LinkRes

A LEADER IN ENTERPRISE RISK MANAGEMENT

Response to the Central Bank's Discussion Paper

on

Risk Appetite

September 1st 2014

Contents

Author: Gerard Joyce

Director, LinkResQ

Chairman, Risk Management Consultative Committee (NSAI)

About this Document

This document was written is response to the Central Bank of Ireland's Discussion Paper entitled "Risk appetite". The views expressed in this response are the personal views of the author and are based on his own experiences and from engagement with risk experts from around the world.

The document is divided into 3 main sections:

1 General Observations

2 Replies to Questions Posed

3 Putting Risk Appetite into Context

Author

Gerard Joyce is the principal author of this document. He has over 30 years of experience working in several organisations (large and small) in the ICT sector. Gerard has worked exclusively in risk management for the past 8 years. He is Chairman of the Risk Management Consultative Committee in the NSAI (National Standards Authority of Ireland) and Head of Delegation, representing Ireland on the ISO (International Standards Organisation) Technical Committee on Risk Management (TC 262). He is also a founding director of LinkResQ, a company dedicated to developing tools to enable the effective management of risk. He can be contacted at gjoyce@linkresq.ie. Contributions also from Paul O'Brien, MD, and Chris Hanlon, Product Manager, at LinkResQ.

1 General Observations

This section contains comments on risk management from a global perspective as well as specific comments on the content of the discussion paper.

1.1 Broad Perspective

The management of risk is topical at the moment because of perceived failures in the past leading to the global financial crisis. What has become clear is that many of the failures were due to organisations taking on too much risk, way beyond their capacity (to bear risk) and without due regard to the potential downside consequences.

Corporate governance codes around the world have been updated to place greater emphasis on the board's role in ensuring effective risk management. The UK corporate governance code states: "*The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives.*" There are two key messages here; the board is responsible and the board must determine the organisation's "risk appetite". Without well-defined, unambiguous guidance from the board the amount of risk assumed by the organisation will be dictated by the risk perception of individuals.

The ISO 31000:2009 risk management standard does not specifically mention risk appetite but it does suggest that organisations define "Risk Criteria"; "*the terms of reference against which the significance of risk is evaluated*". For many risk experts this is a preferable approach, criteria can be specific to the context and/or related to organisational objectives / project objectives. It is the author's opinion that a high level risk appetite statement supported by a strong set of risk criteria will ensure that both the philosophy and the strict limits, that define overall appetite, are better communicated throughout the organisation.

1.2 Discussion Paper Observations

While it is clear that any discussion paper is not the "final cut" and inconsistencies, errors and need for greater clarification are to be expected, I felt it might be useful to the discussion to highlight some of these at this stage.

I. Section 2 defines the RAF as the "*overall approach, including policies, controls and systems, through which risk appetite is established, communicated and monitored*". While is section 3.2.1 it states that "*The articulation of a clear and meaningful risk appetite is a key step in the establishment of any RAF*" I would suggest that the risk appetite statement is an outcome of the framework / process and phrase section 3.2.1 accordingly.

II. Ref: Sec 3.2.3. The understanding of Risk Tolerance is already confused and this section adds to that confusion. Whereas I consider the introduction of the concept of a lower limit (to ensure sufficient risk is taken) novel and interesting, the idea needs further development if it is to be part of a coherent RAF. Most of the discussion around risk limits after this introduction are exclusively around the upper limit or threshold. Fig 2 does not deal with the "lower tolerance point"

III. Ref: Sec 3.2.4. Breaching limits. If going above a limit (but below the upper tolerance) is "yellow alert" what colour is the area below the limit but above the lower tolerance? Green? And what colour is the position below the lower tolerance? Red or yellow? I think this section needs more consideration if risk limits are to become a fundamental element of the risk appetite statement.

IV. Ref: Sec 3.2.6. Diagram is flawed. Greater risk does not mean greater return and lower risk does not mean that there will be no loss! I would suggest that a diagram similar to the one shown below more closely resembles the relationship between risk and return (/loss)

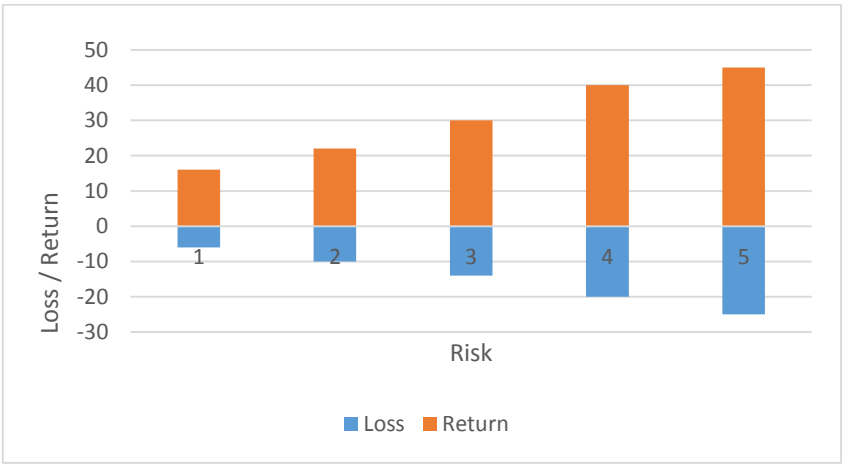


Fig (i) Risk Return / Loss Relationship

V. Ref: Sec 4.1. Risk Culture. Last sentence: "When assessing the RAF of an organisation one should question 'whether the end justifies the means'. I disagree, I think one should question whether the means risks too much!

VI. Ref: Sec 4.3. Setting accountability. In an effective risk culture individuals will not be "encountering a potential risk" they will be actively identifying, analysing and mitigating risks.

VII. Ref Sec 4.3. Why introduce the concept of "material risks" here? Why limit responsibilities to just material risks? I think the important issue pertaining to "material risks" is how the board will respond. Do they have a process / plan to address these?

VIII. Ref: Sec 5.1. Expressing risk appetite. Last paragraph states that "the RAS needs to be simple and understandable by all", I agree, but if the guidance is to be followed as it stands I feel that the RAS will be neither "simple" nor "understandable" unless the nature, scale and complexity of the organisation is correspondingly simple. Please also see section "Putting Risk Appetite into Context" below.

IX. Definitions. As per the FSB document, I would recommend the inclusion of a section with "Key Definitions". It is important that key concepts are defined and their use is consistent. A defined list would help in this regard. I would also suggest the inclusion of some definitions of additional risk terms as describe in ISO's Guide 73 (Risk Management vocabulary) .e.g

a. Risk is the effect of uncertainty on [the achievement of] objectives
b. Risk Criteria the terms of reference against which the significance of a risk is evaluated

2 Replies to Questions Posed

Q1. Should all organisations have a risk appetite framework? Please explain your answer.

A1. The short answer is "Yes". However a RAF that is not an integral part of an organisation's risk management framework will be ineffective.

"*The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels.*" [ISO 31000:2009] Risk appetite is a key element of the risk management system and the approach, policies, controls and systems through which it is established must be embedded in the firm-wide framework for the management of risk.

The framework for the management of risk ensures that information about risks is adequately reported and available to those decision-makers who need it. It also ensures that appropriate resources are dedicated to skills development, risk assessment and on-going monitoring of risks. It specifically addresses the important alignment of the risk management activity with the strategic objectives of the organisation. The risk appetite statement is that critical link between the stated vision and objectives for the organisation and the boundaries within which management should operate.

Q2. How are risk appetite and strategy related?

A2. ISO Guide 73:2009 Risk Management Vocabulary defines risk appetite as "*amount and type of risk that an organisation is willing to pursue or retain*". This must be defined and approved and the highest level of an organisation. For each strategic objective that the organisation has stated it should also articulate how much risk it is willing to accept in pursuit of that objective. This "appetite statement" will inform the strategy employed to attain the objective. For some objectives it is conceivable that an organisation may be very conservative and take little risk, whereas with other objectives it may be prepared to accept uncertain outcomes.

The primacy of objectives will also impact strategy and this can be best articulated in the risk appetite statement(s). Statements that clearly articulate the motivations for taking or avoiding certain types of risks will inform strategic decision-making.

Q3. In your opinion would it be desirable for the Central Bank 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?

A3. No, I do not think a Central Bank facilitated forum would be desirable. My concern is that if a regulatory body were to be the leader in such a forum then whatever might be agreed would become the "standard" answer. I could foresee generic risk appetite statements becoming the norm and that would be a retrograde step. As chairman of the Irish Risk Management Consultative Committee in the NSAI, I would be happy to engage with the CB to discuss how our committee of experts might support or be the vehicle to facilitate a discussion on best practice.

Q4. What definition of risk appetite does your organisation consider to be appropriate?

A4. The most simple and straightforward definition, as defined in the ISO Guide 73:2009 Risk Management Vocabulary, the "*amount and type of risk that an organisation is willing to pursue or retain*".

Q5. In your view, how are risk appetite, risk tolerance and risk limits related to one another?

A5. The use of the term "risk tolerance" suffers from too many definitions that are inconsistent with each other and only add confusion to the debate. In the interest of simplicity I suggest that this term is not used and instead only use: risk appetite; risk limits; and risk capacity.

Risk appetite is the expression at the highest level in the organisation of the amount and type of risk that the organisation is willing to accept. It is an expression of the philosophy and ethos of an organisation and, when well-articulated, will guide management at all levels in their decision making. Risk appetite will be chiefly "qualitative" in nature, but may include some high-level quantitative values or limits.

Risk limits are required at multiple levels in an organisation. These represent the disaggregation of the overall appetite and are necessary if individual managers are to fully understand their decision making constraints. These can be expressed in many ways and units of measure, capital reserves, liquidity, investment concentration, maximum loan size, etc.

Risk capacity as defined in the discussion paper (Sec 3.2.2) is a useful term and I recommend the retention of this term and its definition. It is absolutely imperative that the board and management know where the edge of the cliff is and guide the organisation in a prudent way within its "capacity".

Q6. How does your organisation facilitate early warning reporting of potential breaches of risk appetite?

A6. I suggest looking to the aviation industry for inspiration in how "early warning reporting" might be best achieved. In the belief that the majority of breaches or risk appetite will be unintentional it is key to success that a "just culture" reporting environment is attained. Much research has been conducted into human error, its causes and what can be done to prevent it. Accepting that human error is inevitable is the first step. Putting in systems and "detection aids" that record and report on deviations from the expected is fundamental to effective risk management.

Simple and comprehensive recording and reporting of all near misses, incidents, issues and whatever other terms are used to describe deviations from the expected, should be embedded in the management system of the organisation. It is important that these reports and in particular trends are reviewed and acted upon. Continuous improvement in the management of risk will only come from recognising and responding to deviations from the expected.

Q7. The Central Bank has suggested characteristics of an effective risk appetite statement. How would you improve this?

A7. Any expression of risk appetite must be in the context of the strategic objectives of the organisation. For each stated objective it is important to define the desirable and undesirable risks, the avoidable and unavoidable risks and how these risks will be managed.

I would include some aggregated risk limits, but keep these to a minimum. Detailed, disaggregated risk limits may be included, but this would be best executed at the point of communication to the various business units.

I would not include many of the items suggested in section 5.1, I think these are important and more appropriately belong in a risk management policy document.

I would aim for "brevity and clarity".

Q8. How does your organisation determine the metrics that are most appropriate for your business? (in the context of risk appetite)

A8. We employ a methodology that asks the simple question: "What matters?". Is it people, profit, reputation, service, customers, etc? We seek agreement on 5 "What Matters" and these then form the basis for the types of consequences that are used to characterise the level of risk. We verify that the chosen "What Matters" are aligned with the stated objectives and then proceed to identify how the magnitude of consequence can be best described on a scale of 1-5. We also define a Likelihood scale of 1-5 and use the combination of Likelihood and Consequence to determine the overall level of risk. The outcome from this process is a definition of the "Risk Criteria", the terms of reference against which the significance of risk is evaluated. See section "Risk Criteria" under "Putting Risk Appetite into Context".

Q9. How does your organisation assess risk culture?

A9. There is a lot of useful research and reports on risk culture that I would recommend to the Central Bank, in particular the Institute or Risk Management (IRM, London) and the Risk Management Society (RIMS, New York) have publications that discuss aspects of a healthy risk culture and a risk management maturity model. See: http://www.theirm.org and http://www.rims.org

I see Risk Culture as a sub-set of organisational culture and an outcome of the policies, procedures and practices relating to the management of risk. It is hugely influenced by the "tone from the top" and if that is good then risks will be consistently well managed but if it is bad the risk management will be ineffective.

What does a good Risk Culture look like? (extract from IRM, Risk Culture 2012)

- A distinct and consistent tone from the top
- A commitment to ethical principles
- An acceptance of the importance of the management of risk
- Transparent and timely risk reporting
- Actively seeking to learn from mistakes
- Good behaviour rewarded, inappropriate risk taking sanctioned
- Risk management skills continuously developed

3 Putting Risk Appetite into Context

3.1 Introduction

Is this section I want to take a step back and consider the context in which the appetite is developed and implemented. Organisations differ in nature, size, complexity and objectives and so their appetite for risk will also differ. The risks they face and the choices they have will also differ, so no two risk appetite statements will ever by the same. If a regulator of a significant sector is seen to be prescribing what should and should not be in an appetite statement, I fear that its usefulness will be diminished. The audience for the risk appetite statement is primarily the decision-makers in the organisation who need the guidance to ensure consistency and alignment with objectives.

The International Standards Organisation (ISO) published a standard on risk management in 2009. (31000:2009) This standard is not a requirements standard but one that describes principles and guidelines that, if followed, will make risk management effective. The standard contains 3 key clauses; principles, framework and process. I would like to suggest that the concepts of defining a risk appetite framework (RAF) and risk appetite statement (RAS) are already addressed as part of the framework for managing risk and the process as described in the standard. The remainder of this section describes the key elements in the framework and process that would facilitate the objective of developing an appropriate "risk appetite" for the organisation.

3.2 Establishing the Context

Section 4.3.1 of the standard is entitled "Understanding of the organisation and its context". This is about understanding both the external and internal context. External context looks at the social, cultural, regulatory, technological, economic, et al, aspects of the environment in which the organisation is operating. Relationships, perceptions and values of external stakeholders should also be taken into account.

The goals, objectives and strategies to achieve them, although key, are just a part of what makes up the internal context. Capabilities, culture, information systems and perceptions of internal stakeholders also need to be considered as part of this process.

Understanding the context of the organisation is fundamental if one is to be able to estimate the "risk capacity" (as defined by the FSB) of the organisation and to begin to articulate the "amount and type of risk the organisation is willing to pursue or retain" (ISO). What is required to complete the enablement of effective risk management is specific, detailed risk criteria.

3.3 Risk Criteria

ISO describe risk criteria as "the terms of reference against which the significance of a risk is evaluated". These can be qualitative or quantitative in nature and can be applied to the likelihood and/or consequences of a risk. They can also include "limits" that are specific to processes or projects. The risk criteria will at all times be influenced and guided by the risk appetite expressed by the board.

The challenge for organisations is how to select the best / most appropriate risk criteria. I'd like to suggest a methodology that we use in our organisation and with our customers.

The starting point is the objectives of the organisation, if these are not clearly defined then all effort to manage risk will be ineffective. Objectives bring focus to activities and will inform stakeholders as to what matters. In our process we present a list of things that matter to an organisation that includes words like; profit, people, compliance, reputation, customers, systems, service, and more and we seek agreement on 5 of them.

These 5 "What Matters" are then used to describe the levels of consequence that in turn are used to describe the level of risk. (in combination with likelihood) Fig (ii) below describes an example of consequence risk criteria developed using this method.

Level	Reputation	Compliance	People	Financial	Service
Substantial	Negative publicity-local and national, sustained, having dramatic impact on sustainability	CB sanctions and long-term onerous obligations for the organisation and officers	Departure of X key officers in one month, inability to conduct business within regulatory rules	Financial resources seriously impacted and affecting all new initiatives Losses greater than Z sustained.	Unable to provide any service to customers for 10 days
Significant	Negative publicity-local and national, having significant impact on sustainability	CB sanctions and medium term burdensome obligations for the organisation and officers	Departure of Y key officers in one month, delay in completing critical activities	Financial resources significantly impacted and affecting new initiatives Losses greater than Y sustained.	Unable to provide service to customers for 3 days
Moderate	Once-off local adverse publicity with short-term impact on operations	Strong advice received from regulator with deadline to address a non-compliance issue	Delay in receiving approval from regulator for new officers, some delays in completing activities	Losses of between X and Y sustained and causing delay in some initiatives	Unable to provide service to customers for 1 day
Minor	Verbal expression of dissatisfaction at local level	Temporary non-compliance, not publically known	Delay in recruiting for key role, short-term impact on servce	Losses below X sustained, no material impact on reported results	Unable to provide service to customers for 2 hours
Negligible	Event passing without comment	No appreciable effect on requirements	No impact on personnel or morale	Minimal effect on financial performance	Unable to provide service to customers for 30 min

Fig (ii). Example of Risk Criteria for Consequences

In larger organisations there will be many specific contexts in which risk is being managed and the risk criteria will be set accordingly. If the attitude is to avoid risk that is either "Significant" or "Substantial" then the descriptions and limits will need to reflect this.

3.4 Risk Appetite

I have shown an example of risk criteria already, but in the sequence of things the "risk appetite" would need to be already articulated by the board of directors. There may be some re-iteration of the process but it is important that the risk criteria, applied in the various contexts within the organisation, reflect the acceptable disaggregation of risk limits set at the highest level.

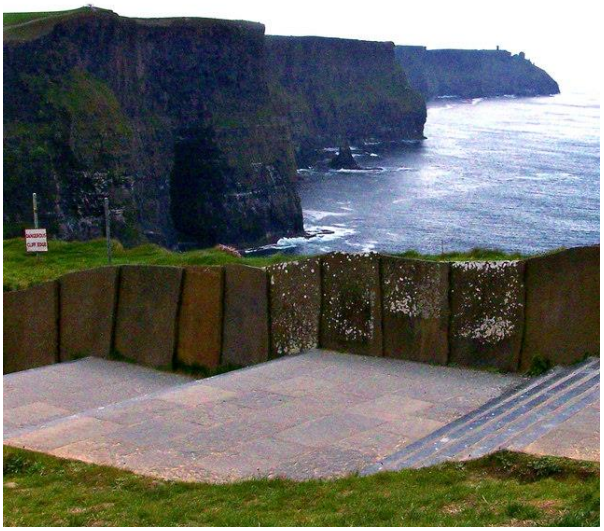
Which brings us back to the question asked at the beginning of section 3.1 in the discussion paper; "Why establish risk appetite?". And who is this for? I believe that this is primarily for the decision-makers within the organisation who are tasked with achieving the objectives. They need clarity on what level of risk is acceptable and guidance when faced with "competing" objectives. The risk

appetite is also for other stakeholders who need assurance that the organisation has actively considered the risks that they will and will not accept.

The “What” needs to be discussed. Section 5 lists a number of “characteristics” for consideration, but if the appetite is to be kept high-level then much of this detail can be avoided. More importantly, in my opinion, is the linkage between the risk appetite statement and the stated strategic objectives. The RAS should bring clarity to the primacy of objectives and to any flexibility which will be entertained in the level of achievement. Where there are decisions to be made that will favour one objective over another, decision-makers need to know the relative importance of the objectives and the willingness of the board to accept a trade-off.

3.5 Communicating the Appetite

As discussed in section 3.2.2 of the Discussion Paper it is important to know the risk capacity of the organisation. Figure 1 in that section shows a simple two dimensional diagram, which while instructive, is deceptively simple. I see the risk appetite like the line of Liscannor stones that keep people away from the edge of the Cliffs of Moher. Some transgressing of the boundary may not result in falling off the edge, but there was wisdom and engineering in placing the boundary there in the first place.



Observers need to monitor adherence to the rules so that instances of breaking them can be recorded and if a negative trend is recognised then perhaps higher boundaries need to be erected. With these boundaries one tries to strike a balance between facilitating the safe enjoyment of the view with the attendant adrenaline rush at being close to the edge and the absolute requirement to protect people from accidently going over the edge.

What this paper does not discuss, but which nevertheless will impact the effectiveness of a risk appetite statement, is the risk perception of employees and especially decision-makers in the organisation. Some will ignore boundaries and confidently stride on the risky side. They either don’t understand the risk or the reasons for the boundary. The organisation’s tolerance or intolerance of breaches of the risk appetite need to form part of the communication.