Financial Services Forum

Scoring Goals in a Changing World

5-6 May 2014
Hilton Sydney

Risk Culture Leadership, Measurement & Management – A Comparison across Industries

Prepared by Sean McGing and Andrew Brown

Presented to the Actuaries Institute
Financial Service Forum
5– 6 May 2014
Sydney

Institute of Actuaries of Australia
ABN 69 000 423 656
Level 2, 50 Carrington Street, Sydney NSW 2000, Australia
t +61 (0)2 9233 3466 **f** +61 (0)2 9233 3446
e actuaries@actuaries.asn.au **w** www.actuaries.asn.au

Synopsis

The paper compares where organisations are on their journey in implementing enterprise risk management (ERM) and the extent to which, and how, organisations identify, measure and seek to improve their risk cultures. We do this for three contrasting industries - financial services, energy and education. Within financial services we consider variations between banking, life insurance, general insurance and superannuation.

An organisation's culture is complex and varies with a wide range of attributes and environment. How it instills its risk appetite and related actions in its people and translates risk and opportunity into improved outcomes will vary across industries. So too will the optimal risk management framework with its policies, systems, processes, controls and procedures.

As a basis for the comparison we picked a sample of companies and identified their ERM frameworks and processes. We considered how the risk culture of the organisation affects their risk management. In particular the roles of the first two of the typical "three lines of defence" - (1) risks being managed by the people responsible for making decisions in the business and (2) the support and enterprise wide view from the risk function headed by the Chief Risk Officer (CRO), line (3) being independent audit. We examined how an organisation's risk culture and it's interaction with the ERM framework affected risk ownership, taking responsibility for risks and being accountable for outcomes.

A key element of our assessment was our design of a risk culture questionnaire which was completed by the organisations' CROs or equivalent. We complement this with interviews of the CROs.

We present our findings including comparisons of risk practices and maturity levels and what each of the disparate organisations might learn from each other. We make recommendations on how to measure and manage risk culture. We reflect on the desirable attributes of a good CRO.

We explore the key insights and reflections from the CROs in relation to the major challenges they are grappling with in relation to risk culture. These include how to identify the steps along a culture journey, the value or otherwise of investing in deep cultural change, how much resourcing of a risk team is enough, and the role of senior leadership (tone from the top) and middle management (the tune from the middle).

Keywords: Leadership, risk, opportunity, enterprise risk management, risk culture, mature risk culture, risk questionnaire, financial services, banking, insurance, superannuation, education, energy.

Table of contents

1 Risk culture in organisations

*"I came to see, in my time at IBM, that culture isn't just one aspect of the game, it **is** the game."*[1]

Lou Gerstner, former CEO IBM/Nabisco

1.1 Introduction

Lou Gerstner's opening quote, was a reflection of his years of experience in turning around the dinosaur that was IBM, and were prefaced by: "*Until I came to IBM, I probably would have told you that culture was just one among several important elements in any organization's makeup and success—along with vision, strategy, marketing, financials, and the like*". We often hear this from Board directors and the C Suite when we attest to the critical importance of culture to reducing risks and improving performance by seeing and making the most of opportunities.

Lou's final words highlight the need to take risks to survive or thrive: *"In the end, an organization is nothing more than the collective capacity of its people to create value. If you don't take risks and don't push innovation you will get left behind very quickly."*

1.2 Purpose of Paper

The objectives of the paper are:

1. To explore how an organisation's risk culture can be measured.

2. To compare and contrast how influences on risk culture differ across organisations in a range of industries.

3. To identify what is important to Chief Risk Officers to achieve effective enterprise risk management.

1.3 Definitions - Risk to mature risk culture

1.3.1 Risk, Risk management, Enterprise risk management

We refer the reader to our previous paper - *Board leadership in a complex world - optimising value from risk and opportunity* (2013)[2] where we defined these key terms.

1.3.2 Culture, Risk culture, Mature risk culture

In the same paper, we defined culture using the three levels of culture in an organisation - artefacts, espoused values and tacit assumptions - as identified by Ed Schein[3] [4] [5] global expert on organisational cultures.

An organisation's risk culture describes the degree to which its culture encourages or limits the taking of risks and the opportunities that arise from those risks.

In a mature risk culture, risk is part and parcel of every conversation and decision at all levels. In a mature risk culture, processes and the organisation's mindset drive the management of immediate risk, the understanding of new and emerging risks, and an ongoing exploration that increases the resilience and adaptive capacity of the organisation to future (unknown) risks.

1.4 Risk Culture Rubric - Evolving levels of maturity

Table 1.1, taken from our 2013 paper, sets out how the different elements of risk culture evolve from simply operating subconsciously to the ideal of a mature risk culture.

Table 1.1 Risk Culture Rubric

Maturity level → *Item*	*Unaware*	*Reactive*	*Mechanical*	*Pro-active*	*Mature risk culture*
Beliefs / mindsets	Risk management is just a concept	Risk management received with cynicism, a management whim	Importance of risk management accepted	Actively aware of and owns risk as part of work	Risk = opportunity
Organisat-ional attitudes	Individuals blamed when risks eventuate	Must eliminate losses; very top down approach	Workforce more involved but with limited understanding	Workforce involvement promoted, though team leaders still organise / take responsibility	Partnership between management and workforce; shared responsibility
Individual behaviours	Takes many risks without realising it, blissful ignorance	Meets minimal legal or compliance requirements; Ignores until reporting time	Day to day risks are managed effectively	Regular discussions on risks, active prioritising to manage risks	Workforce drives risk assessment, shares insights across business
Systems / structures	None, no communic-ation or training	Compliance reports, detailed reviews of failures	Performance management systems. Risk dashboards	Active feedback loops, actions beyond reporting	Culture reviews. Employee perception surveys. Behaviour based training
Risk function	None	Compliance function. Influences through authority.	Function accepted, carries out organisation reviews, focus on improving procedures	Partnership with management, compliance at business line, influences via relationships.	Risk function co-operative and supportive as managers and teams take responsibility. Forward looking.

Source: A. Brown and material provided by S. Bennett (Enhance Solutions). This is adapted from a method by Patrick Hudson[6] applied to safety cultures.

1.5 Key research underpinning Organisational Culture & Maturity

The risk culture evolution rubric has theoretical underpinnings – these are important in not only understanding its origins but also in considering what to measure.

1.5.1 Schein's top seven influences on culture

In his research on what really influences culture, Schein identified the following as the seven most important factors (in order of importance):

1. What a leader attends to, measures, rewards and controls
2. How leaders react to critical incidents
3. Leader role modeling
4. Criteria for recruitment, promotion and retirement
5. Formal and informal socialising
6. Recurring systems and procedures
7. Organisational structure and hierarchy

1.5.2 Wilber's Integral model

Ken Wilber, integral philosopher, has summarised four aspects of a system into his integral model.

Table 1.2 Wilber's Integral Model [7]

	Internal	**External**
Individual	INTENTIONAL Personal meaning and inner skills	BEHAVIOURAL Individual behaviour and outer skills
Collective	CULTURAL Culture and shared meaning	SYSTEMS Systems and procedures

Using business risk as our focus, the upper-right quadrant represents individual behaviours and actions that lead to the risks and opportunities within a firm; the Lower-Right quadrant represents the systems that produce those risks and opportunities; the Lower-Left quadrant represents the values and shared beliefs of a firm; the Upper-Left quadrant represents the interior dimensions of the individuals in the firm (e.g., their intellect, emotional intelligence, ethics, motivation, etc.)

1.5.3 Barrett's hierarchy of organsations and Maslow's hierarchy of needs

Maslow's seminal hierarchy of needs model [8] [9] provided a way to understand how human needs evolve over our lifetime, and how under certain circumstances we may revert to earlier needs. See figure 1.1.

Figure 1.1

Maslow's hierarchy of needs pyramid

Many theorists, including Richard Barrett, have hypothesised that organisational maturity follows a similar hierarchy. See Barrett's comparison to Maslow at slideshare.net[10]

1.5.4 Applying the research to today's entities

The importance of culture change is to better achieve the organisational goals which in our study is reduced risk through better enterprise risk management including better identification and use of opportunities to attain those goals.

The culture of an organisation is heavily influenced by its individual and collective behaviours. To move an organisation to a more mature risk culture requires an understanding of its people's behaviour(s), beliefs and mindsets. To support and reinforce any cultural change, it is also essential to have in place appropriate systems and structures.

To identify most appropriate actions, requires understanding the current risk culture and developing initiatives that will help the organisation in the transition towards the next stage. Section 2 explores measuring the risk culture.

2 Measuring risk culture

"Everything that can be counted does not necessarily count, everything that counts cannot necessarily be counted"

Albert Einstein

2.1 Why measure?

If culture is important to ERM, then we have to find a way to measure it. The case for measuring culture seems very straight forward – by measuring culture we are better able to assess the effectiveness of our attempts to shape or control it. In financial services APRA as the regulator effectively expects you to measure it to manage it. However, there are a number of pitfalls and considerations to be aware of. This is due to the qualitative and subjective nature of culture. We now explore some options and challenges in measurement.

Firstly, we need to be careful that any changes in results are due to changes in the underlying culture and not changes in how the measurement is being applied. Our experience has been that the results of measuring culture often lead to a change in the measurement results from the first to the second time it is measured. However, when we have explored why this occurs, survey correspondents have shared that they now have a better understanding of what they are being asked. Hence the survey result has changed due to participant understanding leading to bias, rather than changes in culture itself.

Secondly, the harder that things are to measure, or the more subjective they are, the more likely it is for people to ignore or discount the results. It would come as no surprise that the poorer the results, the more they are often discounted or rejected.

Thirdly, measurement of the culture isn't independent of the culture. If the survey is not cultural neutral, and implies what is important or what is not important, this may contribute to shaping the culture. This can also potentially bias the measurement.

Finally, The type of measurement that is appropriate will also depend on the stage of organisational maturity. For earlier stages, there may need to be more detailed measuring with specific risk culture surveys. As the risk culture matures and becomes part of the DNA of the business, measurement may be better integrated into broader organisational culture or engagement surveys.

Balancing these points, we believe that it is important to measure risk culture. We also believe that to overcome some of these limitations and challenges, that any surveys must be supplemented with interviews and/or group discussions to appropriately understand the context in which the responses have been supplied.

2.2 Developing a measure for risk culture

The Centre for Creative Leadership (CCL) have identified key drivers of organisational culture, called the Leadership Culture Indicators tool which is described in detail at their web site[11].

While these indicators are broadly aligned to Ed Schein's seven key drivers (in section 1.5.1, they provide a more granular level of detail and hence are a suitable starting point for developing a series of questions to measure risk culture.

We have reviewed the CCL questions, and have adapted these to apply specifically to risk. We have also supplemented these with additional questions relevant for risk. Table 2.1 presents those questions as a starting point for consideration.

Table 2.1 Drivers of organisational culture

Driver	*Question*
Strategy	In the face of the strategy, how clear are the risks and risk appetite?
Fear	What is it not safe to raise in my organisation?
Remuneration	Am I rewarded for taking appropriate risks?
Information	Do I have the information to adequately assess risk?
Knowledge	Even if I have the information, do I have the knowledge to be able to effectively manage risk?
Alignment	Are we aligned on which risks are acceptable, and which ones aren't?
Conflict	If we avoid constructive conflict, will there be important risk considerations that don't see the light of day (until it is too late)
Mistakes	How are mistakes treated in the culture? Learning or shameful?
Feedback	How are people provided feedback in order to autocorrect? How do people get (systems) feedback when they put in place an initiative? What are the red flag mechanisms that provide feedback on the health of the system?
Time scale	What is the time orientation of senior executives / board members?
Integrity	Do I trust people in my organisation to do the right thing?
Distributed nature of leadership	Am I encouraged to take responsibility for managing the risks that occur as a result of the business decisions I make?
Role modelling	Do senior people in my organisation do what they ask of others?
Collaboration	How well do people work together across teams AND across functions AND up and down the hierarchies?

2.3 Methods to Measure risk culture

As Schein clearly identified what you see is not always what you get. Any methods used need to be carefully designed to eliminate bias and misinformation. The interpretation of information received needs to be carefully considered, guided by previous experience.

It is particularly important to be consistent over time in what is measured and how is it so that trends can be identified. The changes over time are usually more important than any absolute value of measurement. The latter is important for benchmarking the entity against its own industry and other industries. Annual assessments are recommended for continuity and to enable actions to be taken promptly.

The following are some methods to consider:

Questionnaire/survey

The first and core tool to measure the culture and by extension the risk culture of an organisation is a well-designed questionnaire which probes people's attitude to risk in their role and their perception of their team's, their manager's, senior management's and the board's attitude to, and level of importance attached to, risk management.

Interviews within the organisation

The next is supplementing these questionnaires by interviewing selected individuals within the organisation. This enables both validating the results of the questionnaire and digging deeper on conflicting information received and potential issues.

Group discussions

Group discussion sessions within an entity based on specific questions around people's experiences, can reveal stories of events that offer a real insight into the entity's culture and how it has or hasn't changed over time. Having a number of people in a group can provide multiple perspectives and hence an opportunity to build off each others' insights. Where there are differing opinions or perspectives, a group discussion can also help to more deeply understand why the differences exist and help to build a more coherent narrative.

Interviews outside the organisation

A further step is to interview people outside the organisation, particularly stakeholders including suppliers, clients and customers. Others with no vested interest in the organisation but see the organisation operate within their industry can be forthright in their views.

Social media analysis

Social media such as Twitter feeds and Facebook commentary can be used to identify potentially recent issues. How they are dealt with by the company can give a real insight into its culture.

The extent of measurement and the use of the above methods will vary with time, budget, ease of access to information, and the degree of confidentiality the organisation wishes to retain.

Self assessment vs other internal assessment versus external assessment

Self-assessment is an important first step on the journey to improvement. It increases the level of self awareness and communicates the expectations of the organisation implicitly or explicitly. It is a key component of any performance review system from staff to Board members. From a risk perspective it is easily tailored to address risk recognition and best practice actions at the individual level.

Other internal assessments range from the Human Resources department's organisation of, and interaction with, peers, managers or a 360° review of the past years actions to the risk function's activities related to risk management through to internal audit's findings on the projects it has carried out during the year.

Assessing externally is usually the most revealing. An independent external review should be the least prone to bias and conflict of interest and can compare to industry common and best practice. But it is the most expensive. Determining the extent of bias - conscious and subconscious - in each of the three components is important. It is important to get an external perspective for debate every few years to reduce the risk from unforeseen internal and external events.

Measuring the operational environment

Evidence of risky behaviour can be gleaned from the standard of upkeep of risk registers / databases and breach registers including the extent and timing of follow-ups and actions ultimately taken or not. These may differ by department.

Extent and attitudes to training

The content of the training, attitudes of staff toward training in ERM, the compulsory or voluntary nature of training and rates of attendance are all important signals of risk culture. Whether the training is separate or integrated into broader organisational training programmes is also an indicator. Lastly, where the training focuses (for risk management - obligations to comply, awareness of risk or responsibility and ownership) is also an indicator.

2.4 Risk culture variation by industry & nature of business

Each industry, organisation and department exists in different contexts and attracts people with different motivations, skills and orientations. This will mean that the types of risk that emerge and how these are managed may vary significantly.

What is important in measuring culture is to consider both the "global" attributes and the "local" attributes of risk cultures. Global attributes are consistently important attributes across industries, companies and departments. Local attributes are attributes that are materially different across industries, companies and departments.

The following table summarises key variations to consider:

Table 2.2 Risk culture variations

Type of variation	*Important distinctions*
Geographical location	Cultural expectations
Industry	Types of risk (e.g. operational vs financial), rate and type of change / disruption
Department	Emphasis on production vs protection
Nature / purpose of organisation	Profit motive vs risk protection motive
Risk history of organisation / industry	Experience of risk consequences
Scale of organisation	Complexity of culture change
Legacy business of organisation	Growth vs run-off risk profiles
Areas of focus within risk management	Strengths / weaknesses
Regulatory environment	Dominant to incidental

2.5 Evolution to a mature risk culture and its measurement

The Risk Culture Rubric (Table 1 in Section 1) provides an easily understood and easily communicated picture of where the organisation stands and where it is moving.

The key is to use this pathway as a guide to getting the organisation to the risk maturity level its board aspires to, so that it can reap the benefits of better ERM and performance.

Improvements can be measured and areas for improvement prioritised and tackled in a way that provides the most benefit for the least cost in time and resources. There are costs of measuring risk culture and acting on the results to increase maturity. These need to be balanced against the related benefits.

3 A comparison across industries

"What marks out a good board is its activism in embedding a strong risk culture throughout the institution. Behaviours, not structure."[12]

Dr John Laker, Chairman APRA

3.1 Organisation and human complexity

There are many material distinctions to consider in managing risk culture. While industry is not the only one, it is one of, if not the most important one. While our comparison is primarily focussed on industry differences in risk, and the management of risk, every organisation is unique. Hence the industry comparison also serves to highlight other important risk culture distinctions.

3.2 Key risks and risk categories by industry

We have used high level risk categories in our comparison. In practice each industry has their most important risk categories further subdivided. Risk categories also overlap and it is the aggregate risk from whatever categories they might be allocated to that matters. Table 3.1 shows an indicative relative importance of the major risk categories in the different industries based on our research. We have used a scale of 1 being the most important to 6 being the least important.

Table 3.1 Risk category relative importance by industry

Industry → *Risk Category*	*Financial Services*	*Energy*	*Education*
Health & Safety	5	1	1
Strategic	1	2	5
Financial	2	3	4
Operational	4	4	6
Reputation	3	5	3
Learning outcomes	n/a	n/a	2

For most commercial / for profit enterprises getting the strategy wrong is the biggest risk to long term survival. For a financial services company, financial risks are naturally particularly important - they are the core business so rightly get most of the attention. For a bank, credit risk is paramount, for an insurance company it's the insurance risk - underwriting, pricing, reserving etc. For a school, having a safe environment for students and staff is the fundamental pre-requisite.

We have not explicitly included regulatory risks in Table 3.1 as they tend to be beyond the control of the organisation so the controls that can be put in place to mitigate them are limited. They affect all players in the industry but can change the balance markedly between players. For example the changes in carbon policy of the last several years within and between governments.

3.3 Relative state of ERM maturity

Banking is arguably the industry with the most developed ERM frameworks globally and in Australia. Formal enterprise risk management as a management function first

developed in the 1990s[13]. Financial risk management at investment banks widened to embrace wider enterprise risk management and the term Chief Risk Officer was coined. With the Australian financial sector - especially the big four banks - dominating the ASX listed sector of the economy, the banks have led the way in setting risk appetite and addressing operational risks as well as credit risk. The effective use of capital from optimising risk adjusted return has been a key driver of ERM in financial services and monitoring risk capital is core to financial services supervision in banking and insurance.

A key element of operational risk as defined by the Bank of International Settlements (BIS) for Basle II and III capital requirements is people risk. Reducing "people risk" within operational risk or more widely improving the performance of most industries' greatest asset (people) means positively influencing people's behaviours.

The insurance industry is arguably the next most developed based on its traditional depth of analysis around its major risk – insurance including underwriting, pricing, claims management, reserving and investment risks. Defined contribution superannuation is a late starter but defined benefit superannuation / pensions have had well developed risk practices around longevity and investment risk.

Energy provides a contrast. Risks vary markedly across energy producers, distributors and retailers. An historical focus almost exclusively on health and safety and the rapid and major changes in Australian and global energy markets have led to ERM getting attention in recent years.

Education possibly has the least developed enterprise risk management but as with each of the other industries there are important exceptions such as the major universities.

This was reflected in the results of our interviews where we specifically asked each CRO where they positioned their organisation on the Risk Culture evolution Rubric. Most CROs scored their organisation as one of:

Between Reactive and Mechanical;
Mechanical; or
Between Mechanical and Pro-active

across each of the five Items being measured.

Within the five Items being measured Systems / Structure was least mature and Risk Function was most mature but in aggregate the differences in levels of maturity were limited.

By sector, Banking was most mature followed by Life Insurance, General Insurance and Energy at a similar level to each other, with Superannuation lagging behind. Education scored high for the Tertiary sector and low for the Secondary sector.

3.4 Comparison of regulatory environments

3.4.1 Different industry regulatory emphasis

In financial services, the primary focus of regulation is on the financial aspects. In Energy and Education a substantial focus of regulation is on health & safety.

Table 3.2 Regulatory environment by industry

Industry	*Area regulated*	*Main regulators*	*Main risks regulated*
Financial Services	Prudential supervision / capital strength	APRA	Customer losses, Provider failure
	Consumer protection	ASIC	Consumers misled / losses
Energy	Energy markets & networks	AER	Rules, markets, pricing
	Health & safety	State based OH&S Acts & related oversight bodies	Employee & public safety
	Consumer protection	ACCC	Competition
Education	Learning standards, licensing	State based Dept. of Education	Access to and quality of learning
	Health & safety	State based OH&S Acts & related oversight bodies	Student and staff safety

Note: Energy and education in particular have a wide range of federal and mostly state based legislation, of which the table reflects just 2 or 3 of the most important elements. This leads to extensive compliance actions and reporting.

3.4.2 Risks - compliance vs opportunity

One of the greatest similarities and shared frustration of all three industries considered is ever increasing volumes of regulations, actively monitored via policies, processes and procedures.

From a risk culture perspective, a "compliance culture" – a tick the box mentality - is dangerous for a business. It limits innovation and lulls staff and management into a false sense of security because it distracts from the bigger picture, leading to long term viability risks such as poor strategies and lack of innovation. To have an innovative culture which reduces the risk of becoming irrelevant or "out competed" requires the organisation to pay due recognition to compliance within a strong governance framework while increasing the focus on positive actions to make and take opportunities for expansion or better performance.

3.5 Comparison of ERM and risk culture maturity

3.5.1 ERM standard and methodologies

Companies listed on the ASX are expected to operate in accordance with the ASX Corporate Governance Principles[14] and if not to report why not. Principle 7

Recognise and manage risk says "A listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework." Non listed entities, when looking for an enterprise risk management benchmark often use this Principle 7 as a sound starting point. The Energy industry has substantial global links and this brings overseas risk management practice and expectation levels which vary by company.

The ISO 31000 methodology is the most common core enterprise risk management framework across industries in Australia and is also used extensively overseas.

3.5.2 Comparison tables

The tables following indicate the broad level of ERM maturity and risk culture maturity we believe exists across each sector. We stress there is significant variation between organisations within an industry, and that this is particularly sensitive to:

- The nature of its particular business within its industry including its target market / area of operation - reflecting the major risks - traditionally driven by the single biggest risk - and its potential impact (see Table 3.1 above).

- Organisation size. The smaller the organisation the less need for formal risk functions but also the less resources.

- The organisation's attitude to the balance of benefits vs costs of enterprise risk management.

Table 3.3 Indicative ERM & Risk Culture maturity - Financial Services

Industry variation Feature	*Banking*	*Life Insurance*	*General Insurance*	*Super-annuation*
Regulator(s) & ERM requirements	APRA CPS220	APRA CPS220	APRA CPS220	APRA SPS220
Common ERM methodology(ies)	Internal refined over years	Internal refined over years	Internal refined over years	ISO 31000 or other refined
Risk function	Yes	Yes	Yes	Yes
Chief Risk Officer	Yes	Yes	Yes	No but have risk manager
Important to Board	Yes	Yes	Yes	Yes
Risk Appetite Statement	Yes	Yes	Yes	Yes
Risk Management Plan	Yes	Yes	Yes	Yes
Level of risk culture maturity	Proactive	Mechanical to Proactive	Mechanical to Proactive	Reactive to Mechanical

Table 3.4 Indicative ERM & Risk Culture maturity - Energy

Industry variation Feature	*Combinations of Generation, Distribution and Retail*
Regulator(s) & ERM requirements	AER, State Govts
Common ERM methodology(ies)	ISO 31000
Risk function	Yes - small
Chief Risk Officer	Some
Importance to Board	Yes
Risk Appetite Statement	Not common
Risk Management Plan	Yes
Level of risk culture maturity	Mechanical

The Energy industry has high levels of vertical and horizontal integration - a single entity may own Generation facilities, Distribution Networks (the poles and wires) and Retailers across more than one State. So at a group level there is a mix of very different organisations with different risks.

Table 3.5 Indicative ERM & Risk Culture maturity - Education

Industry variation Feature	*Primary schools*	*Secondary schools*	*Tertiary (Universities, TAFE)*
Size	Small	Medium	Large to very large
Regulator(s) & ERM requirements	State Dept of Education;	State Dept of Education; Church bodies	Mostly State Based - Some own ACT
Common ERM methodology(ies)	None formal	Limited formality, ISO 31000	ISO 31000 and/or customised
Risk function	No	Some - limited	Many
Chief Risk Officer	No	No but some with Risk Manager	No but many with a Risk Manager
Importance to Board	No	Low / medium	High
Risk Appetite Statement	No	A few	Some
Risk Management Plan	Limited	Some	Most
Level of risk culture maturity	Reactive	Reactive to Mechanical	Mechanical

3.6 Instilling risk appetite and related actions

An organisation's culture is complex and varies with a wide range of attributes beyond its industry including size, geographic location, commercial environment, current issues, its values and strategic goals. From an ERM perspective, how it determines - whether implicitly or explicitly - and how well it communicates its appetite for risk is critical. How it instills that risk appetite and related actions in its people will vary across industries. So too will the optimal risk management framework with its policies, systems, processes, controls and procedures.

4 Findings and insights into risk culture across industries

"…development of a 'risk culture' throughout the firm is perhaps the most fundamental tool for effective risk management."

(Institute of International Finance (IIF), 2008)

4.1 Our risk culture measurement process

For this paper, we undertook a pilot risk culture measurement exercise, from the range of possible elements discussed in section 2. We:

- Conducted a desktop review of contemporary papers on risk culture
- Conducted (mostly) face to face interviews with people in our selected organisations with senior management responsibility for Risk - these were primarily the Chief Risk Officers (CROs)
- Analysed and compared the online questionnaire responses by our interviewees.

The initial intention of this paper was to assess if measuring risk culture can add value to an organisation, and how important risk culture is to effective ERM. However during the interview process, we identified significant sources of wisdom from the CROs. The CRO sits at the centre of the organisational maelstrom, observing the organisation grappling with both its operational and strategic challenges, and the boundaries that connect the two. Their sense of both the vertical and horizontal effects of a particular policy, decision or action was typically highly astute and brought a unique perspective into the direction that ERM is going, and contemporary challenges. We have also documented those insights in the following sections.

4.2 Strengths, weaknesses and priorities for ERM

4.2.1 Questionnaire - Analysis of answers to multiple choice questions

The Appendix describes the nature of the questions included in our questionnaire to the CROs. Notwithstanding the limited number of questionnaires and bearing in mind that the questions are addressed to the CRO rather than staff of different levels of seniority and function in an organisation, we identified the following themes:

1. The risk function does not focus enough on maximising opportunities. Similarly the risk function focuses too much on compliance.
2. There is not enough partnering with supporting business units to manage their own risks.
3. In financial services, risk appetite is reasonably well communicated and organisations take risk consistent with that, but risk appetite is not as clear as

the vision for the organisation, and does not flow through to actions sufficiently.

4. Most organisations are too "siloed". This contributes to different levels of risk culture maturity within organisations.

5. Organisations, partly through time constraints, are not tuned in sufficiently to emerging risk.

4.2.2 Questionnaire - Analysis of answers to "Top 3" questions

The final three questions asked were freeform, requesting views of participants on the top three aspects of importance an effective risk culture, and the top three strengths and weaknesses of their organisation's risk management. We have extracted the overall top three from the total set of responses as follows:

Q1 What do you believe are 3 of the most important aspects of an effective risk culture?

Answers

1. Tone from the top.
2. Open and effective communication in a safe environment.
3. Awareness, understanding and ownership of risk at all levels.

Q2 What do you see as your organisation's 3 greatest strengths in risk management?

Answers

1. Total demonstrated support from CEO and executive leadership team.
2. Interactive risk management support at the ground level and upwards.
3. Appropriate risk governance with full support from the leadership team.

Q3 What do you see as your organisation's 3 greatest weaknesses in risk management?

Answers

1. Lack of capacity for organisation to deal with unrelenting regulatory change.
2. Silos across the business.
3. Time and competing priorities in a changing environment.

4.3 Who has the biggest influence on risk management? Who should?

In considering the major influences on risk culture across industries we were struck by the extent to which regulations and the regulators seemed to dominate what risks and risk management the organisation focused on most. This raised the question of whether in a mature risk culture this would or should be the case?

Based on our research we have formed a working hypothesis on who we perceive has the most influence on risk management in financial services organisations, remembering that this averages over a wide range of organisations with different levels of influencers. See Table 4.1 for our assessment.

Table 4.1 Biggest influences on ERM in Financial Services

Influencer	*Current Ranking*	*Comment (Current)*	*Mature Ranking*	*Comment (Mature)*
Regulator	1	Keep raising the bar. New requirements. Targeting Boards.	6	With a truly mature risk culture businesses would be continuously identifying, mitigating and profiting from risk. This surpasses the regulator (minimum) required levels of risk management so would be monitoring rather than intervening and requiring further actions or reporting.
Board	3	Considerable reliance on executive for interpretation of response to regulators.	1	The board sets the risk appetite which sets expectations and boundaries for risk and opportunity.
Executive leadership	2	Treats new regulatory requirements as very high priority.	4	Understands, trusts and communicates effectively with CRO and ERM framework.
CRO	4	Still on the journey to gaining the full support and trust of executive leadership and board.	2	Risk frameworks incl. support and monitoring in place. Strong influence and trust with executive leadership and Board.
Managers	5	Risk priorities not sufficiently integrated.	5	Assess and support staff on agreed KPIs and KRIs.
Staff	6	Risk and opportunity not sufficiently a core part of day to day expectations.	3	Risk and opportunity owned and well handled at the frontline in accordance with risk appetite.

We would expect a mature risk culture to lead to a flattening of the vertical gap between influencers over time as all in the organisation understand and deliver on their risk related responsibilities in a positive supportive team environment with easy, quick and strong communication across functions and management levels.

4.4 Key themes and insights

1. The driving force behind best practice risk management across an enterprise is the evolving culture

CROs consistently identified the culture of the organisation as the number one factor in risk management. Each risk management initiative therefore must align to the current culture and at the same time be shaping the culture towards its next step on a maturity pathway. All see the Rubric as a useful tool to assist in identifying where

the organisation currently is, and the road it has to travel to get to its preferred risk maturity position.

Considerations include:

- *Measurement* – ensure that how you measure culture is aligned to current culture. It may be appropriate to initially run a broad survey to understand first, second and third line perspectives, and then integrate key questions into other organisational surveys. These would include culture or engagement surveys.

- *Responsibility and risk ownership* – there is a marked progression towards risk ownership at the first line, as close as possible to the person taking the risk. Over this journey, there may be a pendulum which swings between the two extremes of all or no ownership, but each time with a greater level of awareness of risk.

- *Social sophistication* - increasingly mature risk cultures require increasing social sophistication in the organisation, i.e. working with the complexity that occurs in social systems to leverage diversity rather than be floored by it. Risk and Human Resources functions both have a role to play.

- *Recruitment and departure* – the system and its culture will change as people come and go. It is essential that this is managed towards coherence with risk goals and aspirations. This should go beyond an induction process to also ensure there are risk KPIs for new staff, and new staff are recruited for fit to the desired risk culture.

2. If we heed the lessons, history is a wonderful teacher

- Maturity is greatest in industries where the most obvious and biggest financial risks arise. E.g. banks - credit risk, operational risk in trading; insurers - insurance risk (underwriting, pricing, reserving).

- There are good lessons to be learnt on the importance of having a sound risk culture from financial services history including the learnings and actions of APRA, the Australian financial services regulator, from the lessons of the collapse of HIH.

- The literature on organisational crisis suggests that what matters is the respect built through interaction between individuals.

- The learnings from the GFC in that many regulators have moved their focus from risk management to risk oversight both as a responsibility of the Board and of central risk management functions. This is shifting risk taking to being primarily the job of the first line of defence.

3. In risk management of an enterprise, there are more similarities than differences across different industries

- The same risk culture measurement framework (methodologies, techniques and tools) can be effectively used across all industries. However at the same time its application needs to take careful account of the different relative importance of each risk category, and the extent to which the different nature and scale of the organisation influence the type of risks and the relative importance within that set of particular risks.

- There is a range of sub cultures in organisations each of which can have a different level of risk culture maturity.

- Safety is the biggest driver of risk culture in most non-financial services. Hence safety has dominated risk thinking for these industries, leading to a late start for an ERM approach that seriously addresses all other risks.

- Most industries have, or are moving towards, greater responsibility for risks being taken at the front line as an integral part of that person's responsibilities.

4. "The seeds of the next crisis are sown in the solution to the previous crisis"

Whenever a solution is put in place to a challenge, it does it with the wisdom and consciousness available to people at the time. There are almost always unintended consequences that mean what was a well intended solution to a particular problem, potentially creates other challenges. The CROs identified a number of areas where the risk management frameworks being put in place may be solving an immediate challenge, but will need to evolve rapidly as they are creating other challenges. Examples include:

- Three lines of defence model – the metaphor of defence implies that risks are to be defended against rather than exploring the opportunities in risk. Creating a strong second line of defence can create a perception in the first line that risk is no longer their direct responsibility, or even if a risk occurs that they miss, the second line will pick it up.

- A strong compliance focus creates importance on following a process and dealing with risks that are already identified. This can take attention away from identifying emerging risks that don't make the compliance register – "it's what's outside the compliance list that will kill us". It can also increase the sense that compliance "owns" the risk responsibility and reduce the sense of responsibility at the first line.

- Choice of Chief Risk Officer – according to Bill O'Brien[15], former CEO of Hanover Insurance, "the success of an intervention depends on the interiors of the intervener". Hence the understanding, mindset s, attitudes and maturity of the CRO will significantly impact the robustness of the solutions put in place.

5. The thinking and cognitive biases prevalent in human beings will lead to major risks manifesting unless we are aware of and manage them

As human beings, there are various cognitive biases that mean we make decisions that are not fully rational and in worst case scenarios can lead to significant consequences. Some examples from the CROs and from Behavioural Finance literature include the following:

- We place more weight to recent past events. This leads to cycles of under-confidence and over-confidence. In a risk management context, it means that economic cycles are natural and healthy. Lack of economic cycles can mean an underestimation of risk impacts with such over-optimism leading to consequent disastrous decisions!

- The illusion of control – an organisation's belief that it can control the outcomes - often leads to short term decisions to "stabilise" systems. The Fed bank intervention through quantitative easing is an example. However, creating artificial stability (desire to control the outcome) can actually reduce the resilience of the system and make it much more susceptible.

- We are more likely to believe people we like. This might explain why some of the biggest scoundrels have been so likeable. It also might explain why whistle blowers may be ignored in favour of a familiar voice.

- We are loss averse as distinct from risk averse. People are prepared to take a much bigger risk to avoid losing something than they would be to gain something of equivalent value. Any organisational change initiatives imply transference of power, authority, responsibility and resources. And hence loss.

- We place much less weight on information that is vague or ambiguous or lacks coherence. Hence major risks may be ignored if they are vague or ambiguous or inconsistent with how an organisation has framed the likely future.

- We place undue weighting on what we fear or what we are familiar with.

6. Other insights

- The maturity of the risk culture drives the degree of openness of people in an organisation. This becomes a reinforcing loop.

- A mature risk culture drives having an outside in, bigger picture, open organisational attitude which is more likely to see emerging risks.

- Risk culture is shaped through the actions people take on a day to day basis. For these actions to be effective the people taking the actions must have a deep understanding of the risks and it must be aligned to the organisations risk appetite. Hence appropriate ongoing communication about the organisation's risk appetite is critical.

- Seeing risk as an opportunity will drive improvements in risk culture and risk management. Learning and development programs need to target and support this.

- Risk support at the front line is critical. Such support is best channelled directly through the risk champions or facilitators who have such support roles to the risk owners.

- The ideal is the business risk owner being a "mini" risk champion in their own right so that they make the most appropriate risk informed decisions for their organisation.

- Both qualitative and quantitative risk culture and risk management assessment and measurement are useful. The addition of a qualitative assessment can provide deeper insights into the quantitative assessment of the level of an organisation's risk culture.

- Paradoxically, greater level of staffing at second line of defence can both increase cost and reduce effectiveness of ERM. Keeping a trim second line of defence can place more responsibility on the first line to own the management of the risks they are taking. And the organisation must develop the necessary minimum level of maturity in the people and systems / structures on the front line to avoid risk and opportunity falling through the cracks.

- Breaking down silos is essential to have a free and transparent flow of risk relevant information, down and across the organisation. We observed that strongly siloed organisations are more likely to perceive the risk function as being obstructive rather than a partner and supporter. This in turn diminishes the influence of the risk team as well as the flow of information.

5 Chief Risk Officer attributes

"A sound risk culture is a substantial determinant of whether an institution is able to successfully execute its agreed strategy within its defined risk appetite."

Financial Stability Board (UK)

5.1 Attributes of an effective Chief Risk Officer

As a result of our observations, research, interviews and reflection we believe the following attributes are desirable in a CRO. This reflects our belief that a mature risk culture is an essential, albeit not always immediately obvious, foundation to an organisation's sound risk management. More widely a mature risk culture, reflecting the wider culture of an organisation, is essential to strong performance.

- *Reads the play* – understands the political and cultural systems at play in the organisation. Applies this understanding to embed an effective risk culture
- *Manages stakeholders* – builds trusted relationships with key executives and key decisions makers
- *Communicates* - in the language of the business, aligning the language and methodologies of risk management to the language of the business
- *Influences* - peers, senior executives and the board by getting their attention when needed and assisting them to understand the risk and opportunities quickly and effectively. This builds trust in the CRO's wisdom and judgement on risks
- *Passion for building capability* – supporting people across the business, at all levels, to continually increase their capacity to effectively manage risk
- *Holistic / systemic thinking* - understand both the operational and strategic landscape of the organisation and the industry. Understand the typical phases of risk maturity and the stage appropriate interventions for the organisation
- *Commercial* – ensures that the organisation can manage risk at the speed of the business, that risk management is an enabler rather than a disabler
- *Pragmatic* - recognises the practical dynamics of the roles of staff especially at the front line where decisions have to be made quickly. Is aware of the differences between staff in their levels of experience, training and judgement of risks and opportunities in their day to day actions
- *Persistent* - never gives up in communicating what actions are required to deal with what they believe are critical risks and/or opportunities. Persists in raising such risk issues to the point of being prepared to sacrifice their own job.

6 Recommendations

"Human beings, who are almost unique in having the ability to learn from the experience of others, are also remarkable for their apparent disinclination to do so."

Douglas Adams

Our overriding recommendation is to take the time to consider and think through how our section 4 findings and insights into risk culture across industries might apply to your organisation. In doing so we alert you to the need to use a risk culture measuring approach that is appropriate to your organisation's present stage of risk maturity. Take the risk culture journey one step at a time.

Other more specific recommendations are:

1. Incorporate the objective of having a sound, mature risk culture embedded in the organisation's enterprise risk management policy, which is board approved. Ensure that the risk management framework incorporates risk culture and plan the systems, processes and procedures to set, measure and manage risk culture to its higher state.

2. Set the desired risk appetite levels relating to risk culture against which measurements need to be compared. This assists having a risk culture that is appropriate to the organisation's objective.

3. Conduct a risk culture audit annually, measure its level by function, staff management hierarchy level, internal versus external stakeholders and the possible benchmark against this and other industries. Focus on the trends year-to-year and identify the actions required to improve the risk culture.

4. Get external independent objective assessments. Identify practices that other organisations are applying, and identify those appropriate for your organisation in its current circumstances.

5. Incorporate KPI/KRIs relating to the level of risk culture into individuals and teams performance assessments so that it is part of a balanced scorecard as a trigger affecting remuneration. Know that when remuneration is involved, people will take actions to demonstrate the measure is met. These actions aren't always aligned to genuine value creation for the business, so measures need to be set carefully.

6. Where risk culture is a poor match for the risks being addressed, consider as another option changing the risk process(es) to work with the culture you have e.g. evidential risk identification based approaches where self-certification is not working.

The topic of risk culture is one that is relatively new as a management tool to assist in improving risk management and business performance, particularly outside financial services. As such, there is an explosion of relevant material worth reading. A final recommendation is for you to find the time to read two excellent contemporary pieces of literature on the subject directly relevant to financial services in particular but also useful to other industries. They are:

(a) The 2013 Research Report on *Risk Culture in Financial Organisations* by Power, Ashby and Palermo (LSE etc)[16].

(b) The November 2013 paper by the U.K.'s Financial Stability Board, *Increasing the Intensity and Effectiveness of Supervision* [17].

7 Acknowledgements

"We shall not cease from exploration, and the end of all our exploring will be to arrive where we started and know the place for the first time."

T.S. Eliot

Sincere thanks to each of our CRO interviewees for their time and the benefit of their experience.

Thanks also to Josh Corrigan for his peer review of this paper and his constructive suggestions.

8 Appendix - Risk culture questionnaire - structure and sample questions

The questionnaire we asked our selection of Chief Risk Officers to complete comprised seven sections each of seven questions.

There was a choice of five answers - Never, Seldom, Sometimes, Often or Always.

Some questions were identical across more than one section and some were different. The questions were designed to enable us, in aggregate across the full set of 49 questions, to score an indicative level of risk culture maturity for each questionnaire filled and aggregations / averages for all or subsections of the population surveyed.

Our small sample was too limited for statistically significant analysis but we used our assessment of the responses to help validate our interview findings and vice versa.

The survey was conducted online and took around 20 minutes to complete. Typically such a survey is issued to all or to selected target subgroups within an organisation.

The seven sections, designed to capture the person's purvey perceptions of behaviour and standing, were:

1. Me
2. My Manager
3. My Team
4. My Department
5. Senior Management
6. The Organisation
7. Risk Function

The following extract is from the section of the questionnaire covering perceptions of the behaviour of: The Organisation

1. Risk appetite is clearly communicated in my organisation
2. My organisation responds effectively to external opportunities and threats
3. My organisation manages and takes risks consistent with its stated risk appetite
4. My organisation considers the long term impact of its strategic decisions on its risk appetite
5. The mission, vision and values of this organisation are clearly communicated
6. I think this company is doing a good job at taking calculated risks
7. Risk management in my organisation is as good as or better than risk management at similar

We also asked 3 open questions. See section 4.2.2. They were:

1. What do you believe are 3 of the most important aspects of an effective risk culture?
2. What do you see as your organisation's 3 greatest strengths in risk management?
3. What do you see as your organisation's 3 greatest weaknesses in risk management?

9 References

[1] Gerstner, L. Quote - http://quotesforbusiness.blogspot.com.au/2008/08/gerstner-on-culture.html

[2] McGing, S and Brown, A. , 2013, Actuaries Institute, *Board leadership in a complex world - optimising value from risk and opportunity*

[3] Schein, E., August 2009, *The Corporate Culture Survival*, Guide.

[4] Schein, E., August 2010, *Organizational Culture and Leadership*, Jossey-Bass

[5] Schein, E., *Edgar Schein's Ten Change Steps,* website http://www.theleadershiphub.com/files/EdgarScheinsTenChangeTips.pdf

[6] Hudson, P., 2013, *Safety Culture – Theory and Practice*, http://ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP-032///MP-032-08.pdf

[7] Putz, M. (2006): AQAL: Journal of Integral Theory and Practice, Spring 2006, Vol 1, No 1, *Integral Business and Leadership: An Intermediate Overview*

[8] Maslow, A., 1943, Psychological review, *A theory of human motivation*

[9] Maslow, A., 1954, *Motivation and personality*

[10] http://www.slideshare.net/BarrettValues/the-new-leadership-paradigm-richard-barrett

[11] Centre for Creative Leadership, *Leadership Culture Indicators.* http://www.ccl.org/leadership/pdf/community/connection/LeadershipCultureIndicators.pdf

[12] Laker, J, 2013, Australian British Chamber of Commerce, T*he importance of risk governance*

[13] The International Association for the Study of Insurance Economics - The Geneva Papers on Risk and Insurance Vol 26 No. 3 July 2001, *Enterprise Risk Management: Its Origins and Conceptual Foundation*

[14] ASX Corporate Governance Council, March 2014, *Corporate Governance Principles and Recommendations, 3rd Edition*

[15] Scharmer C. Otto, 2009, Berrett-Koehler Publishers*, Theory U – Leading from the Future as it Emerges,*

[16] Power M., Ashby S. and Palermo T., London School of Economics & Plymouth University, 2013, The Research Report on *Risk Culture in Financial Organisations*

[17] Financial Stability Board, November 2013, *Increasing the Intensity and Effectiveness of Supervision. Consultative Document. Guidance on Supervisory Interaction with Financial Institutions on Risk Culture.*