHXOHAK4Q6AEIJjAA

Willis Towers Watson: Series of blogs. Example: http://blog.willis.com/2017/05/how-to-measure-risk-culture/

Oliver Wyman: http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/apr/MMC-Global-Risk-Center-Risk-Culture-2015_2.pdf

Tactix:http://www.tactixconsultancy.com/library/Conduct%20Risk%20and%20a%20Culture%20of%20Voice.pdf

CRO FORUM

The CRO Forum is supported by a Secretariat that is run by

KPMG Advisory N.V.

Laan van 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands