Sound Risk Culture in the Insurance Industry

May 2015

CRO FORUM

Table of Contents

1   Executive summary

This paper aims to convey the importance of a sound risk culture within an insurance organisation. We use the term "sound" instead of "right" or "good" because in the same way that a corporate culture is unique, so is its risk culture. We also want to avoid giving the impression that a "one-size-fits-all" concept exists, that could be applied in any company. Through using the word "sound", we emphasise that a risk culture needs to effectively support the long-term goals, and in particular the risk vision, that a company has set. This highlights how essential it is to look at risk culture from a holistic point of view: an element that influences and is influenced by various forces. Although risk culture is often associated with the elimination or minimization of risk, we argue that it is crucial that it supports the desired level of risk-taking, driven by and aligned to the risk vision.

Although risk culture as a topic has become prominent in regulatory circles, we believe managing one's risk culture should be of intrinsic interest to insurers. Organisations should have a clear vision for their risk culture, actively manage and monitor it and take the necessary steps should there be deviation from a target state. We consider risk culture as an integral part of a holistic risk management framework. A company may have sophisticated risk management tools, models, processes and functions, but if its risk culture is not aligned to the agreed goals of the organisation, these tools, models and processes will not deliver successfully.

This paper reflects on the definition of risk culture and its importance for insurance companies, based on results from a survey among the members of the CRO Forum and CRO Council in February and March 2014. It provides examples of good practice on how cultural change can be driven and what the insurance industry can learn from other industries. It gives an overview of how this seemingly abstract concept can be made more tangible with the identification of essential components of a sound risk culture and how these components can be managed. To make sure that a sound risk culture is not only practiced by risk specialists within an organisation, the paper also looks at ways to make the concept comprehensible for all employees.

We contribute to the current discussion about risk culture by:

■ Providing insights into what risk culture means to CROs in the insurance industry;

■ Offering examples of good practice from the insurance and aviation industries on how to manage risk culture: taking risks seriously, learning from mistakes and creating comfort to talk openly; and

■ Gathering concepts to convey risk culture: setting the example, taking people along the change, answering the question "What's in it for me?"

The aim of this paper is not to derive a single, universally valid risk culture concept with rules for companies across the insurance industry. Rather, we share experiences and best practice and develop a foundation that identifies important cornerstones when establishing a sound risk culture.

2 Definition and issue identification

2.1 Why risk culture matters

The explosion of BP's Deepwater Horizon offshore oil rig in April 2010 resulted in one of the largest environmental catastrophes of its kind. An estimated three to four million barrels discharged until the leak was capped in July 2010. Eleven people were never found after the explosion of the rig. Previous accidents included a narrowly missed platform explosion in 2003, a refinery explosion in 2005 and a ruptured pipeline in 2006 - all in connection with safety standards' violations. It was in 2007, that the then CEO Tony Hayward promised to improve risk management.[1]

Such examples have resulted in an increased awareness of risk culture in various industries and the public eye. The interest increased further in the aftermath of the 2008 financial crisis. According to a survey conducted by Ernst & Young (EY), in cooperation with the Institute of International Finance (IIF), among 52 companies from the financial services industry in 2014, more than half of the participants indicated that they had increased their focus on risk culture within the past 12 months.

The main factors driving risk culture up in the agenda of organisations are:[2]

Leadership pressure

Boards and senior management are increasingly requested to evidence that they hold their staff – across all levels of the organisation – accountable for their behaviour. Furthermore, Boards seek comfort that management is fostering a sound risk culture, which supports the strategy and risk appetite.

Higher consumer protection standards

During the past years, the financial services industry has experienced and observed considerable settlements and fines for actions that are considered detrimental to customers. The resulting initiatives that put the customer at the centre, focus heavily on culture and ethics within the organisations themselves. Organisations are focusing attention on processes that help avoid fines in addition to those usually in place to manage the impact once the lawsuit occurs.

Negative public reputation

Ongoing failures, fines and settlements have publicly questioned the underlying ethics of those in the financial services industry. The wide-spread opinion is that financial institutions put their own interest ahead of customers' and society's.

Additionally, the interest in the topic is fed by the increasing focus of supervisory authorities on risk culture. In its publication in September 2014, the British Financial Reporting Council[3] lists a number of questions for boards to consider, including:

■ In what way does the Board satisfy itself that the company has a "speak-up" culture and that it systematically learns from past mistakes?

---

[1] Enterprise Risk Management Initiative (2010), *How did BP's risk management lead to failure?*, North Carolina State University

[2] Based on expert interview with EY in February 2015

[3] British Financial Reporting Council (2014), *Guidance on Risk Management, Internal Control and related Financial and Business Reporting*

- How has the Board considered whether senior management promotes and communicates the desired culture and demonstrates the necessary commitment to risk management and internal control?
- How is inappropriate behaviour dealt with? Does this present consequential risks?

While we appreciate that such publications may serve as guidance to organisations and their Boards, we nevertheless advocate that risk culture should be of intrinsic interest to insurers and not externally regulated. All our survey participants agree that over-engineered regulatory initiatives to assess risk culture can have destructive consequences. The main fear is that establishing a regulatory framework around risk culture may depreciate alternative approaches to foster risk culture.

Survey on Risk Culture among members of the CRO Forum and the CRO Council

Throughout February and March 2014, we conducted a survey among 35 insurance companies, all members of the CRO Forum and the CRO Council. 75% of the participating companies write both life and non-life business. While almost all companies describe themselves as Global Players, their businesses are primarily based in North America and Europe, with about half of the participating companies also active in Asia and Latin America. The survey evolved around the four topics:

- What are the elements of a sound risk culture?
- Why does risk culture matter?
- How can "good" risk cultures be maintained?
- Can and should risk culture be externally regulated?

The key findings were:[4]

97%
of survey participants believe

Profitability and risk culture are closely linked in the long term.

96%
of survey participants believe

Good risk cultures **cannot be achieved by solely behaving according to the letter of law**.

64%
of survey participants believe

Insufficient control and a **lack of enforced accountability** are among the root causes for degrading sound risk culture.

63%
of survey participants believe

One of the counter measures to avoid degrading a sound risk culture is a **set of effective incentives** such as risk-based remuneration.

---

[4] For more survey results, see section 3

2.2   Definition of risk culture

While there is a common understanding of risk culture's purpose and the high level elements it entails, no single definition exists. Most of the approaches to describe and formalise risk culture build on psychological, behavioural and organisational aspects. In this paper, we will rely on the following definition:

> "RISK CULTURE IS A SHARED PHILOSOPHY OF MANAGING UNCERTAINTY THAT IS EMBEDDED WITHIN AN ENTITY."
>
> DOUG CALDWELL, CRO NN GROUP 2013

This definition has the following assumptions:[5]

- Risk culture is a continuous process. It may renew itself and be subject to shocks;
- Risk culture is a mix of formal and informal processes. It involves a myriad of small behaviours and habits which in aggregate constitute the state of risk culture; and
- An organisation may have one single trans-organisational risk culture or several sub-cultures based on one overarching set of guiding principles.

Risk Culture and Corporate Culture

Similarly to the risk strategy needing to align with the corporate strategy, an organization's corporate and risk cultures must be linked. A risk culture needs to support the objectives of the whole organization and become an integral part of the corporate culture, as opposed to supporting just the objective of those in Risk Management.

---

[5] Based on Power, Ashby & Palermo (2013), *Risk Culture in Financial Organizations*

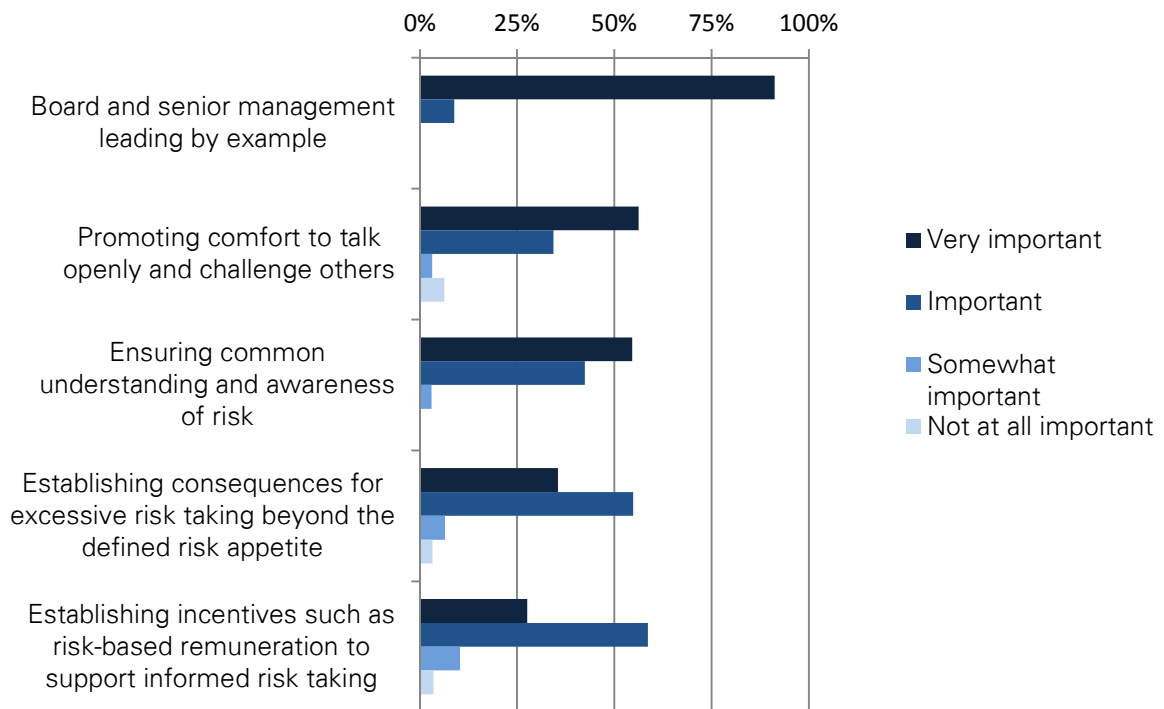## 3 Developing a risk culture concept from a practitioner's perspective

This section provides insights into:

- What are **essential elements** of a sound risk culture?
- How do we **manage** risk culture?
- How to **convey** the concept of risk culture?
- What can we learn from **other industries**?

3.1 What are the essential elements of a sound risk culture?

A number of papers have been published addressing the various elements a sound risk culture entails. The main drivers include the desire to make the concept of risk culture more tangible, and going a step further, making risk culture measurable.

Our survey asked participants to indicate the importance of a number of elements[6] that contribute to a sound risk culture. While the importance of individual elements was rated differently, survey participants agreed that only a combination of multiple measures would allow for an effective implementation.

Survey results highlighted that participants saw the Board and senior management leading by example as the most crucial element for establishing a sound risk culture.

---

[6] Elements were adapted from the FSB's consultative document, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture* (November 2013)

The following quote by Steve Balmer, former CEO of Microsoft, emphasises the importance of this element:

> "EVERYTHING I DO IS A REINFORCEMENT, OR NOT, OF WHAT WE WANT TO HAVE HAPPEN CULTURALLY. …YOU CANNOT DELEGATE CULTURE", STEVE BALLMER, FORMER CEO OF MICROSOFT

The second most important element for fostering a sound risk culture, was seen as the establishment of an environment in which people feel comfortable to communicate openly and challenge each other, including their superiors.

Ensuring a common understanding and awareness of risk was ranked as the third most important factor. However, almost 60% of respondents believed that it was not sufficient to only have a shared understanding of the company's risk culture, its principles and leading practices in order for all individuals to adhere to the risk culture.

The last two elements related to the importance of establishing accountability and incentives towards employees for a sound risk culture. Survey participants saw establishing consequences for excessive risk taking beyond the defined risk appetite as equally important as establishing incentives, e.g. risk-based remuneration to encourage and reinforce informed risk taking.

Risk culture is not applicable to the risk management function alone, but to all activities and levels within an organisation and should thus be mirrored in the operational activities of the firm, for example. This, however, raises the question whether it is sufficient and feasible to have only one concept in place or whether there is the need to establish several sub-risk cultures with an overarching common basis.

Example: How can we make Boards comfortable that there is sound risk culture in place - Risk culture questionnaire

Corporate governance requirements are increasingly demanding that Boards understand and address their firms' risk cultures. It is the Board's responsibility to set, communicate and reinforce a risk culture that consistently supports the embedding of its risk management policy, appetite and overall framework aligned to the overall business strategy.

Zurich Assurance Ltd has developed a catalogue of ten questions that should help the Board form an opinion on the company's current risk culture and assess whether further analysis and monitoring is required, namely:

- What tone does the Board set? Are we providing consistent, coherent, sustained and visible leadership in terms of how we expect our people to behave and respond when dealing with risk?

- How do we establish sufficiently clear accountabilities for those managing risks and hold them to their accountabilities?

- What risks does our current corporate culture create for the organisation, and what risk culture is needed to ensure achievement of our corporate goals? Can people talk openly without fear of consequences or being ignored?

- How do we acknowledge and live our stated corporate values when addressing and resolving risk dilemmas? Do we regularly discuss issues in these terms and has it influenced our decisions?

- How do the organisation's structure, processes and reward systems support or detract from the development of our desired risk culture?

- How do we actively seek out information on risk events and near misses – both ours and those of others - and ensure key lessons are learnt? Do we have sufficient organisational humility to look at ourselves from the perspective of stakeholders and not just assume we're getting it right?

- How do we respond to whistle-blowers and others raising genuine concerns? When was the last time this happened?

- How do we reward and encourage appropriate risk taking behaviours and challenge unbalanced risk behaviours (either overly risk averse or risk seeking)?

- How do we satisfy ourselves that new joiners will quickly absorb our desired cultural values and that established staff continue to demonstrate attitudes and behaviours consistent with our expectations?

- How do we support learning and development associated with raising awareness and competence in managing risk at all levels?

3.2 How do we manage risk culture?

How to create an environment in which everyone understands and embraces the concept of risk culture? How to establish responsibility and enforce accountability?

Internal organisation aspects: necessary pre-conditions

Although a sound risk culture consists primarily of mindset and behaviour – the informal processes - these need to be supported by a set of organisational mechanisms or enablers – the formal processes – that are considered preconditions to establishing sound informal processes.

The most common organisational mechanisms that help provide an fertile background to mindset and behaviour include:

Strategy, policies and company values that are clear and clearly communicated.

Company values reflect the company's beliefs, while policies reflect its boundaries. Together with a clear direction (the strategy or risk vision), values and policies help employees when considering risks in any decision – strategic, tactical or operational - taken on a day-to-day basis. They determine the playing field and encourage empowerment of employees therein.

Risk Appetite statements

Effectively part of the business strategy, each company should define and clearly communicate its key risk appetite statements. In addition to quantitative statements that are omnipresent in the insurance sector, e.g VaR statements, a company should also formulate qualitative Risk Appetite statements that describe the preferences for (or against) certain risk-types. These statements support the strategy and business planning, contribute to avoiding unwanted or excessive risk taking and aim to optimise use of capital.

Clear organisational structure

Going beyond an organisational chart, a clear organisational structure includes documented responsibilities and clear decision making and escalation procedures. Unclear ownership leads to a dangerous lack of accountability. Clarity on roles and responsibilities with regard to oversight and

decision-making contributes to improvement capability and expertise to meet the changing needs of the business. Organisations across industries typically address this challenge by developing operational training, leadership development programs and empowering employees. Programs targeting leaders ensure that leaders understand the tools and techniques available to them in depth and are seen as role models.

Mastering conflicts of interest

It is crucial for risk management and business units to understand and accept to avoid conflicting interests:

- Business units focus on writing profitable business that serves customers' needs and increases shareholder value of the insurance company.

- Risk management functions focus on ensuring the long term viability of the firm, i.e. ensuring that the insurance undertaking is solvent even in the event of unforeseen circumstances, and that risks which the insurer is adverse to are not taken, thereby possibly contributing to a decrease in earnings and capital volatility.

These roles may be conflicting, e.g. when risk management sets limits for writing business. Accepting both roles improves the understanding and objectives of each and establishes the basis of a sound risk culture within the company. Business units and risk managers should communicate and work together to find the optimal solution to fulfilling their individual objectives, for example by involving risk management in new product processes or negotiations for large deals at an early stage.

When addressing these conflicts of interest, it is essential that business objectives and personal performance targets do not undermine the risk culture. It is useful when performance targets (are perceived) as conflicting in themselves (compare the Business Balanced Scorecard), forcing individual employees to balance several angles when taking decisions, without allowing dominance of a single factor e.g. sales targets, or cost reduction targets. All employees need to be aware of the organisation's approach to risk and understand that they will be held accountable for their risk taking behaviour. Encouraging and reinforcing the desired risk management behaviours is a key HR process (see paragraph 3.3). Following incidents in other industries such as transportation, bonus systems have been strengthened through the inclusion of defined safety standards.

To manage conflicting interests collectively, the three lines of defence model has proven to be effective. This model defines three lines, each with distinct roles, decision authorities, execution responsibilities, and oversight responsibilities.

First line of defence: the CEO (and the CEOs of business units), as well as members of their management board collectively make business decisions, and retain primary accountability for the performance, sales, operations, investments, compliance, and related risks affecting their businesses.

Second line of defence: independent oversight and support functions with a major focus on insurance, market, operational, legal and compliance risks. The oversight functions must have an organisational position with sufficient countervailing power and:

- Develop the policies and guidance for their specific risk and control area;
- Encourage and objectively, as well as actively, challenge/monitor sound risk management throughout the organisation and coordinate the reporting of risks;

- Support the first line of defence in making proper risk-return trade-offs; and

- Have escalation power in relation to business activities that are judged to present unacceptable risks to the company.

Third line of defence: internal audit (IA). IA provides independent assurance on the effectiveness of business and support processes, including governance, quality of risk management and quality of internal controls.

People: mindset and behaviour

On a daily basis, people take decisions that can have a significant impact on the company's business outcomes, both in the short- and long-term. To improve effective decision making, all of the following contribute:

Taking risks seriously

Senior and middle management should include an agreed risk perspective, in line with the company's key risk appetite statements, in their decision-making processes, aiming to achieve long-term stability of the business and balancing short-term gains. A common phenomenon is management teams being composed of people with the same personal attitudes. While this may feel comforting for team members, it can lead to sub-optimal decision making, as certain aspects of risks can be neglected. Ideally, Management should aim to foster diversity of thought and solicit different views when taking risk. Diverse management teams, be that with regard to gender, education, nationality, age or "management drive", tend to perform better at managing risks than single-minded teams.

In addition, employees - especially those in management positions or key functions - must be adequately trained to perform their tasks ("Fit & Proper"). This covers both individuals (specialist in a field) and the collective task force (able to ask the right questions outside the specialist field).

Learning from mistakes

People make mistakes. Companies that encourage people to talk openly about them to ensure that they are not repeated, tend to have a better risk profile than companies that do not. This requires senior management to foster a culture of transparency in which early identification of risk issues is communicated in a timely manner to relevant parties. This is not an easy task, as it requires a balancing act between freedom to make mistakes without having to fear consequences and giving the impression that "making mistakes" is ok.

The importance of creating a learning environment within single organisations is one thing, but across the industry is another. Within organisations, a culture that encourages post mortem analysis of events and lessons learned is a good indication of a sound risk culture. Sharing useful information on events in an anonymous and structured way among companies (e.g. via the creation of a consortium) is another path to explore, which could contribute to improving the risk profile of the industry as a whole. The aviation and medical industries may serve as role models in this.

Comfort to talk openly: effective communication and challenge

Creating an open environment where different views are encouraged and effective challenge is part of decision making processes is indicative of a sound risk culture. Examples from the aviation industry illustrate that open escalation and reporting of issues are of paramount importance. The quality of communication is impacted by supporting systems and processes as well as human

factors such as an unwillingness to report issues, tolerance for deviation from policies and procedures, and acceptance of inadequate resources. Executives' response to bad news was also found to be a key cultural factor. Our survey participants were in agreement that an environment in which people feel comfortable to talk openly and challenge others, including their superiors, was very important to a sound risk culture.

> "… WHEN POTENTIALLY CONTROVERSIAL CHOICES ARISE, INDIVIDUALS ARE ENCOURAGED TO "ESCALATE, ESCALATE, ESCALATE"… THE FASTEST WAY TO LOSE A POSITION AT GOLDMAN IS NOT TO LOSE MONEY BUT TO MAKE A DECISION THAT ENDANGERS THE REPUTATION OF THE FIRM WITHOUT CONSULTING OTHERS." GOLDMANN SACHS[7]

Example: How can we assess the quality of Risk Culture - Implementing Risk Culture Dashboard

NN Group has developed a Risk Culture Dashboard that is built on four key components, and further divided into 10 sub-components, that reflect a sound risk culture, namely:

- Strategy
  - Management Behaviour: Commitment from all management to (promote) active risk management;
  - Employee Skillset & Engagement: Engaged and skilled employees in both first and second lines of defence;
  - Embedded Governance: Rules of the game are clear to everyone; and
  - ORSA: Aligning risk objectives with business objectives, risk profile and capital.
- Assess
  - Models: Measuring risks accurately so the business can be well understood;
  - Risk Assessments: Effective identification, communication and follow-up of all risks; and
  - Product Review: Ensuring professional risk assessment of all new products and investments.
- Control
  - Risk Mitigation: Implementation of appropriate risk mitigation for all assessed risks.
- Monitor
  - Risk reporting: Timely and reliable risk information for proper decision making; and
  - Risk committees: Well-functioning risk committees.

The Risk Culture Dashboard is used on a regular basis for business units (BUs) to assess their risk culture in a structured way. The Group CRO provides more detailed guidance on what should be in place and functioning to qualify for a "meets internal standards" score. For each of the items, local BU management teams indicate how they would rate themselves using a five-point scale: excellent, meets internal standards, meets regulatory standards, insufficient and weak. The score must be substantiated in a concise way. To avoid any negative incentives when performing the self-assessments, the overall rating is not part of local performance targets.

The CRO's rating of BUs, based on the overall score of the ten components and findings are communicated and discussed among Group CRO and local CEO and CRO. The aim is to identify

---

[7] McKinsey (2008), *Risk Revolution*

opportunities for improvement. In this dialogue, there is no room for "negotiating" ratings. Furthermore, the Management Board of the company discusses the overall results.

The Risk Culture Dashboard is not only proved to be a catalyst in improving risk culture, it also plays a pivotal role in conveying the concept of risk culture.

Driving cultural change

As pointed out by Strategy&, PwC and the Katzenbach Center in their joint work from 2014,[8] it is rarely necessary to overhaul the existing culture since it is rarely "all bad". So, what is the motivation behind changing a company's culture and what are effective approaches to implementing those changes?

In EY's survey among 52 companies from the financial services industry,[9] 73% of the participants named delivering consistency across organisational culture, employee behaviour, risk appetite and risk culture the main drivers behind their risk culture initiatives. When asked about challenges to strengthening their risk culture, more than half of the participants (56%) answered that achieving balance between front-office behaviour and risk culture is their top challenge. **Even though 86% of the companies confirmed that severe breaches of controls would result in disciplinary actions, only 30% believe it is fully understood that negative behaviour will be penalised despite earnings performance.**

> "FIXING THE CULTURE IS THE MOST CRITICAL – AND MOST DIFFICULT – PART OF A CORPORATE TRANSFORMATION", LOU GERSTNER, RETIRED CEO OF IBM

In their paper, Strategy&, PwC and the Katzenbach Center recommend to "focus on changing only the few critical behaviours at different levels with key populations". One approach that identifies and prioritises areas where changes and enhancements to behaviour are required builds on so-called "moments that matter". Moments that matter are behaviourally-oriented interactions that have disproportionally high effects on business performance and are specific for an individual company, e.g. interactions with customers during renewal periods, or claims handling. The size of the list can lie within the range of 50 to 600 items, depending on the level of granularity and the number of business units and functions involved.

Once the moments that matter have been identified, the target behaviours are specified in line with the risk vision to help guide people in their decision making.

Mechanisms to support the implementation of the target behaviours:

■ Breach management; and

■ Compensation (to what extent is good behaviour taken into account in determining compensation).

---

[8] Strategy&, PwC & Katzenbach Center (2014), *A Perspective on Organizational Culture*

[9] EY (2014), *Shifting focus: Risk culture at the forefront of banking*

3.3   How to convey the concept of risk culture?

Creating the right conditions for a sound risk culture is the first step to conveying the concept of a risk culture. All aforementioned formal and informal elements need to be in place at least in design. If the internal environment is not in line with the design, however, this suggests a change in the organisation needs to be performed. Communication, both verbal and non-verbal, is a crucial element in every change management program.

It is human nature to resist change, trying to hold on to the comfort of familiarity. Although change management literature is vast, the following three golden rules can summarise the most important aspects. These need to be followed until the change is embedded in the organisation.

Set the example

Management must "walk the talk": not only articulate but act in line with exemplary behaviour. People can be informed about the required changes through roadshows by senior management explaining why the change is necessary (incidents usually are a good catalyst), video messages and news items on the Intranet, as well as periodical generic emails, for example. However, for real and lasting change, those demanding change should demonstrate the desired behaviours and their strong commitment to it. They should also constructively deal with people who show dysfunctional behaviour and publically reward those that role model the desired mindset.

Take people along the change

Although incorporating desired behaviour into performance targets contributes to implementing the change, it is insufficient. People need to understand, believe and live the change. A compelling change story, in which people can identify with the end goal and see themselves playing a part in achieving it, is a good start. Another method to increase the chances of success are regular (in)formal coaching meetings during the year in which specific cases are discussed in the context of the desired change (what went well, what should be done differently going forward).

Help those undergoing the change answer the question "What's in it for me?"

People are generally inclined to stick to the status quo rather than actively contribute to the desired change. However, once people understand how they could gain from the change, they have an incentive to change their behaviour. Gains go beyond mere monetary rewards: smooth processes, compliments from colleagues and/or clients etc. also provide strong incentives for change. This will be enforced through positive peer pressure and role modelling when other people in their immediate environment start to adapt to the new desired situation.

As employees go collectively through the change process, an open atmosphere is a *condicio sine qua non*. Regular team meetings where progress, pockets of best practice and "mistakes" are discussed will contribute to realizing the change. Mistakes should be discussed anonymously with the aim of learning, colleagues' advice should be sought and the team should challenge each other in dilemmas. It is vital that team members raise topics themselves, facilitated by a team manager that has specific skills. "Success stories" should be shared regularly through e.g. the intranet or in team meetings.

Example: How can we support a risk-aware culture across all levels of the organisation - Awareness campaign

In 2011, the Zurich Insurance team in Australia developed the "We are all Risk Managers" program to foster a risk-aware culture across all levels of the organisation. The objective was to establish a common language and understanding of risk management. As one of the core elements of the initiative, the Risk team, with support of other functions, published posters illustrating the theme "We are all Risk Managers". The primary objective was to grab the attention of employees with posters that were fun and accessible. The results of this awareness campaign were remarkable with survey results showing significant improvement in understanding. Experience shows, however, that awareness campaigns as the above are developed with a particular business unit culture in mind and can only be transferred across business units upon consideration of differences in culture or context.

3.4 What can we learn from other industries?

The Insurance sector can learn lessons from many sectors including oil and gas, aviation and pharmaceuticals, where effective management of risk is needed. Safety is paramount, often due to the potential risk to life. These industries have experienced challenging periods due to several catastrophic incidents which have resulted in recognition that there are a number of factors that need to be strengthened to improve risk management. These include:

Encourage transparent communication

Overcoming barriers between captain, cockpit crew and air traffic controllers is one of the key elements to encourage transparent communication in the aviation industry. One of the most common reasons for miscommunication is hierarchy and people's attitude towards it. Subordinates, e.g. first officers, may not express concerns clearly enough or even at all as they fear upsetting their superiors.

To overcome this, pilots, captains in particular, are trained to neither use commands nor express their own assessment when analysing errors. They first collect the views of other crew members, allowing for impartial opinions and an active exchange of information.

---

[10] Financial Times (01/2014), *Managers learn to see the error of their ways*

Learn from mistakes

One of the elements that airlines have implemented to increase safety is non-punitive reporting.[11] Voluntary reporting systems encourage employees to report irregularities within a trustful and open frame, without having to be fearful of management or regulatory authorities. The purpose of obtaining and analysing information about errors, hazards and incidents (potential and actual) is to identify and be able to address root-causes so that mistakes can be avoided in the future. Both employees and management must be comfortable that the intention is not to blame individuals. The *quid pro quo* is that employees who made mistakes or misjudgements unintentionally and self-report will not be disciplined, though they may receive additional training. Where rules are broken deliberately, however, no allowances are made.[12]

Lessons in Failure from the Error Management[13]

- "Avoid one size fits all responses. While oversights and blunders are best eliminated, experimental failures that invalidate a theory or expose shortcomings move innovators closer to their goals and should be welcomed"

- "Differentiate between wilful and reckless misdemeanours and well-intentioned mistakes."

- "Avoid witch hunts. Searching for culprits makes people clam up, driving problems underground"

- "Question single-cause explanations: serious failures often have their roots in many smaller lapses that pile up."

- "Applaud messengers. When the messenger is shot, learning stops."

- "Encourage higher-ups to talk about their failures. Leaders who project an image of infallibility are less likely to be challenged and more likely to err."

- "Design pilots and prototypes to test boundaries – not to work perfectly."

---

[11] IFALPA (2009), *Improved accident prevention through non-punitive reporting*

[12] Financial Times (07/2014), *Lessons in Failure from the Error Management Gurus*

[13] Refer to footnote above.

4   Conclusion

A firm's risk culture significantly improves its capability to take strategic risk decisions and deliver business performance targets. Firms with inappropriate risk cultures will inadvertently find themselves allowing activities that are contrary to stated policies. An inappropriate risk culture not only means that individuals will undertake these activities but the remainder of the firm may ignore, condone or choose not to challenge such behaviour.

Risk culture is not always about taking too much risk. Certain firms are so good at developing and implementing formal processes and frameworks that they stifle the risk taking necessary for successful innovation. It is the willingness of individuals within the firm to balance risks and reward and make informed decisions within the context of the firm's stated risk policies that is an important characteristic in agile, commercially successful firms.

The importance of risk culture on the organisational agenda is driven by pressure on leadership to hold staff across the organisation accountable, higher consumer protection standards and negative public reputation associated with ongoing failures, fines and settlements. Increasing focus of supervisory authorities on risk culture is also a contributor. Risk culture is a continuous process, comprising of formal and informal processes and may be of a trans-organisational nature or constitute of several sub-cultures governed by a set of guiding principles.

Essential elements of a sound risk culture are identified as exemplary conduct by senior management, an environment open to discussion and a common understanding and awareness of risk, amongst others. Risk culture should permeate through all levels of the organisation. Catalogues of questions can be developed to aid in the assessment of the soundness of an organisation's risk culture. The main factors promoting and supporting a sound risk culture as discussed in this paper are:

- Strategy, policies and company values that are clear and clearly communicated;
- Risk Appetite statements;
- Clear organisational structure;
- Mastering conflicting interests;
- Taking risks seriously;
- Learning from mistakes; and
- Comfort to talk openly: effective communication and challenge.

Creating the right conditions for a sound risk culture is the first step in promoting the concept of a risk culture. Management must not only articulate what constitutes exemplary behaviour but must also set an example. People must understand, believe and live the change - the change story must be compelling. People also need to understand what personal gains are from going along with change.

Other industries offer lessons for the insurance sector on the need for effective risk management. These industries have gone through difficult periods which have highlighted the need to improve risk management. Lessons highlight the need for open and transparent communication.

Outlook into potential future developments related to risk culture:

- As proactive risk management attempts to take a forward-looking approach, a risk culture that supports innovation will be critical in an industry that is seen as relatively traditional and is currently suffering from a sustained low interest rate environment and the growing burden of insurance regulations.

- Establishing the use of predictive analytics, i.e. the analysis of data capturing individuals' decision making processes, in particular in context of risk breaches, to identify early warning indicators for failure to allow intervention and aversion of failures at an earlier stage.

5   References

British Financial Reporting Council (2014), *Guidance on Risk Management, Internal Control and related Financial and Business Reporting*

EY (2014), *Shifting focus: Risk culture at the forefront of banking*

Enterprise Risk Management Initiative (2010), *How did BP's risk management lead to failure?*, North Carolina State University

Financial Times (07/2014), *Lessons in Failure from the Error Management Gurus*

Financial Times (01/2014), *Managers learn to see the error of their ways*

FSB's consultative document (November 2013), *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture*

IFALPA (2009), *Improved accident prevention through non-punitive reporting*

North American CRO Council and CRO Forum (2014), *Survey on Risk Culture among members of the CRO Forum and the CRO Council*

McKinsey (2008), *Risk Revolution*

Power, Ashby & Palermo (2013), *Risk Culture in Financial Organizations*

Strategy&, PwC & Katzenbach Center (2014), *A Perspective on Organizational Culture*

Appendix: Survey results

Question 1: What are elements of a sound risk culture?

BOARD AND SENIOR MANAGEMENT LEADING BY EXAMPLE

PROMOTING COMFORT TO TALK OPENLY AND CHALLENGE OTHERS

ENSURING COMMON UNDERSTANDING AND AWARENESS OF RISK

ESTABLISHING CONSEQUENCES FOR EXCESSIVE RISK TAKING BEYOND THE DEFINED RISK APPETITE

ESTABLISHING INCENTIVES SUCH AS RISK-BASED REMUNERATION TO SUPPORT INFORMED RISK TAKING

- VERY IMPORTANT
- IMPORTANT
- SOMEWHAT IMPORTANT
- NOT AT ALL IMPORTANT

Question 2: Why does risk culture matter?

THERE IS A HIGH DEGREE OF PLURALITY WITH REGARD TO RISK CULTURE AND HENCE, THERE IS NO UNIQUE APPROACH TO MANAGE RISK CULTURE.

MULTI-NATIONAL ORGANIZATIONS FACE MORE CHALLENGES WHEN ESTABLISHING RISK CULTURE THAN FIRMS OPERATING IN ONE COUNTRY ONLY.

DUE TO THEIR BUSINESS, INSURANCE COMPANIES CANNOT DISTINGUISH BETWEEN CORPORATE CULTURE AND RISK CULTURE.

A FIRM'S RISK CULTURE IS CLOSELY LINKED TO THE CULTURE IN THE COUNTRY THE FIRM OPERATES IN.

HAVING A SHARED UNDERSTANDING OF THE FIRM'S RISK CULTURE, ITS PRINCIPLES AND LEADING PRACTICES HELPS ALL INDIVIDUALS TO IDENTIFY AND ADHERE TO THE RISK CULTURE.

FOSTERING A SOUND RISK CULTURE MAY LEAD TO EXCESSIVE DEGREES OF RISK AVERSION.

ESTABLISHING A CULTURE OF PRUDENT RISK TAKING IS AT ODDS WITH A FIRM'S BUSINESS.

HAVING A CLEAR DEFINITION OF THE FIRM'S RISK APPETITE IS SUFFICIENT TO DEFINE AND ADHERE TO THE RISK CULTURE.

- AGREE
- STRONGLY AGREE
- DISAGREE
- STRONGLY DISAGREE

Question 3: How can "good" risk cultures be maintained?

Categories (top to bottom):
- PROFITABILITY AND RISK CULTURE ARE CLOSELY LINKED IN THE LONG TERM
- "GOOD" RISK CULTURE SHOULD CONSIDER THE LONG-TERM (10-15 YEARS) EVOLUTION OF SOCIETAL STANDARDS
- DEGRADED RISK CULTURES ARE ROOTED IN INSUFFICIENT CONTROLLING AND A LACK OF ENFORCED ACCOUNTABILITY
- DEGRADING RISK CULTURES CAN BE AVOIDED BY PUTTING AN EFFECTIVE SET OF INCENTIVES SUCH AS REMUNERATION IN PLACE
- PROFITABILITY AND RISK CULTURE ARE CLOSELY LINKED IN THE SHORT TERM
- THE PUBLIC PERCEPTION OF FIRMS' RISK CULTURE BEING BAD STEMS FROM SOCIETY AND BUSINESSES HAVING DIFFERENT RISK APPETITES
- AS LONG AS ALL INDIVIDUALS IN THE FIRM BEHAVE ACCORDING TO THE LETTER OF LAW, "GOOD" RISK CULTURE CAN BE PRESERVED
- THERE IS NO NEED FOR INDIVIDUALS IN A FIRM TO CHALLENGE THE RULES SET FOR RISK CULTURE

Legend: ■ AGREE ■ STRONGLY AGREE ■ DISAGREE ■ STRONGLY DISAGREE

Question 4: Can and should risk culture be externally regulated?

Categories (top to bottom):
- OVER-ENGINEERED REGULATORY INITIATIVES TO ASSES RISK CULTURE CAN HAVE DESTRUCTIVE CONSEQUENCES
- SUPERVISORS' DEMAND FOR DOCUMENTATION RAISES THE PRESSURE ON ORGANIZATIONS, EVEN IF THEY FEEL COMFORTABLE ABOUT THEIR RISK CULTURE
- ESTABLISHING A REGULATORY FRAMEWORK AROUND RISK CULTURE MAY DEPRECIATE ALTERNATIVE PERSPECTIVES AND APPROACHES THAT FOSTER RISK CULTURE
- REGULATORS HAVE THE EXPERIENCE AND EXPERTISE TO IDENTIFY PRACTICES, BEHAVIOR AND ATTITUDES THAT COULD UNDERMINE THE RISK CULTURE
- REGULATORS SHOULD CONSTANTLY ASSES RISK CULTURE INDICATORS AND COMMUNICATE THEIR FINDINGS TO THE BOARD AND SENIOR MANAGEMENT
- COMPREHENSIVE DOCUMENTATION OF THE FIRM'S RISK CULTURE IS TO BE PROVIDED TO THE REGULATORS

Legend: ■ AGREE ■ STRONGLY AGREE ■ DISAGREE ■ STRONGLY DISAGREE

Disclaimer:

Dutch law is applicable to the use of this publication. Any dispute arising out of such use will be brought before the court of Amsterdam, the Netherlands. The material and conclusions contained in this publication are for information purposes only and the editor and author(s) offer(s) no guarantee for the accuracy and completeness of its contents. All liability for the accuracy and completeness or for any damages resulting from the use of the information herein is expressly excluded. Under no circumstances shall the CRO Forum or any of its member organisations be liable for any financial or consequential loss relating to this publication. The contents of this publication are protected by copyright law. The further publication of such contents is only allowed after prior written approval of CRO Forum.

© 2015
CRO Forum

The CRO Forum is supported by a Secretariat that is run by
KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org