Risk Appetite: The Interpolation of Risk and Strategy

A Contribution to Central Bank of Ireland discussion on Risk Appetite

Risk Appetite: The Interpolation of Risk and Strategy

A Contribution to Central Bank of Ireland discussion on Risk Appetite

Abstract

This paper has been prepared in response to a call for submissions by the Central Bank of Ireland on the topic of Risk Appetite. The author seeks to contribute to the discussion based on long experience as a practitioner in the Risk Management arena. In the Introduction to the paper the author makes a number of observations of a general nature based on experience of working with a wide variety of companies. The author then goes on to describe the Risk Landscape in broad terms before responding to a set of questions specifically posed by the Central Bank in their call for submissions. The author then finally goes on to offer some additional practical observations and advice in relation to Risk Appetite Statements and Risk Appetite Frameworks, an area where some confusion can often arise. Throughout the paper a number of practical approaches to managing the relationship between strategy and risk are detailed.

About The Author: Mr. Peadar Duffy is founder and Chairman of Risk Management International, a firm that has been advising clients in relation to risk in Ireland and internationally for over 20 years. He is a member of the Irish Risk Management Standards Committee which is governed by the National Standards Authority (NSAI). As such he is one of two Risk Experts representing Ireland on the International Organisation for Standardisation (ISO) working group (WG2) which is undertaking a review of the recently published and now globally accepted risk management standard (ISO 31000: Risk Management 2009). He can be contacted at peadar.duffy@rmi.ie

About RMI: Risk Management International (RMI), is a private Irish company established for over 20 years. RMI provides leading edge thinking, advice and consultancy on risk management to public and private sectors and to local and multi-national businesses. It provides a range of services in relation to risk governance, operational risk management and crisis management. In addition to its core team of consultants the firm has access to a wide range of associates with deep operational experience having filled leadership roles in major organisations. For more information see www.rmi.ie

Contents

Table of Figures

Introduction

RMI welcomes the Central Bank of Ireland's leadership in commencing this series of discussions on the important, and now somewhat vexed, matter of Risk Appetite. Since the Global Financial Crisis (GFC) regulators, investors and boards of directors have become more determined to avoid a repetition of such a cataclysmic event and have increased demand for more effective risk management. Similarly, just as Financial Risk Reporting failed to predict the GFC, there is growing recognition of the need to build organisational resilience through effective mapping of risks and developing appropriate proofs to demonstrate organisational capability to manage low probability high impact events. Concern is also growing over the increase in cybercrime and of digital risk, both compounded by the trend in outsourcing of business activities and the emergence of a virtual business world encompassing cloud based technologies and overseas operational dependence, often through third parties .

With regard to this particular discussion on Risk Appetite initiated by the Central Bank of Ireland, we offer some observations of a general nature based on our experience of working with a wide variety of organisations as follows:

1. Directors and senior managers are in need of a globally accepted guidance on the attributes of an effective Risk Appetite Framework.

2. Emphasis (globally) is shifting from Risk Management to Resilience Building where Risk Optimisation (A State of Organisational Resilience) is achieved when an organization can demonstrably 'Optimise Value through aligning Risk and Strategy with Corporate Objectives'.

   Achieving this requires 'both' board and executive mastery of strategic, emerging and external/global risks, through robust (risk) horizon scanning, proofing and testing.

3. *"Strategic risks" are those risks that are most consequential to the organization's ability to execute its strategies and achieve its business objectives. These are the risk exposures that can ultimately affect shareholder value or the viability of the organization. "Strategic risk management" is "the process of identifying, assessing and managing the risk in the organization's business strategy—including taking swift action when risk is actually realized. Strategic risk management is focused on those most consequential and significant risks to shareholder value, an area that requires the time and attention of executive management and the board of directors"*[1]

   RMI thus defines Board Risk Assurance as assurance that Strategy, Objectives and Execution are aligned.

4. Alignment of Strategy, Objectives and Execution is achieved through operationalising the links between Risk and Strategy. This involves:
   - Strengthening the Strategic Planning Process through organisational integration of the risk and strategy functions/processes with authority derived directly from the Board and CEO's office,
   - Establishing an effective Risk Appetite Framework,
   - Understanding, and improving the organisational level of risk maturity,
   - Building Organisational Resilience,

- Proofing and testing management's ability to offer credible solutions when both exploiting and defending operations, the business model and reputation.

5. The Risk Appetite Framework (RAF)[2] is to the Board of Directors what Risk Management[3] is to the rest of the organisation. As such there is a direct correlation between the efficacy of the RAF and the efficacy of the Risk Management Framework[4]. On this basis ensuring that Risk Appetite Frameworks are both actionable and measurable requires that Risk Charters (at Board Audit and Risk Sub-committee levels) provide a Risk Governance Framework which mandates:
   - Direct CEO oversight of an integrated risk and strategy capability,
   - Board Risk Sub-Committee oversight of:
     i. The Risk Appetite Framework,
     ii. Advancing and maintaining Risk Maturity which at its optimum level delivers value through:
        a) Access to capital at lower cost than that achieved by less mature competitors,
        b) More favourable credit ratings than those achieved by less mature competitors,
        c) Optimisation of risk transfer through both traditional and modern self-insurance methods.
   - Risk Data Governance maintained to standards of rigor and consistency as those which apply for accounting data,
   - Perpetual proofing and testing of management's readiness to offer credible solutions when both opportunity strikes and abnormal and adverse events occur.

We have provided answers to the questions posed in the Central Bank of Ireland discussion paper on Risk Appetite and have sought to establish a fresh and thought provoking tone to our contribution. We are influenced by Peter Bernstein and Robert S. Kaplan who have done much through their respective contributions to thought leadership in the fields of risk management and strategy (balanced scorecard) execution.

The tone of our contribution is thus reflected as follows:

> *In the absence of certainty, the only way to maintain potentiality is to focus on excellent execution and demonstrable resilience at the same time whilst taking as much acceptable risk as is reasonably possible*
>
> *Peter Bernstein, Against the Gods, The Remarkable Story of Risk*

> *The strategy map and scorecard provide the road map to guide this strategic journey. Risk management, in contrast, is about identifying, avoiding, and overcoming the hurdles that the strategy may encouter along the way. Avoiding risk does not advance the strategy; but risk management can reduce obstacles and barriers that would otherwise prevent the organization from progressing to its strategic destination.*
>
> *Robert S. Kaplan, Risk Management and the Strategy Execution System*

Peadar J. Duffy B.Sc.

Chairman

NOTE

RMI notes that the Central Bank of Ireland discussion paper on Risk Appetite is focused primarily at directors and then at senior management within organisations regulated by the Central Bank of Ireland. Notwithstanding we suggest that the absence of any reference to the UK Financial Reporting Council, The Institute of Risk Management, COSO (Committee of Sponsoring Organizations to the Threadway Commission), ISO 31000 (Risk Management 2009), ISO Guide 73 (Risk Management – Vocabulary) etc. limits the scope of international research and understanding which is being used to inform this important discussion. We believe that these globally accepted sources of reference represent critical components of an emerging global response that will be particularly influential in the case of publicly traded companies.

The Risk Landscape

Lessons learned following the GFC include the importance of establishing an effective risk governance framework at the board level. In essence two key questions must now be addressed by Boards.

First, do they express clearly and comprehensively the extent of their willingness to take risk in order to meet their strategic and business objectives? Second, do they explicitly articulate risks which have the potential to threaten their operations, business model and reputation?

In order to be in a position to provide credible answers to these fundamental questions, we must first seek to understand the relationship between Risk and Strategy.

It is RMI's experience that risk and strategy are intertwined. One does not exist without the other, and they must be considered together. Such consideration needs to take place throughout the execution of strategy. Consequently it is vital that due regard is given to Risk Appetite when strategy is being formulated.[5]

Crucially, Risk is now defined as *'the effect of uncertainty on objectives'* [6]

It is clear therefore that effective corporate governance is strategy and objective setting on the one hand; and superior execution with due regard for risks on the other.

This particular landscape is what we in RMI refer to as 'The Interpolation of Risk and Strategy'.

For this reason RMI describes *Board Risk Assurance* as assurance that strategy, objectives and execution are aligned.

Alignment is achieved through operationalization of the links between risk and strategy which is described in greater detail later throughout this paper.

Before further discussion however, we would like to draw attention to observations based on our practical experience which give cause for concern, namely:

1. **Risk Appetite**: While we now have a globally accepted risk management standard[7] and sharper regulatory definition of effective risk management for regulated organisations, there is as yet much confusion, and neither a consensus nor an internationally accepted guidance as to the attributes of an effective Risk Appetite Framework.

2. **Risk Reporting:** In relation to risk reporting two significant matters arise as follows:

   Risk Registers which are primarily generated on the basis of a *compliance* centric requirement, as distinct from an *objectives* centric[8] approach, tend to contain *lists of risks* which are not explicitly associated with objectives. As such they offer little value in terms of reporting on risk performance.

   NOTE: RMI supports the adoption of a board driven objectives centric approach[9] to reporting and monitoring risks to operations, the business model and reputation.

Risk Registers and other reporting tools detail known risks and what *we know we know*. They tend not to detail emerging or high velocity risks which have the potential to threaten the business model. As such they tend to be of little /limited value in terms of reporting or monitoring either known unknown[10], or unknown unknown[11] risks. This is a matter which should give boards of directors cause for concern given pace of change, hyper-connectivity and the disruptive nature of new technologies.

3. **Risk Data Governance:** The quality, rigour and consistency in application of accounting data which is present in well managed organisations does not equally exist in those same organisations in the risk domain.

   The responsibility of directors to use reliable accounting information and apply controls over assets etc. (internal controls) as part of their legally mandated role extends equally to information pertaining to risks which threaten financial performance. The latter is not however treated in an equivalent fashion to accounting data. Whereas the integrity of accounting data is assured through the use of proven and accepted accounting systems subject to audit, the latter typically relies on the use of disparate excel spreadsheets, word documents and Power Points with weak controls over the efficacy of copying and pasting of data from one level of report to another.

   Weaknesses and failings in Risk Data Governance can be addressed in much the same way as for other governance requirements.

   For example:

   a. Comprehensive training for business line managers and supervisors on:
      - (Risk) Management Processes,
      - (Risk) Vocabulary,
      - (Risk) Reporting,
      - Board (Risk) Assurance Requirements.

   b. Performance in executing (risk) management roles and responsibilities included in annual performance appraisals,

   c. System[12] put to process through the use of database/work flow solutions.

      Crucially systems providing an *evidence* basis of assurance that:
      - The quality, timing, accessibility and auditability of risk performance data is as rigorously and consistently applied as that for accounting data,
      - Dynamic management of risk data (including Risk Appetite/tolerance/criteria) can be tracked at the pace of change,
      - Tests can be applied to the aggregation of risks to objectives at the pace of change and prompt interdictions applied as and when required,
      - Reports, or notification, of significant risks are escalated without delay, and without risk to the originator of information.

4. **Lack of understanding of the Nature of the Risks which need to be Mastered, in the Boardroom:**

   Risk is defined as *the effect of uncertainty on objectives.*

There are many types of objectives for example economic, financial, political, regulatory, operational, customer service, product innovation, market share, health safety etc. and there are multiple categories of risk.

But what is uncertainty?

Uncertainty[13] *is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood*.

There are essentially two kinds of uncertainty:

1. Measurable Uncertainties: These are inherently insurable because they occur independently (for example traffic accidents, house fires etc.) and with sufficient frequency as to be reckonable using traditional statistical methods sufficient to reasonably and confidently project likelihood and consequence.

   Measurable uncertainties are treated individually through traditional (risk) management supervision, and residually through insurance.

   Measurable uncertainties are funded out of operating profits.

2. Un-measurable uncertainties: These are inherently un-insurable using traditional methods because of the paucity of reliable data. For example whereas we can observe multiple supply chain and service interruptions, data breaches etc. they are not sufficiently similar or comparable to be soundly put to a probability distribution and statistically analysed.

   Un-measurable uncertainties are treated on a broad basis through organisational resilience. For top 5-15 corporate risks[14] which are typically inestimable in terms of likelihood of occurrence, the organisation seeks to maintain an ability to absorb and respond to shocks and surprises and to deliver credible solutions before reputation is damaged and stakeholders lose confidence.

   Un-measurable uncertainties are funded out of the balance sheet.

The hyper-connected and multispeed world in which we live today has driven the effect of un-measurable uncertainties on company objectives to new, unprecedented, heights, and so amplified the risk potential enormously.

5. **Urgent need to recognise the mission critical importance of Building Resilience** and preparing management to *always be prepared* to offer credible solutions in the face of unexpected shocks and surprises

Figure 1 below describes the evolution of risk management as depicted within the red dotted line[15] and the next stage of the evolution (Resilience) as envisioned by RMI.

RMI's View: Next Evolution in Risk Management: Resilience: Focus on Un-measurable Uncertainties

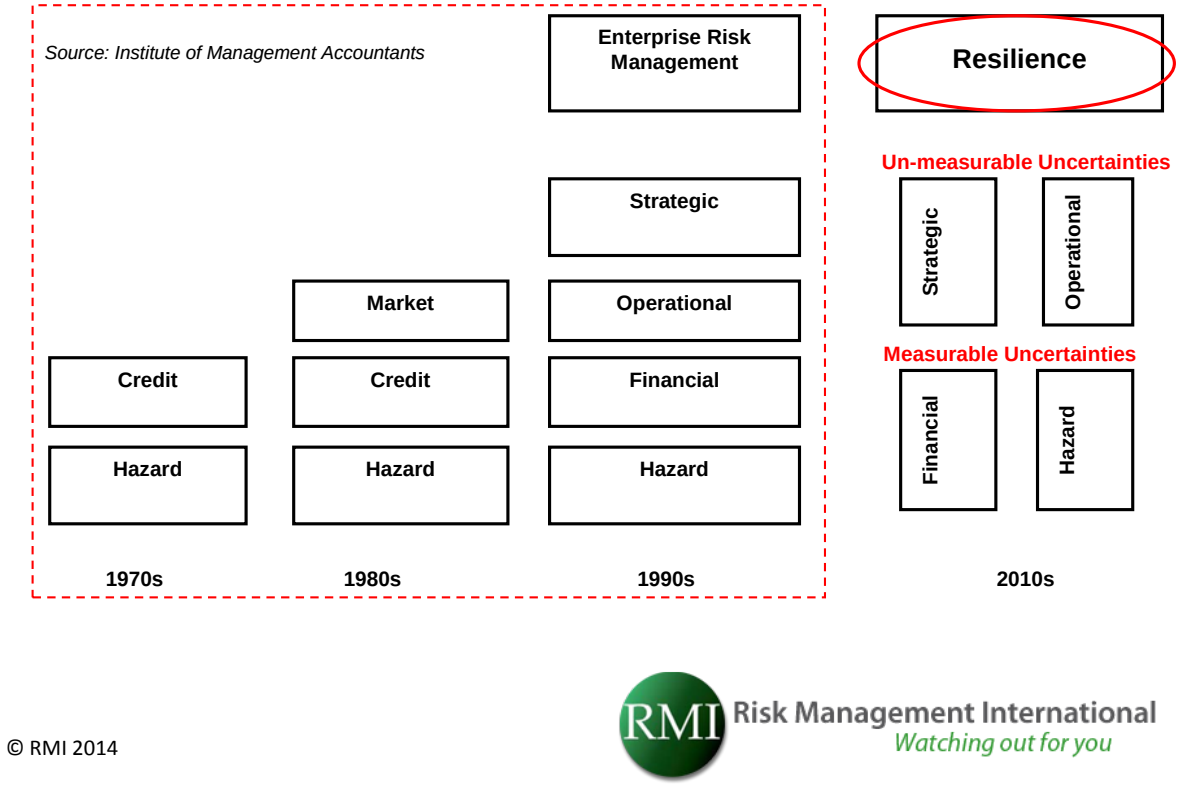

Figure 1: Evolution of risk and the emergence of "Resilience" as the current era in the evolution of 21st century understanding of risk

Resilience was the theme which ran through the World Economic Forum: Global Risks 2013, Eight Edition Report.

Resilience was described thus *as capability to*

1. *Adapt to changing contexts,*
2. *Withstand sudden shocks, and*
3. *Recover to a desired equilibrium, either the previous one or a new one, while preserving the continuity of operations.*

The three elements in this definition encompass both recoverability (the capacity for speedy recovery after a crisis) and adaptability (timely adaptation in response to a changing environment).

The Global Risks 2013 Report emphasized that global risks do not fit neatly into existing conceptual frameworks but that this is changing insofar as The *Harvard Business Review (*Kaplan and Mikes[16]) recently published a concise and practical taxonomy that may also be used to consider global risks[17].

The report advises that building resilience against external risks is of paramount importance and alerts directors to the importance of scanning a wider risk horizon than that normally scoped in traditional risk frameworks.

When considering external risks directors need to be cognisant of the growing awareness and understanding of the importance of emerging risks.

Emerging risks can be internal as well as external, particularly given growing trends in outsourcing core functions and processes.

> *''Effective risk management requires understanding more about what we don't know than what we do know. In particular, it must recognise when new risks are emerging. Too often, risk assessments plot the usual "known knowns", leaving executives and directors underwhelmed because the process doesn't really tell them anything they don't already know''*[18]

It is also interesting to observe the diversity in understanding of Emerging Risk definitions, for example:

- **Lloyds:** An issue that is perceived to be potentially significant but which may not be fully understood or allowed for in insurance terms and conditions, pricing, reserving or capital setting,
- **PWC:** Those large scale events or circumstances beyond one's direct capacity to control, that impact in ways difficult to imagine today,
- **S&P:** Risks that do not currently exist,

The 2014 annual Emerging Risks Survey (a poll of more than 200 risk managers predominantly based at North American re/insurance companies) reported the top five emerging risks as follows:

1. Financial volatility (24% of respondents)
2. Cyber security/interconnectedness of infrastructure (14%)
3. Liability regimes/regulatory framework (10%)
4. Blow up in asset prices (8%)
5. Chinese economic hard landing (6%)

This leads us to conclude that maintaining business defense systems capable of defending the business model **has become an additional fiduciary requirement for the board of directors**, alongside succession planning and setting strategic direction[19].

Central Bank of Ireland Questions on Risk Appetite Statements

Should all organisations have a Risk Appetite framework?

The relationship between risk and strategy described above is a function or neither risk management, nor strategic management.

Rather it is simply ***Good Management in an Uncertain World*** where business models are:

a. Increasingly driven to be available on a 24/7 global footprint,

b. Online using telecom networks,

c. Becoming more dependent on third party service providers,

d. Becoming more interconnected within larger financial, supply chain and energy supply chains.

It is our view that the term *risk management* will within the 2010 decade become supplanted by the term *resilience management* and that the latter term will become an integral part of *risk culture* in organisations which, in the first instance, are trading internationally or vulnerable to international supply chains.

Figure 2: Smartphones and the speed of twitter

Maintaining a Risk Appetite framework will thus before the end of this decade be a matter of necessity, and not a matter of choice. The driver in this regard will be the pace of change. Note the images in Figure 2 above. Same location, same event (papal inaugurations), same type of people BUT different ways in which people are living the same moment!

What is leading Organisations to put formal Risk Appetite Frameworks in Place?

Greater investor and regulatory focus, combined with a recognition that risk practices are becoming increasingly professional, has caused organisations to change attitude towards risk from a broadly negative stance towards a more positive, engaged and proactive approach.

We note a global scarcity of skilled Chief Risk Officers and unwillingness by organisations to commit resources in the current economic climate. Notwithstanding enlightened organisations are gaining appreciation of the links between risk and strategy and in turn towards putting in place the necessary resources and supports to provide greater risk professionalism.

How are Risk Appetite and strategy related?

The diagram below describes the relationship between risk and strategy.

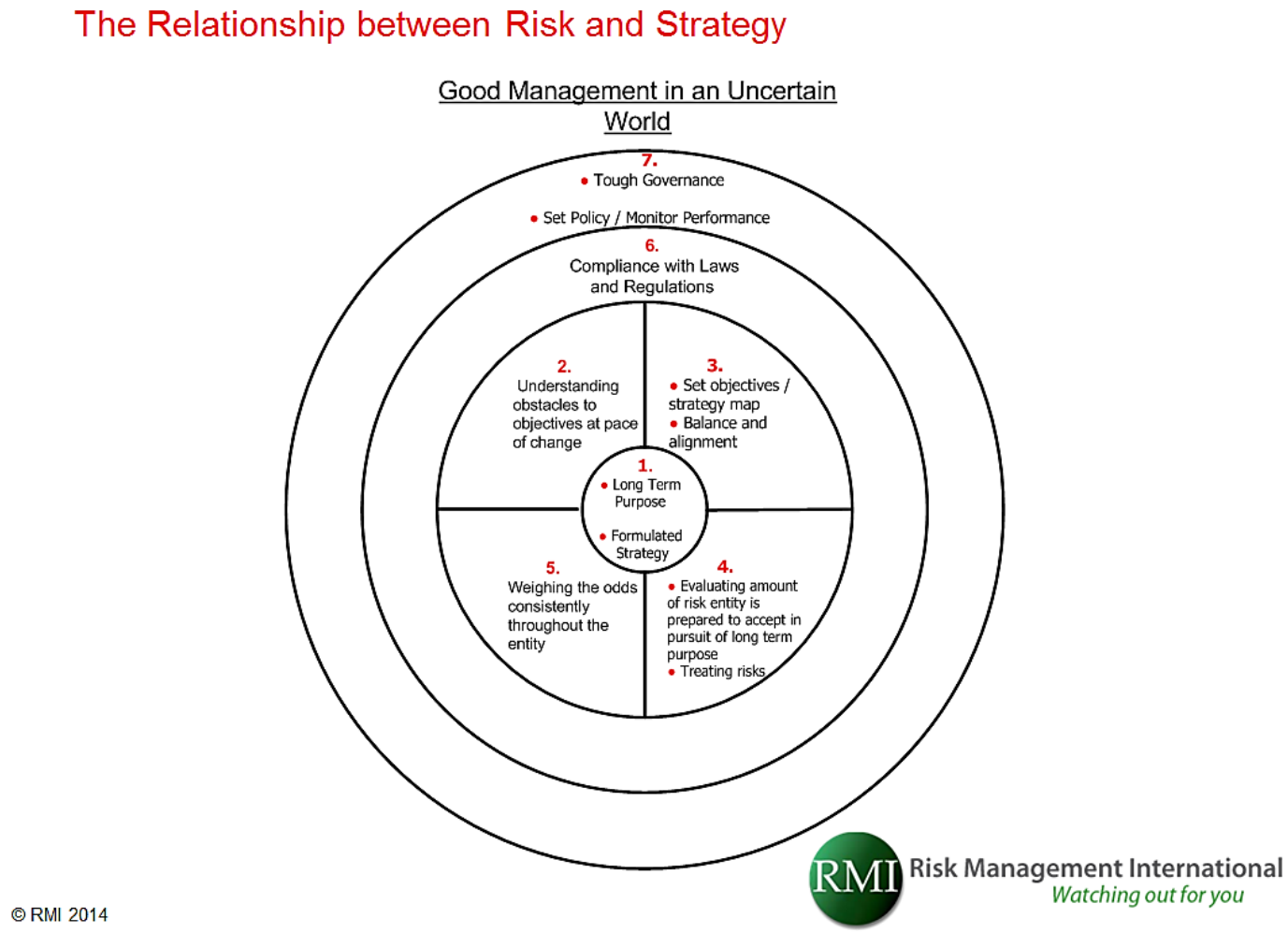

Figure 3: RMI's 7 elements approach to aligning strategy and risk

Earlier in this paper we described Board Risk Assurance as assurance that *Strategy, Objectives and Execution are aligned.*

We further explained that alignment is achieved by *operationalising the links between risk and strategy.* This is achieved by integrating each of the seven numbered elements described in the diagram above as follows:

1. **Reaching a determination as to Long Term Purpose and Formulating those Strategic Initiatives and Objectives which are required to achieve it[20],**

2. **Understanding Obstacles to the Achievement of Objectives**: This needs to be understood PRACTICALLY in terms of a motor journey from say Dublin to Cork, or Berlin to Paris.

   Before the journey people need to understand, and manage, what can stop them, slow them down, or distract them on the journey. Once people understand risk management in these simple and practical terms they understand that risk management is more about achieving objectives (getting from point A to point B) than compliance with regulations. It is about improving performance on the journey.

   What people? In the simplest of terms they are the owners of the car (shareholders represented by the Board), the driver (CEO and executives), and passengers (comprised of primary stakeholders i.e. customers, employees, investors, suppliers and secondary stakeholders and others with a legitimate interest in the business).

3. **Setting Objectives and getting balance and alignment (Note: Strategy Maps e.g. Balanced Scorecard)**:

   This is done in risk management terms by:

   a. **Strengthening the Strategic Planning Process,** for example:
      i. Increasing rigour, formality and consistency in the strategic planning office (SPO) which derives its authority from the board and the CEOs office,
      ii. Aligning strategy, risk and audit board sub-committees (through cross representation) in a manner which largely mirrors the conventional three lines of defence model[21] and reflects the requirement to strengthen board risk oversight, reporting and monitoring[22],
      iii. Embedding risk management competence within the SPO[23],
      iv. Explicitly articulating corporate and organisational objectives,
      v. Testing the alignment of group, corporate and organisational objectives through development and review of Risk Appetite statements.

   b. **Establishing an effective Risk Appetite Framework** which includes:
      i. Statement of Purpose and Values of the Organisation,
      ii. Explicitly stated *Board Risk Assurance* Requirements; factors to consider would include:
         1. Mapping objectives to a Risk Appetite Continuum,
         2. Qualitatively expressed Risk Appetite Statements,
         3. Quantitatively expressed Risk Criteria related to both Risk Tolerance and Risk Limits.

   c. **Understanding, and improving the organisational level of risk maturity**
      Risk Maturity is outside the scope of this paper; however discussion on the topic would be welcomed by RMI. RMI has developed a five level RMI Risk Maturity Index which provides a road map to risk optimisation. The index scores risk maturity capability requirements etc. In summary it describes:
         - Level 5: 'Value Driven' Optimising Value though aligning risk and strategy with corporate objectives,
         - Level 4: 'Managed' Gaining Value through aligning risk and strategy in pursuit of corporate objectives,
         - Level 3: 'Insight' Gaining Insights into how to better align risk and strategy in pursuit of corporate objectives,
         - Level 2: 'Awareness' Developing awareness into how to align risk and strategy in pursuit of corporate objectives,

- Level 1: 'Basic' Seeking awareness of the links of risk and strategy in pursuit of corporate objectives.

d. **Building Resilience**:
   i. Ensuring that the SPO engages in systematic risk horizon scanning as well as:
      1. Understanding near misses and escalation reports in own organisation and externally,
      2. Monitoring performance of risk treatments[24],
      3. Proofs and tests of the quality of decision making, and decision making processes, through simulated 'Threat' and 'Opportunity' Crisis[25] Scenario(s) Exercises,
   ii. Anticipating Emerging Risks[26].

4. Evaluating the amount of risk the organisation is prepared to accept in pursuit of the long term statement of purpose; AND THEN DECIDING how to treat risks:

Just as implementation is mission critical to performance[27], risk treatment is at the cutting edge of risk management; and managing risks!

Disappointingly however very many organisations commit disproportionate resources to risk assessment with inadequate attention paid to *what really matters;* that is treating risks. In essence very many organisations concentrate on the P in the PDCA (plan do check act) cycle with not enough attention paid to doing, checking, and acting on continuous improvement requirements.

This is pretty much in evidence in a review of many of the risk registers we have examined on behalf of clients. The majority of the surface area/content of the report (sadly, and sometimes tragically, an excel, word or Power Point; as distinct from a credible database solution[28]) is given to risk assessment.

In our experience it is often the case that precious little detail is given to:

a. Who, specifically is responsible for individual risk treatments,
b. Change management and resource requirements supporting risk treatments,
c. What are the project/risk treatment KPIs, milestones and gateways,
d. What is the expected residual effect of risk treatments on likelihood and impact,
e. What is the role of management in reviewing performance against KPIs, milestones and gateways.

Risk Treatment reports which are presented to the level of detail described above; and which are evaluated by the SPO in a manner that provides a feedback loop to the performance of objectives become *leading Indicators* of the future state of health of objectives.

5. **Weighing the odds consistently throughout the organisation:** This is the function of the Chief Risk Officer (CRO), a most important role within the organisation, and Risk Committee.

The ability of the CRO and risk committee to efficiently and effectively perform this function is directly proportionate to the efficacy of the assurances delivered as described above.

Typical weaknesses and challenges which can occur include:

a. Frequency of changes required to Risk Criteria (tolerances and limits) in early stage (risk) maturity organisations as a consequence of:

- Pace of change internally and externally in the organisation,
- Identification of emerging and external risks hitherto not understood.

b. Inability to undertake real time dynamic tests of risk aggregations:
   - Around discreet objectives,
   - Across risk categories.

The weaknesses and challenges described above often result in:

a. Meetings where questions asked can only be answered in terms of:
   i. This is the historic 'point in time' information we have prepared,
   ii. We will need to revert with answers to your query in X days.
b. Risk aggregation tests not being run and emerging/known unknown risks not being identified until there is an occurrence which can be minor, or substantial.

6. **Compliance with Laws and Regulations:** Organisations are established to achieve superior returns, with limited liability to risk takers. However they are expected to do so having full regard for all rules, regulations and legal requirements.

   Clearly it is axiomatic that assuming the lawful intent of a company's original promoters, and thereafter its directors and the executive, that the company will at all times operate within the law. To this extent compliance is an operational imperative and a sunken cost.

   Compliance alone does not drive value; but without it value cannot be created.

   It would seem inappropriate to place compliance at the centre of board agenda. Just as it would be a mistake to place compliance at the centre of the diagram above which describes the relationship between risk and strategy.

   However compliance is a mission critical element within the risk/strategy governance framework as described above.

7. **Tough Governance, Setting Policy and Monitoring Performance:** In the context of the relationship between Risk and Strategy *Tough Governance* means *Risk Culture.*

   Risk Culture is a term describing the values, belief, knowledge and understanding about risk shared by a group of people with a common purpose, in particular the employees of an organisation or of teams or groups within an organisation. This applies whether the organisations are private companies, public bodies or not-for profits and wherever they are in the world.[29].

   Risk Culture, as an aspect of Culture, can be practically described thus:

   Culture: The way we do things around here!

   Risk Culture: The Freedom we have to Challenge around here!

   Risk Culture is capable of being demonstrably and credibly evidenced by:

   a. Board and executive messaging[30] on threats and risks to operations and jobs when people fail to act/report when they:

i. Identify a smarter way of completing a task, achieving an objective,
ii. See a threat or risk to the organisation.

b. Escalation reports and their treatment by the executive and management,
c. Near misses reported and averted.

In the later section 'Questions on Risk Culture' RMI links the achievement of a target State of Risk Culture with Risk Maturity

Would it be desirable for the Central Bank of Ireland to facilitate a forum, comprising participants with experience in the financial services industry to develop a range of good practices with respect to the preparation and monitoring of Risk Appetite Statements?

A number of lessons can be drawn from the Global Financial crisis:

1. In relation to Strategic[31] Risks, Leaders ignored common sense and did not challenge the absence of any scientifically sound basis for accepting that paradigm shifts (property prices, economic and monetary super performances across major economies) had occurred,

2. In relation to Operational[32] Risk, Nassim Nicholas Taleb, in his seminal work *The Black Swan: The Impact of the Highly Improbable,* described the Bell Curve as the Great Intellectual Fraud. He was not saying that Value at Risk (VAR) as a model was fraudulent but that when misused it certainly was. He wrote that *the rarer the event, the higher the error in our estimation of its probability –even using the Gaussian.* VAR is still in use, and when used correctly it is perfectly valid. What occurred in effect was a confluence process, people and systems failures.

It is our view that advancing Risk Professionalism requires an understanding of the entirety of the risk landscape. In the absence of such an understanding defining, communicating and monitoring Risk Appetite becomes a theoretical exercise which offers limited value.

RMI is therefore not convinced that a regulatory body should directly facilitate a forum, particularly given the commercial nature of strategy based information and the potential to offend the Competition Act. Rather we recommend that the Central Bank of Ireland should mandate that industry create an effective coming together[33] to facilitate the consolidation of information and best practices.

We recommend that *advancing risk professionalism* should become the Central Bank of Ireland's focus of attention. In this regard emphasis should be placed on:

- Building Resilience against shocks and surprises[34],
- Increasing Risk Maturity.

In issuing such a mandate boards would be made aware of their particular risk oversight responsibilities manifest in:

- Optimising Value though aligning risk and strategy with corporate objectives[35],
- Defining, communicating and monitoring Risk Appetite(s),
- Strengthening risk culture,
- Advancing Risk Maturity,
- Demonstrating proficiency in risk management,
- Establishing and demonstrating confidence in Risk Resilience and the ability to manage the organisation through a crisis.

Questions on Risk Appetite, Risk Tolerance and Risk Limits

What definition of Risk Appetite does your organisation consider to be appropriate ?

We concur with the observation that difficulties arise in the absence of agreed common definitions.

We agree that as Risk Appetite, tolerance and limits can be difficult concepts to communicate that the use of diagrams is desirable.

In its discussion paper, the Central Bank of Ireland set out to contextualise Risk Capacity and Risk Appetite (See Figure 1, page 7 of the discussion paper). We observe what appears to be a difference in understanding between the CBI view, and its associated definitions, and the sequence of diagrams and explanations given in the Institute of Risk Management's (IRM) (http://www.theirm.org/knowledge-and-resources/guides-and-briefings/ 2011 Risk Appetite Guidance.

We consider this worthy of discussion and recommend further consideration before particular definitions are formally adopted.

We further recommend that the scope of international research and understanding be broadened to include relevant material from:

- The UK Financial Reporting Council,
- The Institute of Risk Management,
- COSO (Committee of Sponsoring Organizations to the Threadway Commission),
- ISO 31000 (Risk Management 2009) and ISO Guide 73 (Risk Management – Vocabulary).

In your view, how are Risk Appetite, risk tolerance and risk limits related to one another?

We are aware of the nature of differences in philosophy which are influencing the gradual determination of internationally accepted definitions. Notwithstanding we commend the definitions and the sequence of diagrams and explanations given in the Institute of Risk Management's (IRM) (http://www.theirm.org/knowledge-and-resources/guides-and-briefings/ 2011 Risk Appetite) Guidance.

A number of models exist which seek to describe the relationship between Risk Appetite, tolerance and risk, for instance, the Ernest and Young Risk Pyramid below.

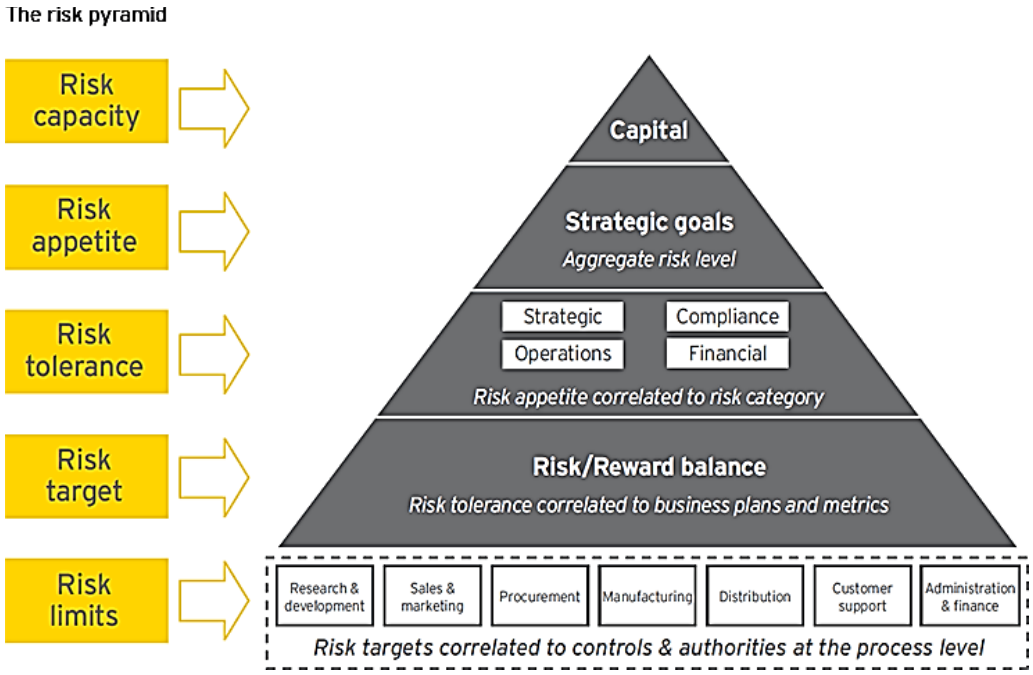

Figure 4: Ernst & Young Risk Pyramid

How are organisations using risk limits and risk tolerances around those limits?

Our experience in working with clients shows that organisations are continuing to struggle with basic risk concepts, definitions, language, responsibilities, reportage and delivery. Accordingly while risk limits are set to contain risk taking practices, lack of common language and loose interpretation of concepts is causing confusion within organisations and leading to limits being seen as negotiable within the context of risk tolerances.

As a corporate discipline, risk management is in its infancy and the quality of risk practitioners is generally poor. Risk limits are perceived negatively by business practitioners who then use their limited knowledge of risk tolerances to argue for greater flexibility in applying limits.

How do organisations facilitate early warning of potential breaches of Risk Appetite?

In practice we find that there is limited such facilitation. Rather, as referenced above, there is a belief that as business people using risk to derive reward, the concept of risk is seen more for its capacity to delimit practices which drive value and thus it is easier to adopt the business school mantra of 'seeking forgiveness rather than permission'. This is made easier in organisations where risk is seen as a nuisance and impediment to business and where lack of appreciation of quality risk management is not apparent at senior level. The tendency for business generators is often to view risk as friendly and flexible, designed to support business generation and thus for limits to be viewed as speed limits are on the public highway, more for observation than observance. Accordingly we find few cases where early warnings are seen as other than flashing lights on the

dashboard. In many cases, early warnings predicate the need to prepare a case to take to the risk committee for revised limits based on the gains for the business to be had from underwriting new risk opportunities rather a cause of severe braking being needed in risk management practices to ensure conformity.

Much of the foregoing represents the cultural challenge of embedding risk as a serious discipline rather than a faux science treated as an 'add on'. This reflects the nascent nature of risk and its failure to be seen at Board level as front and central to strategy and its effective and safe execution. Culture, and 'tone from the top' are critical here along with strong support for risk executives at senior management level and an appreciation that risk management is more akin to the medical profession where the basis of hygiene underscore all procedures and provide a safe and secure means of conducting business rather than an impediment. The absences of good quality risk officers and of universally accepted definitions of risk also lead to an undermining of the discipline in organisations where there are few effective sanctions against limits being broken.

Questions on Risk Culture

How do organisations assess risk culture?

What are the challenges that organisations face in terms of communicating risk culture to stakeholders?

Optimal Risk Culture is designed and, thereafter nurtured, on building blocks practically described as blocks ABC akin to the Institute of Risk Management A-B-C[36] approach to risk culture.

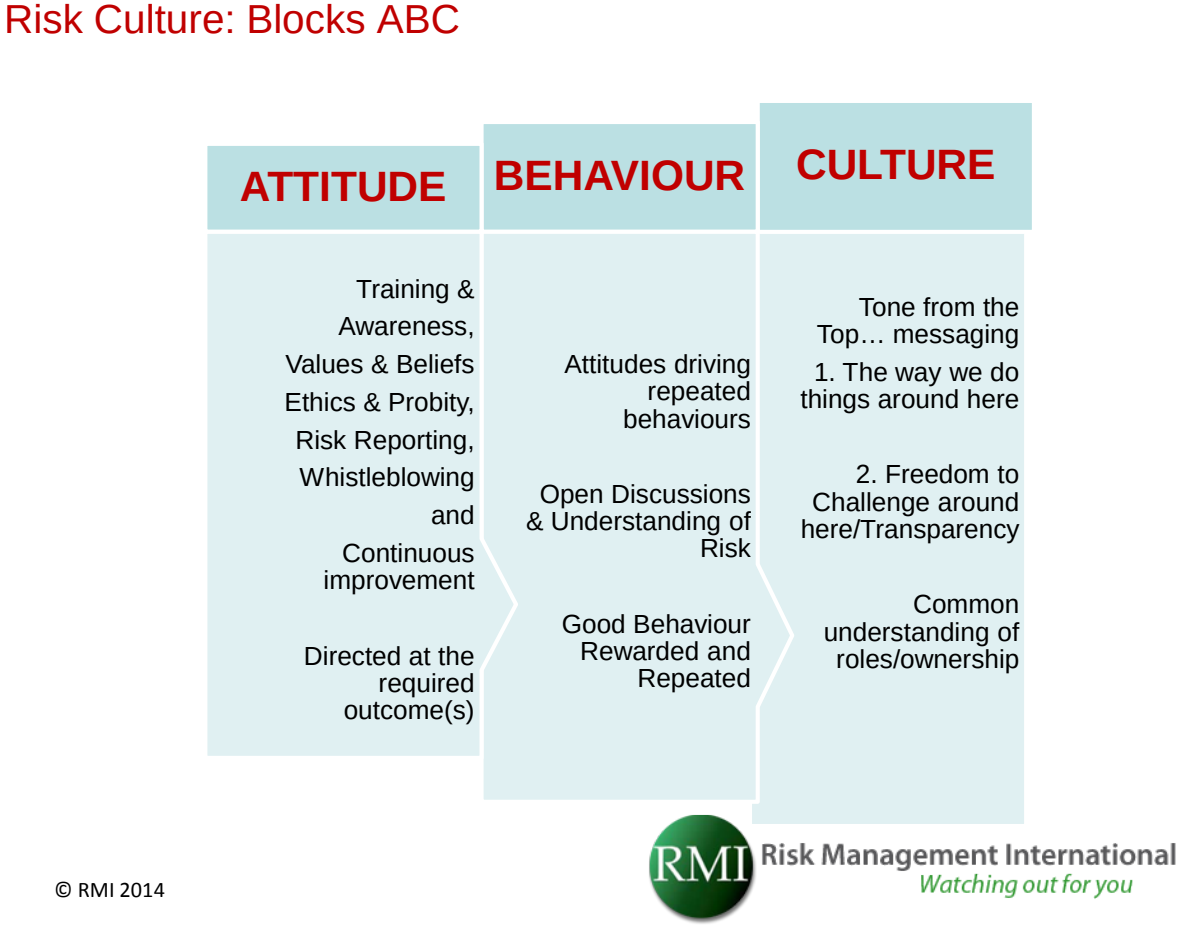

Figure 5: The Building Blocks of Culture

The building blocks are briefly summarised as follows:

1. Training, values and beliefs, reporting and continuous improvement directed at outcomes driving **attitudes** displayed by people, which
2. Influence their **behaviours** and thus the quality of their discussions and decision making, thereby
3. Manifesting as demonstrably credible risk **culture**.

Other than retrospective analysis of poor Risk Culture following various corporate crises there is a limited body of reliable knowledge, and experience, in the field of assessing 'existing risk culture' and successfully thereafter navigating a course to a 'target risk culture'.

The Iinstitute of Risk Management (IRM), Risk Culture, Under the Microscope: Guidance for Boards makes reference to the IRM Risk Culture Framework which describes multiple interactions (reference Figure 6 below)

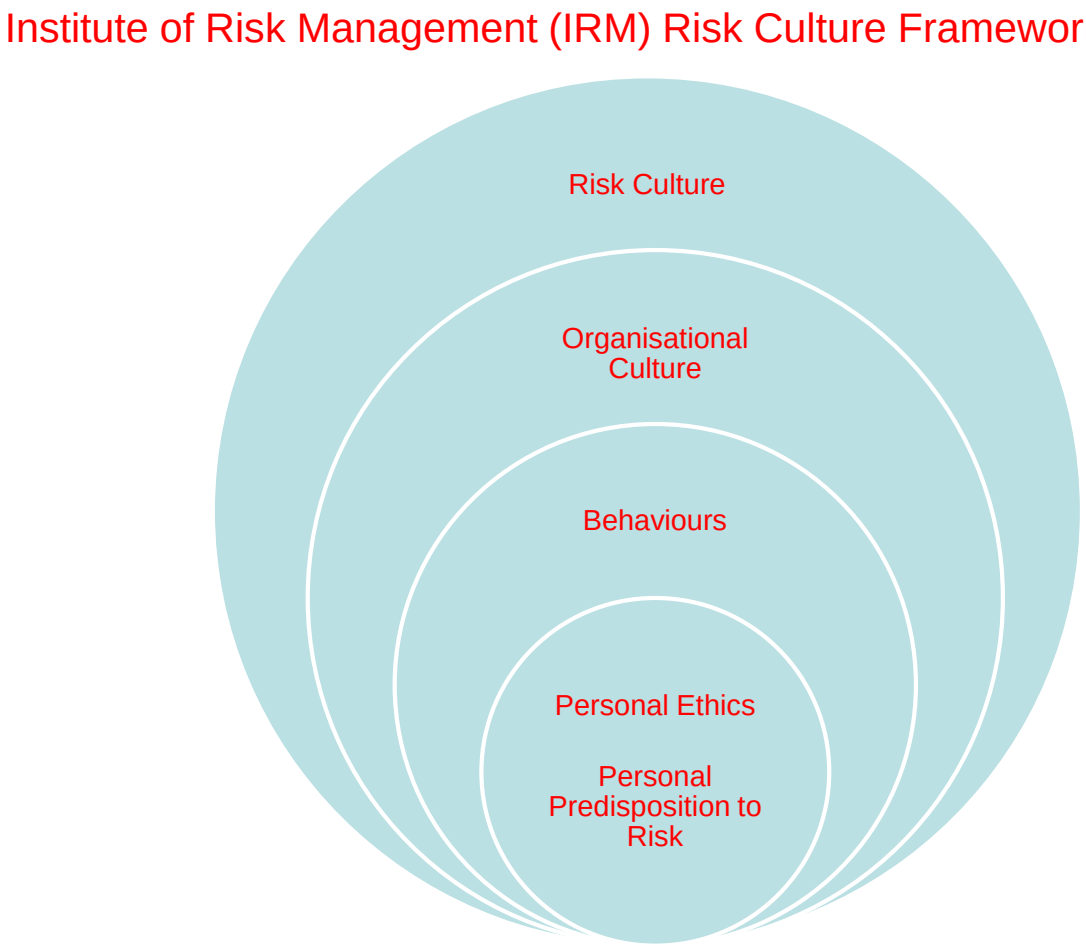

Figure 6: Institute of Risk Management Risk Culture Framework

A range of diagnostic tools are available to indicate and track the components described within the framework above. In our experience however such is the poor state of risk maturity in very many organisations that they are not sufficiently advanced to practically determine how they might chart a course from the existing to the target state of risk culture.

In 2011 the Financial Reporting Council produced the report: Boards and Risk: A Summary of Discussions with Companies, Investors and Advisors. In the section on Risk and Control Culture it said:

- It was recognised that risk and control culture was one of the issues on which it was most difficult for boards to get assurance, although boards appeared to be making more efforts to do so…

- The risk management and internal audit functions could play an important role, as could reports from and discussions with senior management, but some directors felt that there was no substitute for going on to the ,shop floor and seeing for themselves. It was otherwise very difficult to judge whether risk awareness was truly embedded or whether it was seen as a compliance exercise. This in turn assumed that non-executive directors had a sufficient understanding of the business, which some participants noted may not always be the case,

- One common approach was to ensure that responsibility for managing specific risks was clearly allocated to individuals at all levels of the organisation, and their performance was measured and reflected in how they were rewarded,

- In some companies the Remuneration Committee had been given responsibility for considering how to align the company's approach to risk and control with its remuneration and incentives. Examples were also given of the head of the risk management or internal audit function submitting reports to that committee, for example on how the company was performing against certain key risks, or being invited to comment on the details of proposed incentive schemes.

More recently the FSB In its Peer Review Report on Risk Governance, published in February 2013, identified ''business conduct'' as a new risk category and said *''One of the key lessons from the crisis (GFC) was that reputational risk was severely underestimated; hence, there is more focus on business conduct and the suitability of products, e.g., the type of products sold and to whom they are sold. As the crisis showed, consumer products such as residential mortgage loans could become a source of financial instability."* In consulting and developing guidance for regulators the FSB emphasizes the importance of risk culture as a principal influencer reducing the risk of mis-selling financial services products which can end up in the wrong hands with detrimental prospects for consumers[37] in particular and society in general. Clearly conduct risk is systemic in nature, and inherently so with considered in the context of big data; that is to say it is very unlikely to exist in isolation within an organisation.

Separately the FSB has articulated what it considers to be the foundation elements of a strong risk culture in its publications on risk governance, Risk Appetite and compensation. It has broken down the indicators into four parts which need to be considered collectively, and as mutually reinforcing, and has made it clear that looking at each indicator in isolation will ignore the multi-faceted nature of risk culture. The four parts[38] are:

1. ***Tone from the top***: The board of directors and senior managers are the starting point for setting the financial institution's core values and risk culture, and their behaviour must reflect the values being espoused. The leadership of the institution should systematically develop, monitor and assess the culture of the financial institution,

2. ***Accountability***: Successful risk management requires employees at all levels to understand the core values of the institution's risk culture and its approach to risk, be capable of performing their prescribed roles and be aware that they are held accountable for their actions in relation to the institution's risk-taking behaviour. Staff acceptance of risk-related goals and related values is seen as essential,

3. ***Effective challenge***: A sound risk culture promotes an environment of effective challenge in which decision-making processes promote a range of views, allow for testing of current practices and stimulate

a positive, critical attitude among employees and an environment of open and constructive engagement,

4. ***Incentives***: Performance and talent management should encourage and reinforce maintenance of the financial institution's desired risk management behaviour. Financial and non-financial incentives should support the core values and risk culture at all levels of the financial institution.

Clearly there is consistency in thinking as to the importance of risk culture, and its core attributes. Monitoring risk culture is however very challenging indeed. To the particular question of communicating risk culture to stakeholders we question whether this can be done credibly in the absence of finding proxies for attitudes and behaviors described in the ABC risk culture building blocks described above?

Our experience tells us that risk maturity capability requirements are today well understood, reliable and credible proxies for risk culture. On this basis we recommend that organisations are best advised to travel the better known road of 'risk maturity' for which there are a number of capability maturity models in existence.

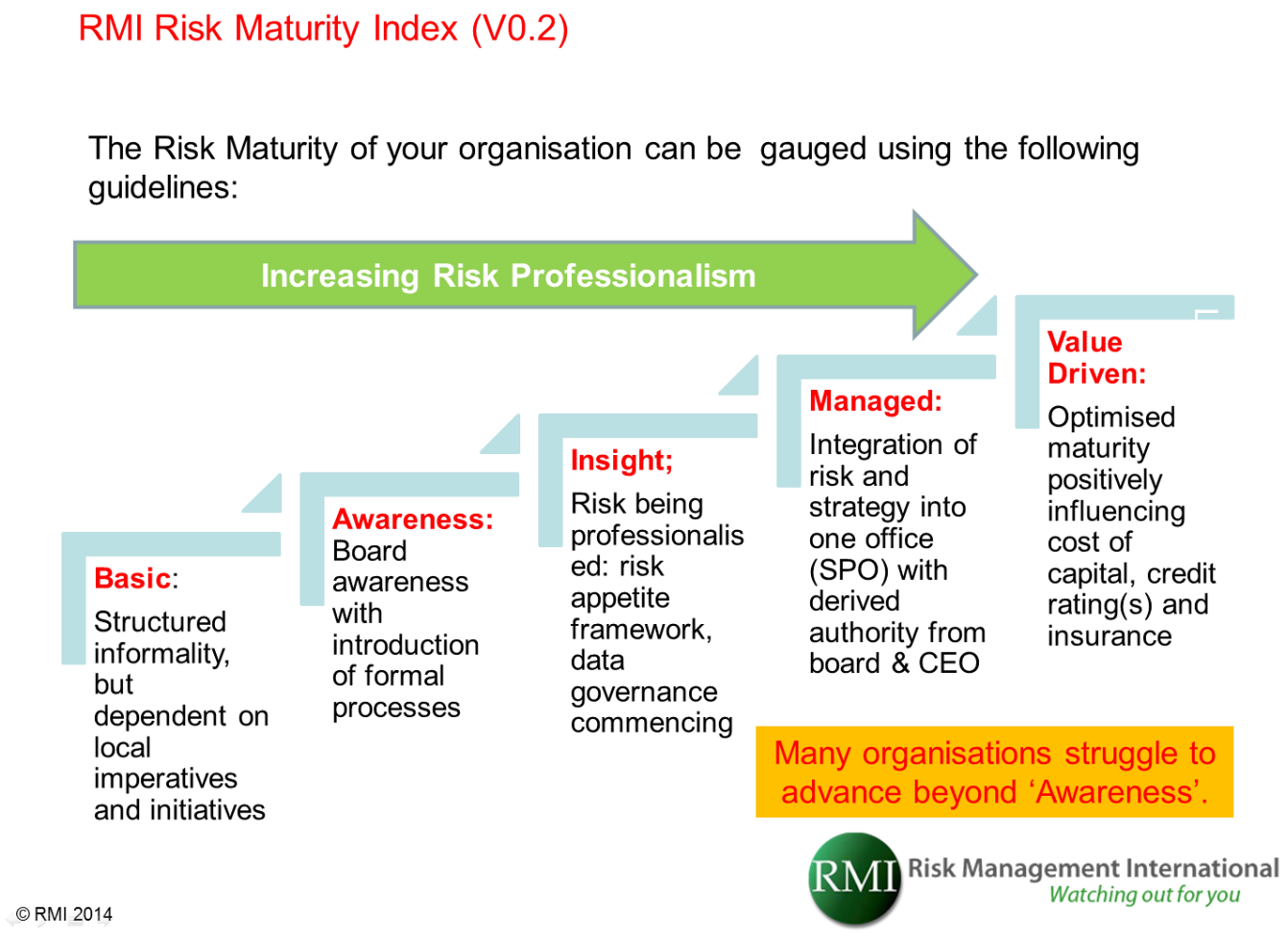

Figure 7: RMI Risk Maturity Matrix

We believe there to be a demonstrably credible correlation between full maturity (RMI Risk Maturity Index 'Value Driven' Optimising Value though aligning risk and strategy with corporate objectives) and board ownership of the Risk Appetite framework, building resilience (defending operations, business model and reputation) and risk culture.

The RMI Risk Maturity Index correlates:

1. Level of Alignment of Risks to Strategy, Objectives and Execution,
2. Risk Role Affirmations at each Maturity Level,
3. Risk Culture Affirmations (practices confirmed by internal and external attestors),
4. Risk Defence Affirmations (practices confirmed by internal and external attestors),
5. Board and Organisational Processes, and
6. Value Realised at three levels:
    a. The Investor,
    b. The Organisation, and
    c. Stakeholders.

Progression from one level to the next requires a blend of internal and external independent attestations which are facilitated with the aid of a database containing structured question sets for use by attestors.

Risk maturity scores are weighted according to the:

1. Quality of answers provided to questions,
2. Availability of demonstrably credible evidence supporting answers,
3. Rigor and consistency of risk data,

No more than it is difficult, if not impossible; to dupe psychometric testing we believe that risk maturity attestation by seasoned practitioners' will provide 'evidence based assurance' as to organisational risk culture.

Some additional Observations

The Central Bank has suggested characteristics of an effective Risk Appetite statement. How would you improve this?

The purpose of a Risk Appetite Statement (RAS) is to provide clear guidance to people, at all levels, of the acceptable ranges of risk within which they are required to operate in pursuit of objectives.

A RAS exists within a Risk Appetite Framework (RAF).

The RAF is the ''overall approach including the policies, controls and systems, through which Risk Appetite is established, communicated and monitored''[39]

As a particular RAS is devolved down through an organisation its content will change relative to the intended recipients. For example a RAS at:

- Group Executive level will be high level in nature and inclined towards expressing appetite for risks to objectives which are required to deliver value and increase performance. They will describe objectives, risks, expected returns and control(s) requirements,

- Middle management level will articulate levels of tolerance which if breached will require escalation and 'circuit breaking' reports with priority attention given to immediate interdictions and a review of internal controls,

- Business unit level will be more detailed and inclined towards expressing risk limits and internal controls.

A RAS which is not explicit and clearly communicated has limited value.

For this reason a RAS exists within a compendium of (Risk Appetite) statements which take their root at the intersection between a particular group level objective and its associated subsidiary objective(s).

The RAF, like the strategic plan, is explictly approved by the board. Properly crafted and implemented it has powerful value and utility to directors in that the RAS approval process requires a *series of linear RAF discussions.* Wisely conducted these discussions can result in a pealing back of the many layers of complexity associated with operational drivers and the business model. Independent non executive directors (INEDs) in particular, can find this immensely useful as most INEDs will typically only possess a relatively superficial understanding of the principal operational exigiencies which drive performance.

The RAF Discussions will include discussions on:

1. Explictly stated objectives[40] and where they reside on the Risk Appetite continuum,

2. The associated subsidiary objectives[41], and where they reside on the Risk Appetite continuum,

3. First RAS drafts at group and subsidiary levels,

4. RAS approvals once operational and business model implications are fully understood and satisfied.

RAF Template Headings:

RMI offers frequently used headings which we use in helping organisations develop their Risk Appetite Frameworks (RAF).

1. Mission/Purpose/Mandate:
    a. Plcs' and large privately held companies will have clearly established and communicated mission statements etc.
    b. For a large number of regulated entities in Ireland this will reflect the subsidiary goal set by the parent for the subsidiary,
    c. For Public Companies this will be reflected in the legislation establishing the entity,
2. Strategic Initiatives:
    a. Very many organisations will not have a board approved 10-15 year strategic plans. Rather they will have business plans wihtin which various strategic initiatives are either implied or explicitly stated,
    b. The development of a strategic plan is outside of the scope of a RAF, however each document informs the other,
3. Board (Risk Committee) Statement of Risk Assurance Requirements: This is a prescriptive statement addressing a wide range of requirements, and would include the following among others:,
    a. Objectives that are clearly articulated, aligned with strategy and performing to expectations,
    b. Risks to objectives that are identified, assessed and evaluated against approved risk criteria,
    c. Risk Treatment Plans that are executed efficiently and effectively, and the likelihood of achieving objectives thus increased,
4. Objectives: As discussed above,
5. Risk Appetite Continuum: Five level continuum against which company (Group and Subsidiary) objectives are mapped relative to appetites for risk (from very high to very low)
6. Risk Appetite Statements:
    a. Overall Group RAS
    b. Objectives Level RASs'
    c. Risk Treatment Level RASs'[42]
7. Risk Criteria Tables (Risk Tolerances and Limits)
    a. Five levels (Substantial down to negligable impacts),
    b. Measurable risk limits[43]
    c. Measurable risk tolerances.

How can organisations ensure that Risk Appetite Frameworks are both actionable and measurable?

The RAF is to the board of directors what Risk Management is to the rest of the organisation.

As such there is a direct correlation between the efficacy of the RAF and the efficacy of the Risk Management Framework.

On this basis ensuring that Risk Appetite Frameworks are both actionable and measurable requires an understanding of how boards work in this particular context.

When RMI converses with board members and the executive we share with them what we call the RMI Tell me, Show me, Prove it to me questions.

Questions will vary from company to company, however broad results in terms of an informal scoring which we would thereafter apply, do not vary greatly.

For example:

- Tell me: (Score: 9/10)
    - How you relate your strategic plan to critical objectives and their associated KPIs,
    - About your board audit/risk charter,
    - Risk management framework.

  We are told about external attestation (sometimes exemplary), policies, board committees and rich processes.

- Show me: (Score: 5/10)
    - Your strategic plan / objectives statements,
    - Your risk register and how it links to objectives, KPIs and threats/risks to the enterprise,
    - Your Risk Appetite statements,
    - Your risk treatment plans,
    - Your top 5 contingency plans.

  We find that most of these documents do not always exist and that the excel spread sheets, word documents and Power Points (invariably with differing formats for different parts of the organisation) make no consistent reference to objectives, other than obliquely. In addition we find that original risk reports are edited on multiple occasions as they travel from original risk owners to the executive and the Board.

- Prove to me that: (Score: 2/10)
    - Your risk register is not just a list of risks,
    - Top 10 risks are the real top 10,
    - Risk owners actually input to the flow of information and ultimately to the risk register,
    - Known issues and risks on the ground can be escalated to decision makers, without jeopardy to the originators of information,
    - Dynamic risks can be aggregated in real time and with confidence because of your data governance practices,
    - Your crisis management team (CMT)[44] is developed and capable.

We find that risk data governance is so poor that answers to these questions can only be determined after manual searches over a number of days. This is compounded when invariably we also find that managers have not been adequately trained in the use of common language, risk management processes, or board risk assurance requirements. Furthermore we find that ''risk culture'' is such that people are un-inclined to speak up with regard to matters giving them cause for concern lest they jeopardise relationships' with colleagues and their next reports.

We therefore recommend that fundamental questions for the CEO and INEDS should include:

1. What demonstrable evidence do you have that your top 5 Group Risks are the right Top 5?
2. Can you monitor threats and risks to objectives in real time and what kind of dynamic tests can you run on your red flags?
3. What proofs do you have that management is capable from switching from
    a. Business as Usual, to
    b. Delivery of credible solutions to stakeholders under Abnormal/Adverse conditions?
4. Where are you in terms of risk maturity, and how do you know?

RMI also recommends the following framework which summarises how to ''Operationalise the links between Risk and Strategy'' thus ensuring that RAFs are measurable and actionable.

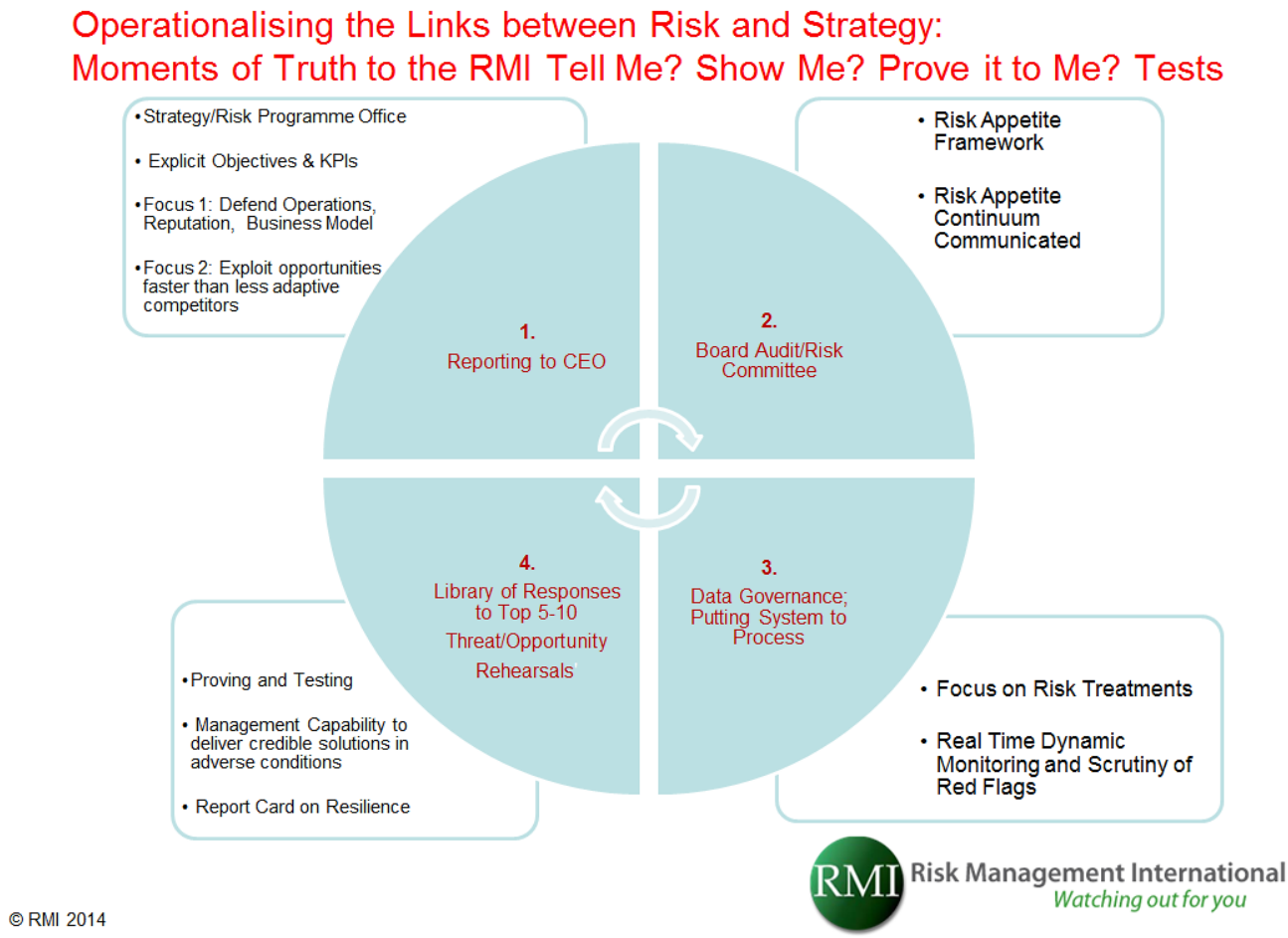

Figure 8: RMI 4 step Framework for Operationalising Risk/Strategy

The Framework is summarised as follows:

1. Reporting to the CEO:

   Strategy/Risk Programme Office reporting to the CEO and Board Audit/Risk Committee as described earlier in this paper with:

   - Focus 1: Defend Operations, Reputation, Business Model,
   - Focus 2: Exploit opportunities faster than less adaptive competitors.

2. Board Audit/Risk Committee:

   Executing responsibilities with regard to risk in the manner described earlier in this paper and in particular as described in the RMI answer to the question: *The Central Bank has suggested characteristics of an effective Risk Appetite statement. How would you improve this?*

3. Data Governance: Putting System to Process:

   Understanding the significance of integrating:

   - Executive and Management (Risk) Training;
   - Inclusion of Risk Management KPIs in annual appraisals, and
   - Deployment of a database solution designed and specified to the ISO 31000 series

   Note: Lessons learned from the Global Financial Crisis include that of database solutions, of themselves, not being the solution. The adage 'poor information input, misinformation output' is appropriate and reminds us that tools and techniques in the wrong hands can precipitate disastrous consequences.

4. Library of Responses to Top 5-10 Threat/Opportunity Rehearsals

   Seminal works which have been undertaken include:

   - 1996: The Impact of Catastrophes on Shareholder Value: Rory F. Knight & Deborah J. Pretty, THE OXFORD EXECUTIVE RESEARCH BRIEFINGS, Templeton College, University of Oxford, Oxford OX1 5NY, England[45].

     Conclusions:

     - Recoverers and Non-Recoverers are discernible in first 10-50 days
     - Direct Factors:
       - Cash, Fatalities, Management Responsibility, Management Talent
     - Indirect Factors:
       - Management skills hitherto not reflected in Value
     - Indirect factors, more so than direct factors, determine which companies recover, and which companies do not recover.

   - AIRMIC[46]
     i. 2011: Roads to Ruin
     ii. 2014: Roads to Resilience

     Conclusions:

     What contributed to catastrophic failure?

     - Poor crisis management,
     - Failure to recognise the significance of the event early enough in the crisis,
     - Poor stakeholder communications, including with news and social media,
     - Lack of awareness of the potential for reputational damage,
     - Failure to appreciate the importance of transparency early enough,
     - Failure to learn from prior experience (even with the same company).

Resilient Companies:

- Have exceptional Risk Radar,
- Build effective internal and external networks,
- Review and adapt based on excellent communications,
- Have the ability to respond rapidly and flexibly,
- Have diversified resources.

These separate and unrelated studies similarly conclude that management's capability to defend operations, the business model and reputation are mission critical to sustainable performance in the 21st century

In conclusion it is our view that operationalising the links between risk and strategy in the manner outlined above will, with positive CEO and Board endorsement, have the effect of fulfilling the Role of the Board as concluded by the Financial Reporting Council (FRC) report: Boards and Risk: A Summary of Discussions with Companies, Investors and Advisors, Sept 2011…RMI representation in figure 9 below:

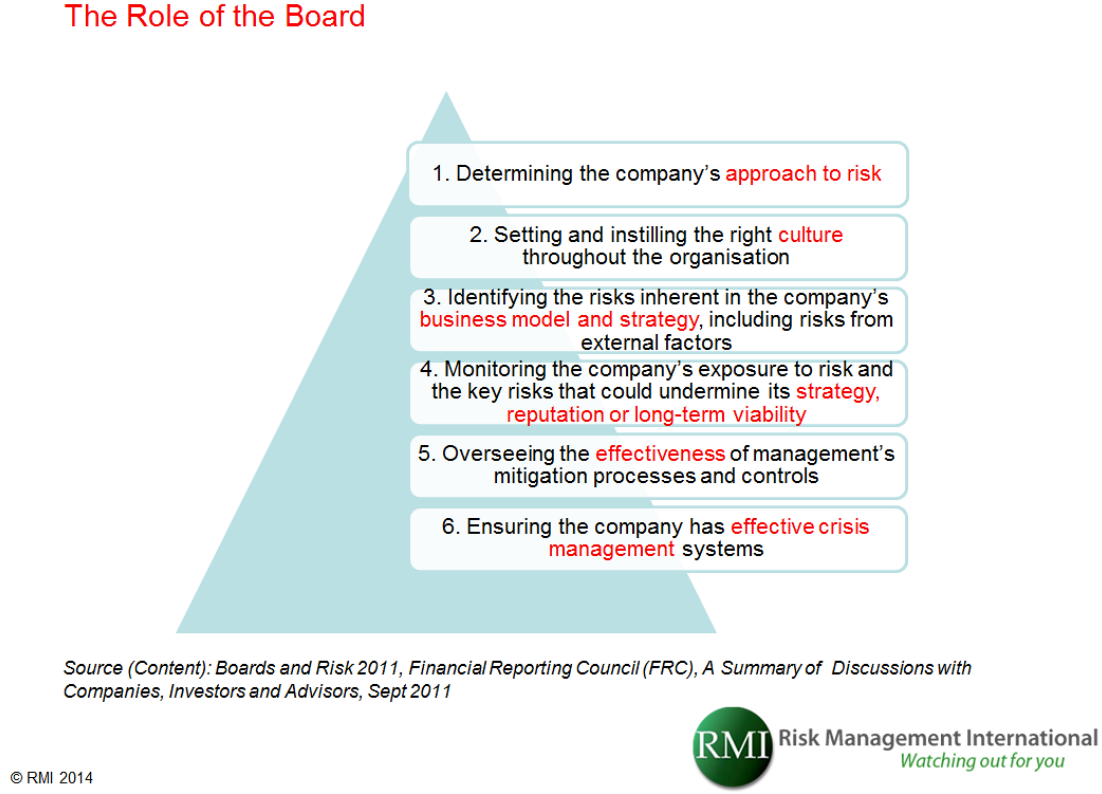

Figure 9: The role of the Board

References

[1] Source: Harvard Law School Forum on Corporate Governance and Financial Regulation: Strategic Risk Management: A Primer for Directors Aug 2012

[2] The RAF is the ''overall approach including the policies, controls and systems, through which Risk Appetite is established, communicated and monitored''

[3] Risk management: coordinated activities to direct and control an organisation with regard to risk Source: ISO Guide 73 Risk Management - Vocabulary

[4] Risk management framework: set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization

- NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk.
- NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
- NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

(Source: ISO Guide 73 risk management vocabulary)

[5] Influenced by COSO (Committee of Sponsoring Organizations of The Threadway Commission, Enterprise Risk Management (ERM) Understanding and Communicating Risk Appetite by Dr. Larry Rittenberg and Frank Martens

[6] Source ISO 31000 (Risk Management 2009). ISO 31000 is now the globally accepted risk management standard.

[7] The new globally accepted risk management standard (ISO 31000) is not intended for the purposes of certification. Rather it contains guidance as to risk management principles, a framework and risk management process which can be applied to any organisation, part of an organisation or project etc. As such it provides an overarching context for the application of domain specific risk standards and regulations for example Solvency II, environmental risk, CSR, supply chain risks etc.

[8] Risk Communication Aligning the Board and C-Suite: Exhibit 1 Top Challenges of Board and Management Risk Communication *by Association for Financial Professionals (AFP), the National Association of Corporate Directors (NACD), and Oliver Wyman*

[9] The Conference Board Governance Centre, Risk Oversight: Evolving Expectations of Board by Parveen P. Gupta and Tim J Leech

[10] A known unknown risk is one which is known, and understood, at one level (e.g. typically top, middle, lower level management) in an organisation but not known at the leadership and governance levels (i.e. executive and board levels)

[11] An unknown unknown risk is a so called black swan (The Black Swan: The Impact of The Highly Improbable, Naasim Nicholas Taleb)

[12] Specified to the ISO 31000 series

[13] Source ISO 31000 (Risk Management 2009). ISO 31000 is now the globally accepted risk management standard.

[14] More than 80 percent of volatility in earnings and financial results comes from the top 10 to 15 high-impact risks facing a company: Risk Communication Aligning the Board and C-Suite: *by the Association for Financial Professionals (AFP), the National Association of Corporate Directors (NACD), and Oliver Wyman*

[15] Source Institute of Management Accountants, Statements on Management Accounting, Enterprise Risk Management : Frameworks, Elements and Integration
[16] Managing Risks: A New Framework
[17] Kaplan and Mikes third category of risk is termed "external" risks, but the Global Risk 2013 report refers to them as "global risks"… *they are complex and go beyond a company's scope to manage and mitigate (i.e. they are exogenous in nature).*
[18] Audit and Risk, *21 July 2014* Matt Taylor, Protiviti UK,
[19] The Financial Reporting Council has determined that it will integrate its current guidance on going concern and risk management and internal control, and to make some associated revisions to the UK Corporate Governance Code (expected in 2014). It is expected that emphasis will be placed on the board making a robust assessment of the principal risks to the company's business model and ability to deliver its strategy, including solvency and liquidity risks. In making that assessment the board will be expected to consider the likelihood and impact of these risks materialising in the short and longer term;

[20] Strategy Formulation is not part of the development of Risk Appetite Frameworks however each is intrinsic to, and informs, the other.
[21] IIA Position Paper: The Three Lines of Defense in effective Risk Management and Internal Control January 2013
[22] Board Risk Oversight, A Progress Report: Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities (Protiviti Report commissioned by COSO (Committee of Sponsoring Organisations of The Threadway Commission))
[23] NOTE: Risk Management and the Strategy Execution System By Robert S. Kaplan which advances a method and Aligning Enterprise Risk Management with Strategy Through the Balanced Scorecard

[24] Effective reporting and monitoring of risk treatments delivers the twin benefits of 1) monitoring risk performance, and 2) establishing leading indicators on the future state of health of objectives
[25] Crisis is defined as: *An inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organization*: PAS 200:2011 Crisis Management – Guidance and Good Practice, UK Cabinet Office in partnership with the British Standards Institute
[26] Reference Kaplan, Mikes Level 1 Global Enterprise Risks,
[27] Mc Kinsey&Company, August 2014, Why Implementation Matters: Good implementers—defined as companies where respondents reported top-quartile scores for their implementation capabilities—are 4.7 times more likely than those at the bottom-quartile companies to say they ran successful change efforts over the past five years. Respondents at the good implementers also score their companies around 30 percent higher on a series of financial performance indexes. Perhaps most important, the good-implementer respondents say their companies sustained twice the value from their prioritized opportunities two years after the change efforts ended, compared with those at poor implementers

[28] Functionally designed and specified to meet the ISO 31000 series
[29] Institute of Risk Management (IRM) , Risk Culture, Under the Microscope: Guidance for Boards
[30] Speak up/Stand up/Ethics Line/Whistleblower Lines etc.
[31] Strategic Risk is defined by the Committee of European Banking Supervisors (CEBS) as "the current or prospective risk to earnings and capital arising from changes in the business environment and from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment".
[32] Operational risk is defined by the Basel Committee as "the risk of loss resulting from inadequate or failed business processes, people and systems or from external events".
[33] Within the parameters of Competition Legislation and similar in construct to the Irish Bankers Forum High Tech Crime Forum,
[34] In addition to the current stress testing regime particular emphasis would be placed on major operational (emerging and external risks, particularly cyber/digital/IT security etc.) and strategic (poor risk culture, leadership etc.) risks
[35] RMI Risk Maturity Index Level 5

[36] Institute of Risk Management (IRM) , Risk Culture, Under the Microscope: Guidance for Boards
[37] In March 2014 the Financial Conduct Authority fined JP Morgan's UK wealth management business £3.1 million for failing to keep complete and up-to-date information on client objectives, risk profile and Risk Appetite placing them at risk of receiving inappropriate investment advice. This example is particularly interesting because it was not related to human failure or a failure of controls alone. Instead, the regulator argued that the firms' computer systems did not allow sufficient client information to be retained. This is indicative of the way in which narrow definitions of conduct risk cannot be taken at face value or viewed independently. Source: Banking Technology 26 Aug 2014.
[38] Reuters: Financial Regulatory Forum, Conduct Risk An Overview, 19th March 2014
[39] http://www.financialstabilityboard.org/publications/r_131118.htm.
[40] Strategic plans and business plans without explicitly stated objectives have no meaning
[41] Theoretically objectives are devolved from Group to subsidiary boards. In reality what happens is that group and subsidiary executives and directors (the latter through respective Risk Committees) engage in operational discussions directed at ensuring understanding thus increasing likelihood of success.
[42] Properly constructed Risk Treatments are the leading indicators of the future state of health of objectives. As such risk treatments are at the cutting edge of the management of risks to objectives.
[43] Dr Peter Drucker '' if it can't be measured it can't be managed'. As with determination of leading indicators in balanced score cards, these can often be difficult to establish.
[44] CMTs are activated when issues and events which threaten to overpower operations, the business model and/or reputation arise/occur.
[45] Reference Oxford Metrica: deborahpretty@oxfordmetrica.com
[46] Reference AIRMIC CEO John Hurrell