



Leading the risk profession

# Risk Appetite and Risk Tolerance

---

A consultation paper from the Institute of Risk Management

May 2011

# Risk Appetite and Risk Tolerance

---

This paper has been prepared under the overall direction of a working group of the Institute of Risk Management. The group has held a series of meetings to explore ideas and agree the direction of the paper. We have had healthy discussions, and given the nature of the topic, there have been areas that have proved contentious. We have presented the outline of the thinking in various meetings and we have circulated a draft of this paper to in excess of fifty individuals. We are now circulating it for a wider consultation. We know that future editions of this guidance may well be subject to major revisions. That will be a sign of good and healthy progress. It is in that context that we present this paper for your comments.

## Preface

The purpose of this paper is in the first instance to provide guidance to directors, risk professionals and others tasked with advising boards on compliance with the part of the UK Corporate Governance Code that states that “the board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives” (Financial Reporting Council, 2010).

However, we hope that the approach contained in here will have far broader resonance with anyone interested in the subject of Risk Appetite and Risk Tolerance. While this is not a subject with an untarnished history: most UK banks would have been expected to define their risk appetite, we are now poised to move beyond that thinking. Not a single bank would have said that it wished to court (and in some instances succumb to) oblivion in the form of the financial crisis. Whether it is a matter of setting, monitoring or overseeing risk appetite, this is a subject that has proved to be somewhat elusive - it means many different things to many different people. For example, some see it as a series of limits, some see it as empowerment, some see it as something that has to be expressed in terms of net risk and others gross. For this reason the subject deserves some serious attention.

In writing this paper, we are conscious that we may appear to have come at this from a UK, quoted company-centric perspective and that this is counter to IRM's international ethos. In fact, while this guidance has been written with the UK Corporate Governance Code in mind, it has also been developed in the hope that it is applicable to all sectors in all geographies. We would welcome feedback from readers in this regard.

Our objective in writing this booklet has been to give:

1. A theoretical underpinning to the subject of risk appetite; but more importantly to provide
2. Some guidance for those who need to deal with the subject, either for their corporate governance statements, or, alternatively, simply because they think the discussion would inform the way their business or organisation is run.

This guidance is not definitive: we do not think that we have uttered the last word on the subject. Thinking on the subject of Risk Appetite and Risk Tolerance will continue to develop and, if, as we hope, this booklet is superseded before too many reporting seasons come and go, then we will know that the concept is beginning to take root.

It is our view that Risk Appetite, correctly defined, approached and implemented could be a fundamental business concept that will make a substantial difference to how businesses and organisations are run. We fully expect that the initial scepticism about risk appetite will be gradually replaced as boards and executive directors gain greater insight into its usefulness. We also anticipate that analysts will soon be asking chief executives, chairmen and finance directors about risk appetite. After all this subject is at the heart of the organisation: risk-taking, whether private, public or third sector, whether large or small is what managing an organisation is about. The guidance from the Financial Reporting Council represents an opportunity to place risk management, and in particular risk appetite, right at the centre of the debate on effective corporate governance and the role of the board in running organisations.

We would like to know whether or not the approach in this paper has been helpful to you as you work through the ramifications of Risk Appetite and Risk Tolerance in your own organisation. Please take the time to tell us so that we can both keep abreast of developments and make sure that we are sharing best practice. At IRM we are passionate about leading the profession, and this is one way that we can do so.

At a personal level, I would like to thank the numerous people who have contributed to this paper, ranging from the working group, through various IRM meetings which debated early versions of the thinking to Carolyn Williams, Head of Thought Leadership at IRM, and of course, all of those people, clients, fellow risk professionals, internal auditors, and many, many others, who have discussed this subject with all of the members of the Working Group.

Comments are welcome on any aspect of the paper but we would be particularly interested to know:

1. To what extent do you think that the approach set out in this consultation paper provides a workable basis for developing an organisation's approach to risk appetite and risk tolerance?
2. Do you agree that an organisation has multiple risk appetites? Is that concept appropriately reflected in the guidance?
3. Do you agree that risk management maturity is an appropriate concept as a starting point for risk appetite and risk tolerance? Is there sufficient guidance on this in the document?
4. Do you agree with the approach of looking at the propensity to take risk and the propensity to exercise control?
5. Do you agree with the need to apply some form of measurement to risk appetite? Is shareholder value appropriate for quoted companies? Do you think there are better alternatives?
6. Do you think there is sufficient guidance on the development of risk appetite? What additional guidance would you like to see?
7. Do you think there is sufficient guidance on the oversight by the board (or risk committee) over the development and implementation of risk appetite?
8. Are there any critical elements that you believe are missing from the guidance?

9. Are there any other matters you would like us to consider before this is issued in a final version?

Your comments should be sent to Carolyn Williams, Head of Thought Leadership at IRM, by e-mail to [carolyn.williams@theirm.org](mailto:carolyn.williams@theirm.org) to arrive by Tuesday 31 May 2011.

Please provide sufficient detail and suggested amendments in replying to us so that we have a full understanding of your comments when we review them together with all the other comments at the end of the consultation period. Please provide your name, contact details and organisation and please indicate whether and how we can contact you to discuss your comments, should the need arise. We may publish your comments, as submitted, including your name and organisation, unless you explicitly request otherwise.

Richard Anderson  
**Deputy Chairman, Institute of Risk Management**

May 2011

### **About IRM**

The Institute of Risk Management (IRM) is the world's leading enterprise-wide risk education Institute. We are independent, well-respected advocates of the risk profession, owned by practising risk professionals. We provide qualifications, short courses and events at a range of levels from introductory to expert and support risk professionals by providing the skills and tools needed to deal with the demands of a constantly changing, sophisticated and challenging business environment. We operate internationally with members and students in over 90 countries, drawn from a variety of risk-related disciplines and a wide range of industries.

### **About the Author**

**Richard Anderson**, the principal author of this booklet, is Deputy Chairman of IRM. A Chartered Accountant, and formerly of PricewaterhouseCoopers, where he led the Strategic Risk Services practice in EMEA, Richard has also run his own GRC practice for seven of the last ten years. Richard has been professionally involved with risk management since the mid-nineties. Richard has broad industry sector experience. He wrote a report for the OECD on Corporate Risk Management in the banking sector in the UK, the USA and France. He is a regular speaker at conferences and contributes to many journals on risk management and governance issues.

# Table of Contents

- Preface ..... 2
  - About IRM ..... 4
  - About the Author ..... 4
- Executive Summary..... 7
- I Background ..... 12
  - The UK Corporate Governance Code ..... 12
  - What is risk appetite? ..... 14
  - Risk tolerance..... 16
  - Conclusion..... 16
  - QUESTIONS FOR THE BOARDROOM ..... 17
- II Designing a risk appetite..... 18
  - Organisational Maturity..... 20
  - Multiple risk appetites ..... 22
  - Risk culture..... 23
  - QUESTIONS FOR THE BOARDROOM ..... 23
- III Constructing a risk appetite ..... 25
  - Levels of risk appetite ..... 25
    - Strategic ..... 25
  - Strategic Risk..... 25
  - Risk Taxonomies ..... 26
    - Tactical ..... 27
    - Project or operational..... 28
  - Propensity to take risk ..... 28
  - Propensity to exercise control ..... 28
  - Balanced Risk ..... 29
    - Risk management clockspeed..... 30
    - Dimensions of control..... 31
  - Measurement..... 32
    - Strategic ..... 32
    - Tactical and operational..... 34
  - Data..... 34

QUESTIONS FOR THE BOARDROOM .....	34
IV Implementing a risk appetite .....	35
Sketch.....	36
Stakeholder engagement.....	36
Develop .....	36
Approve.....	36
Implement.....	37
Report .....	37
Review.....	37
QUESTIONS FOR THE BOARDROOM .....	37
V Governing a risk appetite.....	38
QUESTIONS FOR THE BOARDROOM .....	40
VI The journey is not over .....	41
QUESTIONS FOR THE BOARDROOM .....	42
Bibliography .....	43
Appendix: Determining the Risks the Board is Willing to Take .....	44
Responsibilities for risk taking .....	44

## Table of Figures

Figure 1 - Our Approach.....	17
Figure 2 - Risk Appetite in Context.....	19
Figure 3 - Risk Culture Diagnostic .....	24
Figure 4 - Risk Appetite - Main Issues.....	25
Figure 5 - Shareholder Value Model (1).....	32
Figure 6 - Shareholder Value Model (2).....	33
Figure 7 - Shareholder Value Model (3).....	33
Figure 8 - Stages of Development of Risk Appetite .....	35
Figure 9 - Governing a Risk Appetite.....	38
Figure 10 - Risk Appetite In the Organisation .....	39

## Executive Summary

No company can make a profit without taking risk. And yet taking risks without consciously managing those risks can lead to the downfall of organisations. This is the challenge that has been highlighted by the recent developments in the UK Corporate Governance Code issued by the Financial Reporting Council (the “FRC”) in 2010. Following the financial collapse, precipitated by banks which we all assumed were outstanding at managing risk, which was after all their *raison d’être*, first the Walker Report, and then the review of Corporate Governance by the FRC highlighted the need for boards to re-evaluate just how good they are at managing risk. As a consequence Risk Appetite and Risk Tolerance are now on the agenda for all listed companies. But this represents a massive challenge: risk professionals are divided as to how to determine risk appetite and there is precious little in terms of useful guidance. As a consequence, the Institute of Risk Management has produced this guidance. For some the detailed pages will seem over burdensome and too complicated. There is a reason for this: we are pulling together a disparate set of thinking into one document and until we are all confident in the day to day usage of Risk Appetite and Risk Tolerance, we think it is better to provide more, rather than less.

More important still, is our over-riding sense that any approach has to be (i) theoretically sound (but that can quickly disappear into the background); (ii) practical and pragmatic: we do not want to create a bureaucracy, rather we are looking to help find solutions that can work for organisations of all shapes and sizes; and (iii) something that will make a difference: we suspect that in the early days particularly, a successful approach to reviewing Risk Appetite and Risk Tolerance in the board room will necessarily lead to some tensions. In other words we think that it should make a difference to the decisions that are made, otherwise it does diminish into a mere tick-box activity – and nobody needs any more of those in the board room. Consequently, the approach that we are setting out in the detailed guidance can and should be tailored to the needs and maturity of the organisation: it is definitively not a one-size-fits-all approach.

There were four overriding principles in developing our approach:

1. Excessive simplicity, while superficially attractive, could lead to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it.
2. Risk appetite needs to be a measurable concept. We are promoting an approach of shareholder value at a strategic level, but other approaches could equally be valid. Underlying the shareholder value, we anticipate more use of key risk indicators and key control indicators based on data available inside or from outside the organisation.
3. There will be a range of appetites for different risks and these will vary over time: the temporal aspect of risk appetite is a key attribute to this whole development.
4. As discussed below, risk management maturity.

In essence what we are recommending is that an organisation’s approach to risk appetite and risk tolerance should:

- Be developed in the context of their **risk management maturity**. This might sound odd to some people, but risk management remains an emerging discipline and some organisations, irrespective of size or complexity, do it much better than others. This is in part due to their risk management culture (a subset of the overall culture), partly due their systems and processes, and partly due to the nature of their business. However, until an organisation has a clear view of its risk management maturity it cannot be clear as to what approach would work or how it should be implemented.
- Take into account differing views at a **strategic, tactical** and **operational** level. In other words, while the Code envisages a strategic view of risk appetite, in fact risk appetite needs to be addressed throughout the organisation for it to make any practical sense.
- Not be done in isolation of understanding the control culture of the organisation. This model explores this by looking at both the “**propensity to take risk**” and the “**propensity to exercise control**”. The model promotes the idea that the strategic level is proportionately more about risk taking than exercising control, while at the operational level the proportions are broadly reversed. Clearly the relative proportions will depend on the organisation itself, the nature of the risks it faces and the regulatory environment within which it operates.
- The approach envisaged by this risk appetite model suggests that it is important for organisations to identify **measures of risk appetite**. Otherwise there is a risk that any statements become empty and vacuous.

We think that this dual focus on taking risk and exercising control is innovative but critical to a proper understanding of risk appetite and risk tolerance. Proportionately more time is likely to be spent on risk taking at a strategic level than at an operational level, where the focus is more likely to be on the exercise of control. One word of caution though, we are not equating strategy with board level and operations with lower levels of the organisation. A board will properly want to know that its operations are under control as much as it wants to oversee the development and implementation of strategy. In the detailed paper we have included a few suggestions as to how boards might like to consider these dual responsibilities. Above all, we are very much focused on the need to take risk as much as the traditional heartland of many risk management programmes, which is the avoidance of harm.

In our paper we have set out an illustrative process for the development of an approach to risk appetite. This includes appropriate consultation with external and internal stakeholders, with whom the board believes it appropriate to consult on this matter. It also includes a review process by the board, or an appropriate committee of the board, and finally, it includes a review process at the end of the cycle so that appropriate lessons can be learned.

We have also included a brief section on the role of the board or risk committee: we are suggesting that the board should retain governance over the model at four key points:

- **Approval:** as discussed in the development of the risk appetite statement;
- **Measurement:** there needs to be regular and consistent measurement against the model and demonstration that the model is used in real life;

- **Monitoring:** the board will need to deal with breaches of the appetite, or tensions that arise from its implementation. If there are no breaches and no tensions then the likelihood is that it has not been properly developed.
- **Learn:** as discussed in the development section, the board needs to ensure that the organisation learns from the implementation of the risk appetite model so that it becomes more embedded into the organisation.

All of this needs to be carried out with the basic precept in mind that risk appetite can and will change over time as, for example, the economy shifts from boom to bust, or as cash reserves fall. In other words, breaches of risk appetite may well reflect a need to reconsider the risk appetite part way through a reporting cycle as well as a more regular review on an annual cycle. Rapid changes in circumstances, for example as were witnessed during the financial crisis in 2008-9, would certainly indicate a need for an organisation to re-appraise its risk appetite.

It is our belief that the development of risk appetite as a useful construct in the governance and management of organisations will evolve over time. However there are a number of issues that we think are worth keeping in mind. In particular, risk appetite:

- Is as much about “enabling” risk taking as “constraining” adverse risks;
- Is a management tool as well as a governance requirement;
- Requires active “stakeholder” engagement;
- Needs to be built into “business as usual” processes;
- Should be approved by the board (or non-executive board risk committee)
- Has to be actively monitored by management
- Has to be reviewed regularly by the board; and
- Needs measurement tools and techniques.

But equally there are some substantial benefits. Risk appetite can help in:

- Safeguarding the organisation;
- Creating a framework for better decision making;
- Identifying issues at an early stage (allowing more wriggle room to deal with risks);
- Provide a framework for reducing surprises;
- Developing a model for structured thinking;
- Facilitating better achievement of long term objectives while respecting stakeholder views; and
- Bringing sense to the risk process.

Within IRM it is our intention to work with companies, boards, risk professionals, regulators and others to develop the thinking around risk appetite. For us the immediate next steps include:

- Developing a consensus as to what risk appetite means: this booklet is just a first step in the discussion;
- Working with interested parties to develop appropriate mechanisms for measurement, including understanding:
  - The data sources that will be needed;

- The impact on operational frameworks; and
- The new data architecture and data governance models that will be required;
- The communications campaign that will include addressing the needs of boards and individual board members.

Finally, we set out below the questions that we think that boards will want to answer as they develop their approaches to risk appetite:

1. Is the board clear about the nature and extent of the significant risks it is willing to take in achieving its strategic objectives?
2. What are the strategic objectives? Are they clear? What is explicit and what is implicit in those objectives?
3. What are the significant risks the board is willing to take? What are the significant risks the board is not willing to take?
4. What steps has the board taken to ensure oversight over the management of the risks?
5. Does the board need to establish clearer governance over the risk appetite and tolerance of the organisation?
6. How mature is risk management in the organisation? Is the view consistent at differing levels of the organisation? Is the answer to these questions based on evidence or speculation?
7. What specific factors should the risk appetite take into account in terms of the business context? Risk processes? Risk systems? Risk management maturity?
8. At which levels would it be appropriate for the board to consider risk appetite?
9. What are the main features of the organisations risk culture in terms of tone at the top? Governance? Competency? Decision making?
10. How much does the organisation spend on risk management each year? How much does it need to spend? What are the business, regulatory or other factors that will influence the relative importance of the organisation's propensity to take risk and its propensity to exercise control at strategic, tactical and operational levels?
11. Does the organisation employ helpful risk taxonomies that facilitate the identification and responsibility for managing risk as well as providing insight on how to manage risks?
12. Does the organisation understand clearly why and how it engages with risks?
13. Is the organisation addressing all relevant risks or only those that can be captured in risk management processes?
14. Does the organisation have a framework for responding to risks?
15. What approach has the organisation taken to measuring and quantifying risks?
16. Has the organisation followed a robust approach to developing a risk appetite?
17. Who are the key external stakeholders and have sufficient soundings been taken of their views? Are those views dealt with appropriately in the final documentation?
18. Is the risk appetite tailored and proportionate to the organisation?
19. Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?
20. What is the evidence that the organisation has implemented the risk appetite effectively?

21. Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?
22. To what extent did the board identify tensions arising from the implementation of the risk appetite?
23. How much resource has it taken to develop and implement risk appetite? Was this level of resource appropriate? Does it need to be amended going forward?
24. What needs to change for next time round?
25. Does the organisation have sufficient and appropriate resources and systems?
26. What difference did the process make and how would we like it to have an impact next time round?

Above all, we want to hear from you. Please tell us what you think is good or bad about this booklet, what needs changing, where you need further information or guidance and above all how we can act as a support to boards and those that advise them in this important area of corporate governance.

## I Background

101 The financial crisis of 2008 had many consequences, not least of which was the question as to why boards failed to see it coming. At the request of the Prime Minister of the day, Sir David Walker carried out a review of the corporate governance of Banks and Other Financial Institutions (“BOFI’s”) and this was followed swiftly by a review of the broader corporate governance landscape in the UK by the Financial Reporting Council (the “FRC”). The FRC made the all important link between this question and the subject of Risk Appetite and Risk Tolerance by inserting reference to these two topics in their draft changes to Section C of the UK Corporate Governance Code (the “Code”) (Financial Reporting Council, 2010). While those very words failed to survive the cut, the concept did survive. Under the newly expanded Section C, a board is explicitly tasked with being responsible for “determining the nature and extent of the significant risks it [the board] is willing to take in achieving its strategic objectives”. This is Risk Appetite and Risk Tolerance by any other name. The rest of this section explores the nature of the words in the Code, and looks at the existing guidance which might help to understand the words.

- Sections II and III look at a proposed new model of Risk Appetite and Risk Tolerance;
- Sections IV and V look at the practicalities of implementing and overseeing Risk Appetite and Risk Tolerance;
- Section VI addresses some of the issues that might require further thought; and
- The appendix presents a summary of how, in practical terms, a board might go about determining the risks it is willing to take.

Throughout the paper we have indicated questions that could usefully be explored in the boardroom to ensure that the subjects of Risk Appetite and Tolerance are being appropriately addressed.

### The UK Corporate Governance Code

102 In its recent update to the UK Corporate Governance Code, the FRC has expanded the section of the Code on Accountability as set out in the box below:

#### **Section C: Accountability**

The board should present a balanced and understandable assessment of the company’s position and prospects. The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.

The board should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles...

103 This Section is further expanded in the detailed provisions of the Code:

### **C.1 Financial and Business Reporting**

C.1.2 The directors should include in the annual report an explanation of the basis on which the company generates or preserves value over the longer term (the business model) and the strategy for delivering the objectives of the company.

### **C.2 Risk Management and Internal Control**

#### **Main Principle**

The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.

#### **Code Provision**

C.2.1 The board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls.

104 This paper explores the risk management ramifications of these high level statements, and in particular those relating to the “nature and extent of the significant risks [the board] is willing to take in achieving its strategic objectives”. These are the words that replace the references to risk appetite and tolerance in earlier drafts. It is worth noting that this sentence immediately precedes the requirement that “the board should maintain sound risk management and internal control systems”. So this is not empty rubric, but rather a matter of substance, especially since Code Provision C.2.1 goes on to require the board “at least annually [to] conduct a review of the effectiveness of the company's risk management and internal control systems...” To some this sounds like a recipe for Sarbanes-Oxley s404 style work. This is clearly not the intent of the FRC, nor would it be welcomed in most UK boardrooms. However, the fact of this review has to be reported to shareholders. The juxtaposition of the “significant risks” sentence with the requirement to maintain “sound risk management and internal control systems” would suggest that the risk appetite element is one of the reasons that organisations require risk systems. This is a radical new departure for the FRC and introduces a new concept for many directors and boards of non-financial services organisations.

105 As an aside, it seems that the terms “Risk Appetite” and “Risk Tolerance” have deep associations with the financial services industry in some minds (particularly in the UK), and attempts to move non-financial services organisations in that direction might have been difficult. However clarification to an IRM meeting suggests that the FRC sees the new words, for all intents and purposes, as being indistinguishable from the previous phrases. It is our feeling (and we stand to be corrected) that the more difficult of these subjects is risk appetite. Accordingly we focus predominantly on the concept of risk appetite in this paper as a way of providing guidance to directors and those tasked with advising directors on the requirements of the Code in so far as they relate to risk appetite.

## What is risk appetite?

106 Risk appetite is a phrase that is widely used but frequently in different contexts and for different purposes. It is a phrase that for some people conveys poorly its meaning, and in respect of which the meaning is different for different groups of people. Based on the limited work undertaken for this paper it was clear that there is little certainty as to what the phrase means, but there seems to be almost unanimity that it could be, and indeed ought to be a useful concept, if only it could be properly expressed. In this booklet we are taking a very pragmatic view: Risk Appetite is the most common phrase that we have come across, is the one that was used by the FRC in the context of the corporate governance code (and in informal sessions still is used by them) and therefore we would prefer to define it in a way that begins to make sense for as many people as possible.

107 Given the lack of conformity about the meaning of the phrase, it is worth looking at the key standards on risk management, ISO31000 (ISO, 2009) and BS31100<sup>1</sup> (British Standards, 2008), to see what light they shed on the subject. Interestingly ISO31000, the international standard, is silent on the subject of risk appetite (focusing instead on ‘risk attitude’ and ‘risk criteria’), although Guide 73 (ISO, 2002) defines risk appetite as the “amount and type of risk that an organisation is willing to pursue or retain.”

108 BS31100 contains more detail. It defines risk appetite as the “amount and type of risk that an organisation is prepared to seek, accept or tolerate” – very similar to Guide 73. The standard goes on to define Risk Tolerance (bearing in mind that the definition of risk appetite includes reference to tolerating risk) as an “organisation’s readiness to bear the risk after risk treatments in order to achieve its objectives”. The definition then includes a rider which states: “NOTE: Risk tolerance can be limited by legal or regulatory requirements”.

Definition of Risk Appetite	
ISO 31000 / Guide 73	BS31100
Amount and type of risk that an organisation is willing to pursue or retain	Amount and type of risk that an organisation is prepared to seek, accept or tolerate

109 Notwithstanding the regular appearance of risk appetite and risk tolerance in the same sentence (or definition in the case of BS31100) it is our belief that Risk Tolerance is a much simpler concept in that it tends to suggest a series of limits which, depending on the organisation, may either be:

- In the nature of absolute lines drawn in the sand, beyond which the organisation does not wish to proceed; or
- More in the nature of tripwires, that alert the organisation to an impending breach of tolerable risks.

<sup>1</sup> At the time of writing, this document is undergoing revision. Nevertheless the approach in the 2008 document has proved most useful for this discussion.

We are therefore focusing in this booklet much more on seeking to develop an understanding of risk appetite.

110 While neither standard is very informative, it is instructive to see how the “appetite” word or similar words are used in BS31100:

- **Paragraph 3.1 Governance** includes a bullet to the effect that the risk management framework should have “defined parameters around the level of risk that is acceptable to the organisation, and thresholds which trigger escalation, review and approval by an authorised person/body.”
- **Paragraph 3.3.2 Content of the risk management policy** has the first explicit reference to risk appetite saying that this should be included in the policy and should outline “the organisation’s risk appetite, thresholds and escalation procedures”.
- **Paragraph 3.8 Risk appetite and risk profile** provides a much more comprehensive commentary on risk appetite, which is set out below:
  - “Considering and setting a risk appetite enables an organisation to increase its rewards by optimizing risk taking and accepting calculated risks within an appropriate level of authority.
  - “The organisation’s risk appetite should be established and/or approved by the board (or equivalent) and effectively communicated throughout the organisation.
  - “The organisation should prepare a risk appetite statement, which may:
    - “provide direction and boundaries on the risk that can be accepted at various levels of the organisation, how the risk and any associated reward is to be balanced, and the likely response;
    - “consider the context of the organisation’s understanding of value, cost-effectiveness of management, rigour of controls and assurance process;
    - “Define the control, permissions and sanctions environment, including the delegation of authority in relation to approving the organisation’s risk acceptance, highlighting of escalation points, and identifying the escalation process for risk outside the acceptance criteria, capability or capacity;
    - “be reflected in the organisation’s risk management policy and reported upon as part of the organisation’s internal risk reporting system;
    - “include quantitative statements, described as limits, thresholds or key risk indicators, which set out how certain risks and their rewards are to be judged and/or how the aggregate consequences of risks are to be assessed and monitored.
  - “... [T]he risk appetite... should be monitored by the Board (or equivalent) and formally reviewed as part of the organisation’s strategy and planning process. This should consider whether the organisation’s risk appetite remains appropriate to deliver the organisation’s objectives in light of internal and external drivers and constraints.”

- Paragraph 4.7 Risk review suggests that a regular risk review should consider “whether key risks are being managed within the risk appetite.”

111 In conclusion, BS31100 provides some guidance on how to **use** risk appetite, but it does not (nor did it ever set out to) provide guidance on how to **calculate** or **measure** risk appetite, although the standard does suggest the use of “quantitative statements”, without further elaborating.

## Risk tolerance

112 It is worth noting that in the eyes of some commentators, risk tolerance is the more important concept. While risk appetite is about the pursuit of risk, risk tolerance is about what you can bear. Without a doubt there will be occasions where an organisation can bear more risk than it is thought prudent to pursue, we still remain of the view that articulating the tolerance is comparatively simple, while working out what you wish to pursue is relatively complicated.

113 What is clear is that different boards in different circumstances will take different views as to which of these two concepts is more important for them at any given time.

## Conclusion

114 There are three early conclusions that we have drawn from the work we have undertaken in preparing this booklet:

- The first is that setting a risk appetite is only a worthwhile exercise if you, as an organisation, are able to manage the risk to the level at which it is set.
- The second is that there is very little by way of formal guidance on the definition of risk appetite. We have reviewed plenty of documents both from professional organisations and from consulting firms. However, our belief is that this subject remains under developed and the remainder of this booklet aims to play a part in redressing that shortcoming.
- The third is that risk appetite can and indeed must change, for example as the economy shifts from boom to bust and back again, or as cash reserves fall. Risk appetite, and indeed risk tolerance, both have a temporal element, which is reflected in the way in which we have discussed the monitoring and governance of risk appetite later in this booklet.

115 We have set out a route through this topic of risk appetite as set out diagrammatically below:



**Figure 1 - Our Approach**

This is reflected in the rest of the paper which is set out under the following main headings:

- Section II:** Designing a risk appetite
- Section III:** Constructing a risk appetite
- Section IV:** Implementing a risk appetite
- Section V:** Governing a risk appetite

In **Section VI**, which we have called “the journey is not over”, we explore some of the issues that we will need to explore as we develop this concept as a boardroom topic.

## **QUESTIONS FOR THE BOARDROOM**

1. Is the board clear about the nature and extent of the significant risks it is willing to take in achieving its strategic objectives?
2. What are the strategic objectives? Are they clear? What is explicit and what is implicit in those objectives?
3. What are the significant risks the board is willing to take? What are the significant risks the board is not willing to take?
4. What steps has the board taken to ensure oversight over the management of the risks?
5. Does the board need to establish clearer governance over the risk appetite and tolerance of the organisation?

## II Designing a risk appetite

201 In developing a possible model for risk appetite, the IRM working group was conscious of five key factors:

- We heard about organisations that appeared to have defined very **misleading risk appetites**: for example an organisation that concluded that it was “hungry” for IT risk and which therefore apparently relaxed many of the normal process controls that surround system development. As a consequence they failed in at least two major implementations because basic and fundamental control processes were not followed. The system failures were so far reaching that most of the board either felt compelled to resign or were removed from post. The lesson that we drew from this and other examples was that risk appetite has at least two components: **risk** and **control** and that to consider either in isolation could result in sub-optimal decisions.
- We were conscious that risk appetite **needs to be a measurable concept**. There are many examples of risk management being a rather empty and vacuous process which can at best be described as being “data-lite”, if not “data-free” zones. We therefore believe that risk appetite needs to have some form of meaningful “yardstick” to support its proper implementation.
- There appears to be a broad consensus that there is no single risk appetite, but rather **a range of appetites** for different types of risk. It therefore seemed appropriate to look at the subject of risk appetite at different levels.
- Risk appetite has a **temporal dimension**: in other words the appetite and tolerance will change over time as circumstances change. This is not something that can be written in tablets of stone and then ignored for the rest of the year.
- Finally, we are conscious that different organisations are at different stages in their development of risk management, let alone risk appetite. For some it will be a comparatively simple additional step, for others it will be harder. For this reason we have adopted the phrase that crops up repeatedly in BS31100: organisations should develop a tailored and proportionate response. We have defined this in terms of **organisational maturity**. We do not mean this in any sense pejoratively: an immature risk management approach is not of itself a problem; it simply is a statement of fact for a given organisation. There are some very large companies that are relatively unsophisticated in their risk management and smaller ones that are very advanced.

202 With all of this at the back of our minds, the risk appetite working group of IRM has developed an approach to unpack the various elements of risk appetite. The model is depicted in the diagram below:

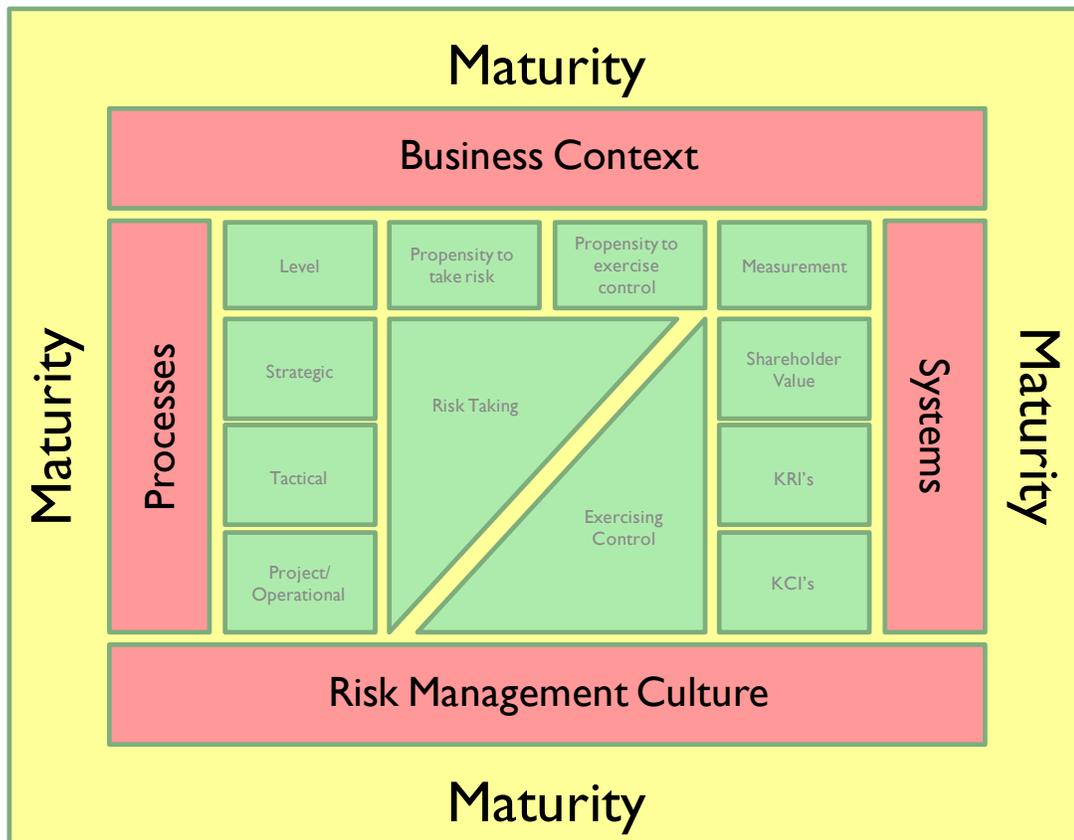


Figure 2 - Risk Appetite in Context

203 This model has several key features:

1. We think that risk appetite has to be set in the context of the maturity of the business. In other words there is little advantage for a relatively immature business seeking to set a sophisticated risk appetite if it does not have the competence and capability to manage to the risk appetite that they are setting. Therefore, it is important that this is not seen as a “one-size-fits-all” model of risk appetite, but rather it should be tailored and proportionate to the size, nature and maturity of the business.
2. We are suggesting that maturity of the business can be seen in four dimensions of:
  - a. **Business context:** the state of development, size, industry sector, geographical spread, complexity of business model and so on;
  - b. **Risk management culture:** the extent to which the board (and its relevant committees), management, staff and relevant regulators understand and embrace the risk management systems and processes of the organisation;
  - c. **Risk management processes:** the extent to which there are processes for identifying, assessing, responding to and reporting on risks and risk responses within the organisation; and

- d. **Risk management systems:** the extent to which there are appropriate IT and other systems to support the risk management processes.
3. The approach outlined envisages risk appetite being set at strategic, tactical and operating levels. In other words, while the UK Corporate Governance Code envisages a strategic view of risk appetite, in fact risk appetite needs to be addressed throughout the organisation for it to make any practical sense. This “allocation” of risk appetite across different aspects of the organisation represents one of the biggest challenges, and remains an area where we believe that further work is required.
4. We are of the view that understanding risk appetite cannot be done in isolation of understanding the control culture of the organisation. This model explores this by looking at both the “**propensity to take risk**” and the “**propensity to exercise control**”. The model promotes the idea that the strategic level is proportionately more about risk taking than exercising control, while at the operational level the proportions are broadly reversed. Clearly the relative proportions will depend on the organisation itself, the nature of the risks it faces and the regulatory environment within which it operates.
5. The approach envisaged by this risk appetite model suggests that it is important for organisations to identify measures of risk appetite. Otherwise there is a risk that any statements become empty and vacuous.

## Organisational Maturity

204 Risk management maturity is an increasingly familiar concept. Many organisations have developed risk management maturity models which cover a variety of attributes. Some address the maturity of risk management and control processes, some consider the culture of risk management, and some consider the preparedness of the organisation to face up to (or be susceptible to) disaster.

205 We think that there are four dimensions of risk management maturity that a board should consider in determining its preparedness to embark on a risk appetite exercise. These are:

- **The business context:** there is little advantage to an organisation in defining a risk appetite that is not based firmly in the context of the business. A wide variety of business factors will influence the risk appetite and some examples of these are set out in the table below. In essence a good understanding of the business model is an essential first step in determining how much risk the business is currently

### Clear Perspectives

One factor has become clear in talking to many organisations over a long period: risk management maturity is not clearly discernible from the top of the organisation. Where many board members and senior managers take a comparatively benign view of their organisational maturity vis-à-vis risk management, as you survey further down the organisation, there is typically a greater degree of scepticism about the organisational capability in managing risk.

Accordingly, we do not think that organisations should take it as read that the view of risk management maturity from the top is comprehensive. We strongly recommend that boards should commission a review of risk management maturity, either internally, or by an outside provider, to ascertain the level of risk management maturity to ensure that the organisation is sufficiently prepared to embark on the development of a corporate risk appetite.

engaging with and how much more it might wish to engage with in the future.

- **Risk management culture:** the ability to determine, manage and monitor a risk appetite will depend to a large extent on the maturity of the risk management culture within the organisation. Where the attitude to risk management is one of indifference, or a sense that risk management is little more than a bureaucratic paper chase, then the likelihood of developing an effective risk appetite is remote. Equally, it is essential that the tone for risk management is set from the top: if the chairman and chief executive are indifferent, then that will most likely be reflected in attitudes further down through the organisation.
- **Risk management processes:** there are some common factors that should be present in all risk management processes, namely risk identification, risk assessment and risk monitoring and reporting. The issues that need to be understood include the extent to which these are common across the organisation, the extent to which there is a common language across the business and above all whether gathering and reporting all of the risk management information makes any difference to the way in which the business is run. As we said earlier, setting a risk appetite is only a worthwhile exercise if you, as an organisation, are able to manage the risk to the level at which it is set. This implies the need for effective risk management processes.
- **Risk management systems:** most organisations have comprehensive and effective systems for collecting rearward looking key performance indicators (KPIs): namely accounting systems. IT systems, people, responsibilities and so on are all well-defined in a more or less smoothly operating system. Few organisations have similar approaches to managing forward looking issues: in other words the systems (in the broadest sense of the word) are rarely subject to the same extent of rigour or complexity. Increasingly we anticipate that organisations will need to collect, process and disseminate risk information across the business in order to be truly effective.

Area of focus	Factors to consider
Business context	<ul style="list-style-type: none"> <li>● Nature of business</li> <li>● Size of business</li> <li>● Geographical spread of operations</li> <li>● Degree of virtualisation</li> <li>● Complexity of value chain</li> <li>● Interdependencies with other partners</li> <li>● Political climate</li> <li>● Regulatory environment</li> <li>● Competitive environment</li> <li>● Risk clockspeed (see page 25 -the rate at which information necessary to understand and manage a risk becomes available (Smith, 2010))</li> </ul>
Risk management	<ul style="list-style-type: none"> <li>● Tone from the top</li> <li>● Attitudes to governance in the organisation</li> </ul>

culture	<ul style="list-style-type: none"> <li>• Attitudes to the management of risk</li> <li>• Attitudes to control</li> <li>• Attitudes to regulation</li> <li>• Attitudes to innovation</li> <li>• Competencies and capabilities</li> </ul>
Risk management processes	<ul style="list-style-type: none"> <li>• Identification processes</li> <li>• Assessment processes</li> <li>• Monitoring and reporting processes</li> <li>• Common language</li> <li>• Extent of common processes</li> <li>• Delegations of authority</li> <li>• Integration with strategy and business planning</li> <li>• Integration with regular periodic reporting</li> <li>• Escalation procedures</li> </ul>
Risk management systems	<ul style="list-style-type: none"> <li>• Extent of organisational structure to facilitate the management of risk</li> <li>• Risk management strategy and policy defined</li> <li>• IT support systems</li> <li>• Enterprise data warehouse for risk data</li> <li>• Risk reporting</li> </ul>

206 Needless to say, these “factors to consider” are not comprehensive and any organisation would need to tailor a review of maturity to their own circumstances. As with everything in this guidance it is important that the review of risk management maturity is tailored and proportionate to the organisation itself rather than being dictated by external guidance and checklists.

### Multiple risk appetites

207 We believe that it is almost impossible to encapsulate risk appetite for a business in a phrase such as “**risk averse**” or “**risk welcoming**”. Such phrases fail to recognise that in all but the very simplest businesses there is inevitably more than one risk appetite. There might be one risk appetite for selling a particular product, and a different appetite for taking risk while selling another product. There might be one appetite for regulatory risk in one country and another appetite in a different regulatory regime. It seems inevitable that risk appetite has to be capable of being expressed differently for different classes of risk and at different levels of the organisational structure. However, we believe that there needs to be a cross-check between risks and a holistic view at the top of the organisation.

208 The model that we have depicted in Figure 1 above incorporates the ability to represent multiple risk appetites in two ways:

- In the first instance it recognises that there will be different appetites for risk at different levels. The diagram explicitly shows risk appetite at a strategic, tactical and operational level. The next section of this paper discusses this in more detail. However, in essence the importance of this is that it binds together the two elements of the “propensity to take risk” and the “propensity to exercise control”. The essence of the model is that proportionately more time, effort and resources are devoted to taking risk at a strategic level, and proportionately more time, effort and resources are devoted to exercising control at an operational level of the organisation.
- An important aspect of the model is that it requires a mechanism for measurement. This will facilitate comparison of different risk types, and allow for some form of aggregation across the organisation.

## Risk culture

209 We think that it is worth reflecting on risk culture, which most risk professionals recognise as an important area of debate. A good risk culture will facilitate the better management of risk and indeed will underpin an organisation’s ability to work within its risk appetite (see 'Risk Culture' box for more discussion). Symptoms of a poorly functioning risk culture include:

- Leadership sends inconsistent or unclear messages on acceptable levels of risk;
- Risk is perceived to be managed intuitively and not discussed in making decisions;
- Provided business results are delivered, few questions get asked regarding what might go wrong; and
- There is little or no sanction for those taking inappropriate levels of risk.

## QUESTIONS FOR THE BOARDROOM

1. How mature is risk management in the organisation? Is the view consistent at differing levels of the organisation? Is the answer to these questions based on evidence or speculation?
2. What specific factors should the risk appetite take into account in terms of the business context? Risk Processes? Risk Systems? Risk Management maturity?
3. At which levels would it be appropriate for the board to consider risk appetite?
4. What are the main features of the organisations risk culture in terms of tone at the top? Governance? Competency? Decision making?
5. How much does the organisation spend on risk management each year? How much does it need to spend?

## Risk Culture

There are many approaches to measuring or diagnosing risk culture and many models of risk culture. One illustrative model (Hindson, 2010) suggests eight key indicators, grouped into four themes:



Figure 3 - Risk Culture Diagnostic

Typical issues under each of these headings would be:

### I Tone at the Top

- **Risk Leadership:** Do senior management set clear expectations for risk management? Do leaders provide a role model in risk management thinking and actively discuss tolerance to risk issues? How are messages consistently delivered over time?
- **Responding to Bad News:** Do senior management actively encourages management information related to risks to travel quickly across the organisation? Is there openness and honesty in communicating on risk issues?

### II Governance

- **Risk Governance:** Accountability for the management of key business risks is absolutely clearly defined. Risk accountabilities are captured within role descriptions and performance targets.
- **Risk Transparency:** Risk information is communicated in a timely manner to those across the organisation. Lessons, both positive and negative are shared from risk events.

### III Competency

- **Risk Resources:** The risk function has a defined remit and scope of operations and has the support of leaders. It is able to challenge how risks are being managed when appropriate.
- **Risk Competence:** A risk champion structure is in place to support managers in better managing risks. Structured training programmes are in place.

### IV Decision Making

- **Risk Decisions:** Leaders seek out risk information in supporting decisions. The business's willingness to take on risks is understood and communicated.
- **Rewarding appropriate risk taking:** Leaders are supportive of those actively seeking to understand and manage risks. This is recognised through the performance management process.

### III Constructing a risk appetite

301 In Section II of this paper we explored the main attributes of the risk appetite model: in this section, we look at each of the main aspects in more detail.

302 At the heart of the risk appetite model we have the main issues that an organisation has to deal with in setting and monitoring its risk appetite. These are set out in the diagram below:

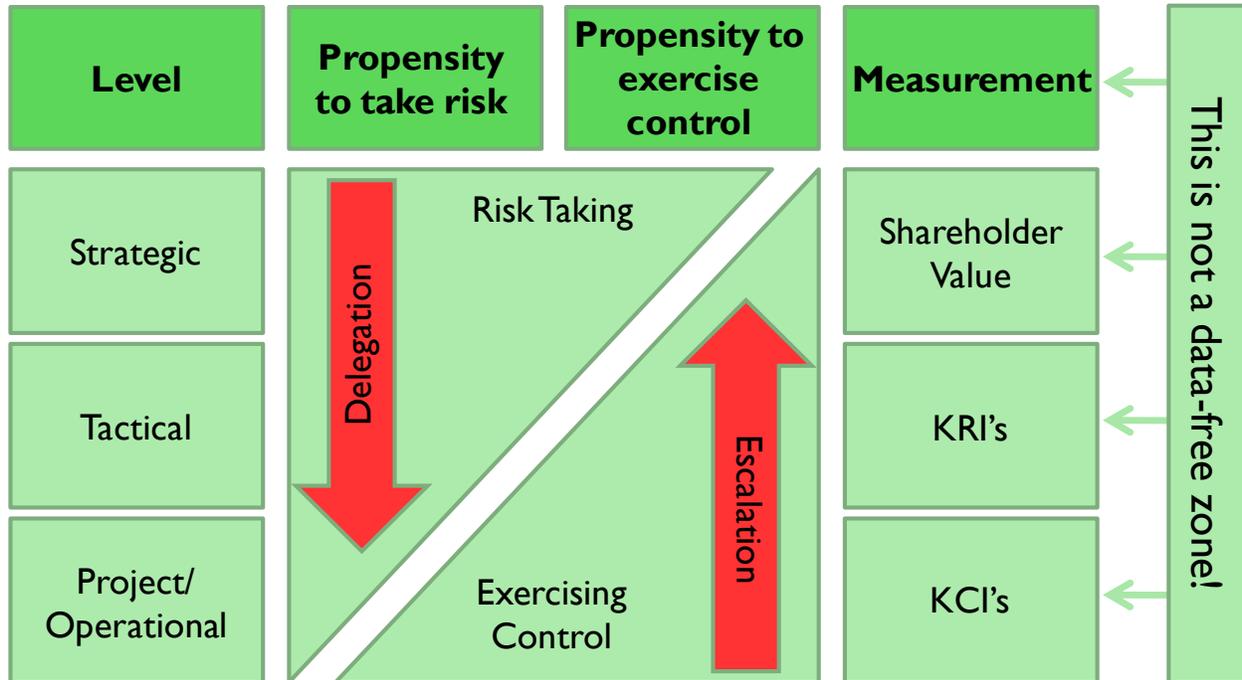


Figure 4 - Risk Appetite - Main Issues

#### Levels of risk appetite

303 This model envisages at least three levels of risk appetite as set out in the following paragraphs.

##### Strategic

304 At a strategic level risk appetite is predominantly about the risks or types of risks that an organisation has a unique competency to manage (or indeed know that they can neither manage nor mitigate) and that provide it with its competitive advantage (private sector) or its ability to achieve its objectives (public or third sector). Risk appetite at the strategic level will also be about deciding from which risks or types of risk the organisation needs to protect itself.

##### Strategic Risk

Some examples of strategic risks:

- Decisions about outsourcing.
- Decisions about new products developments.
- Decisions about new sources of finance.
- Decisions about acquisitions or disposals.

## Risk Taxonomies

There are lots of possible taxonomies of risk that the organisation might use in determining its approach to any particular risk. Three illustrative examples are shown in the table.

Different risk taxonomies can be useful for different purposes			
Taxonomy	John Adams	Organisational	Source
Classifications	<ul style="list-style-type: none"> <li>• Directly Discernible</li> <li>• Visible through Science</li> <li>• Virtual</li> </ul>	<ul style="list-style-type: none"> <li>• Head office</li> <li>• Department A (eg marketing)</li> <li>• Department B (eg Finance)</li> <li>• Geography X</li> <li>• Geography Y</li> </ul>	<ul style="list-style-type: none"> <li>• Strategic</li> <li>• Operational</li> <li>• Compliance</li> <li>• Process</li> <li>• Reputational</li> <li>• Change</li> </ul>
Use	Useful for determining the type of response required to manage or monitor a risk	Useful in determining the responsibility for managing a given risk	Useful in helping to identify sources of risk.

Under the first column we have shown the taxonomy suggested by Professor John Adams (Adams, 2001). This will be familiar to many people who have sat the exams for IRM's International Diploma. In broad terms, Professor Adams defines three types of risk as follows:

- **Directly discernible** risks are those that we are culturally attuned to managing on a day to day basis. These are often basic risks, which might have quite literally life and death consequences, but which we cannot imagine not existing. We manage them automatically.
- **Visible through science** risks are those that benefit from a significant amount of data which informs managers how they should be controlled. Typically there are professional disciplines that ensure that these risks are managed effectively, and the availability of the appropriate skill base may well determine the appetite of the organisation to engage with these risks.
- **Virtual** risks are those for which there is comparatively little prior personal or institutional knowledge and where the range of outcomes is almost impossible to determine. As a consequence there is frequently little agreement as to how the risk should be managed.

This can be a useful approach to consider when determining the type of response required to monitor or manage a particular risk.

Under the second column we are representing a traditional organisational hierarchy of risk, a view that can be particularly useful in determining responsibilities for managing risk. In the third column we represent a taxonomy based on the source of the risk.

It is important that a taxonomy is adopted that is understood throughout the organisation and that can be used in detailed implementation of the risk appetite at lower levels of the organisation.

305 In considering the risks (or types of risk) that an organisation wishes to engage with or to avoid, it should take into account also the performance culture of the organisation, because this will determine the amount of these risks that individuals which take, and also the corporate ethics and behaviours that an organisation displays, because these will be important in determining the extent of risk taking and avoiding.

306 Figure 4 above shows more emphasis on risk taking than exercising control at strategic level. This should not be confused with implying that strategic equates to board level. The board may well take an appropriate interest in control, in part because of its governance responsibilities, in part because of the organisation's regulatory environment, and in part because control has to start at the top of the organisation. Therefore the diagram should be viewed as the relative strategic importance, not the overall importance of risk versus control.

307 It is for the board and senior management to determine the relative strategic importance of the organisation's propensity to take risk and its propensity to exercise control and to influence that relative focus throughout the organisation. However, in broad terms an organisation that under-emphasises risk at the expense of over-emphasising control at a strategic level may run the risk of suffering from an inability to take risk throughout the hierarchy. Whereas an organisation that over-emphasises risk taking at the expense of under-emphasising control at a strategic level may run the risk of taking un-controlled risk which can result in dangerous exposure to unwanted risk. The skill is in determining the right balance for the organisation.

### **Tactical**

308 Many organisations struggle to implement their strategy, regardless of how finely developed and well honed their strategy is. There is a well recognised phenomenon of a gap between definition and implementation of the strategy. We are describing this as the tactical element of risk appetite: the cusp between strategic vision and implementation. This may well be where existing control mechanisms need to be reviewed and refined in order to enable the new strategy to be implemented effectively.

309 Our model suggests that this is where there needs to be a balance between risk taking and exercising control. A well articulated risk appetite will assist in defining the relative proportions of time, effort and resources that might need to be spent respectively on taking the risk and exercising control. By way of example, the company that decides that it has a large appetite for a given type of risk will determine at this level how to refine the way in which control mechanisms operate. A high appetite for, say, IT risk, which strategically results in major new systems developments will not mean that all control mechanisms should be thrown out. However, the level of detailed implementation of the controls, the levels of review and hierarchies of delegated authorities may well be more relaxed than in an organisation that continues to have a sceptical or hostile appetite for IT risk.

## **Project or operational**

310 At a detailed level of delivering products or services, following processes or running projects, it is likely that the emphasis will be on minimising adverse risk by exercising appropriate controls.

311 The preponderance of time, effort and resources will be deployed to minimise risk, rather than on taking new risks. However, even at this level it is important for individuals to understand how they are able to respond to new and emerging risks that they encounter and to have a risk appetite framework to help them to come to an appropriate decision. As one organisation describes it, they want front line supervisors to be able to respond to a new or emerging risk as though a member of the executive management team were standing at their shoulder. By defining risk appetite, staff will understand how they should react, and when they should escalate an issue for consideration further up the line.

## **Propensity to take risk**

312 At its most basic, the propensity to take risk is little more than understanding whether a risk or type of risk is one that the organisation wishes to engage with or not. Some organisations express this in simple terms such as:

- Avoid (terminate risk);
- Averse;
- Conservative;
- Receptive (take risk if expected reward warrants, within limits); or
- Unlimited (take risk if expected reward warrants, unconstrained by limits).

313 Others use words like “risk hungry” or “risk cautious”. However, some would argue that the propensity to take a risk is dependent on the reason for engaging with that particular risk or group of risks.

314 Risk appetite cannot be defined in totality for an organisation using simple one word labels. Risk-averse companies have little or no future, while risk-reckless organisations can expect a rapid exit from business. So, at the simplest level, the propensity to take any given risk can be defined by single word labels. At its most sophisticated it will take into account the reasons that organisations engage with any given risk and the nature of the risk itself.

## **Propensity to exercise control**

315 Having defined an organisation’s propensity to take risk, it is then important to establish its propensity to exercise control. It is our view that setting a risk appetite without identifying the level of control is a self-defeating exercise:

## Balanced Risk

Richard Anderson (Richard Anderson & Associates, 2009) argues that there are four main reasons for engaging with a risk:

- Taking more managed risk;
- Avoiding pitfalls;
- Because of the performance culture; and
- Because of the corporate ethics and behaviours.

In essence he argues that organisations engage with risks for one or more of these four reasons, each of which represents a different managerial challenge. It could be argued that many of the large international banks focused unduly on taking more managed risks, largely because of their performance cultures, rather than considering the pitfalls and their corporate ethics and behaviours. The issue, from a risk appetite perspective, was that they failed to understand the importance of balancing across these four reasons for engaging with risk and therefore exposed their businesses (and in the case of the banks, the entire economy) to an undue risk of failure.

Therefore, defining and measuring risk appetite would by default, for more sophisticated organisations, imply developing an understanding of why the organisation is engaging with a given risk or class of risks.

Another perspective on the propensity to take risk might be taken from Professor John Adams' taxonomy of risks as shown in the section on Risk Taxonomies. However, different organisations will have different appetites for the three types of risk defined by Adams.

There is a sense in which the classification of the risk into any of these three categories is effectively based on the experience of the organisation. Many things which are taken as read in say the nuclear industry, and which to staff would be a matter of routine (directly discernible risks) might be completely alien in another organisation where there is no prior knowledge or expertise in the firm or amongst its staff (virtual risks).

For some organisations, their appetite will be to stick to what they know best, expose themselves only to those risks visible through science where they have existing expertise on tap, and to the maximum extent possible, avoid virtual risks. Other organisations will want to exploit the potential of virtual risks by bringing the risk under managerial control.

- Traditionally risk “averse” organisations that decide they are “hungry” for a particular type of risk and that forget the need for retaining appropriate levels of control are likely to fail, sometimes dramatically;
- Traditionally innovative organisations that decide that they are “averse” to a particular type of risk and that forget to exercise or increase levels of control, are equally likely to fail.

316 Making risk appetite work depends on identifying the right level of control to match the risk aspirations. At a simple level, controls will have to match the risk appetite, so “risk hungry” might require “empowering controls”, whereas “risk averse” might require “harsh controls”. Empowering controls might be about high levels of delegation, minimal supervisory review and reporting by exception, whereas harsh controls might include regular detailed sign-off, re-performance, pre- and post-authorisation and detailed regular reporting. Clearly there is a myriad of different approaches in between.

317 In conclusion, the propensity to exercise control is the all vital counter-weight to the propensity to take risk. Taking risk cannot be considered without also contemplating control mechanisms. There is a range of possible approaches from the simple single-word definitions, through traditional accounting or other similar models, through to the COSO approach as outlined in their report on Internal Control (COSO, 1992). However, two new approaches that are worthy of consideration are that of analysing risk management clockspeed, and Dimensional Control.

### **Risk management clockspeed**

There has been considerable interest in the newly defined concept of Risk Management Clockspeed. Essentially the author of this concept, Keith Smith (Smith, 2010), argues that slow clockspeed risks, those that are managed over a lengthy period of maturation, are those that are managed most effectively through traditional control mechanisms. On the other hand fast clockspeed risks (those where there are unplanned or unexpected events that require a rapid response, or a response that is faster than internal processes are designed to manage) may require a different approach. In essence he argues that fast clockspeed risks need to be managed by cultural mechanisms as well as by process. The first stage of management will be to understand the heuristics (rules of thumb) that managers typically use to manage the fast clockspeed risks. These need to be assessed for efficacy, and then either changed or reinforced by rigorous training programmes so that the response to the risk is embedded into the culture of the organisation. Typically fast clockspeed risks, those that take a relatively short time from first identification through to impact, will by definition be subject to less data and will probably be less susceptible to pre-analysis.

It is quite plausible to think that many organisations focus on slow clockspeed risks in their risk management programmes and may give insufficient attention to fast clockspeed risks.

## Control Issues

Irrespective of risk clockspeed, there are many traditional ways of addressing control. COSO's report on Internal Control (COSO, 1992) provides a comprehensive approach, identifying five control components covering the control environment, risk assessment, control activities, information and communication, and monitoring. It also identifies preventive, detective and monitoring controls. At a more basic level, the traditional accounting models of control identify control objectives such as completeness, accuracy and timeliness. It is not the purpose of this booklet to identify all of the possible sources of information on approaches to control, but much work has been done to update this, for example the approach to Dimensional Control initially developed by Rob Baldwin of the LSE looks at five dimensions of control, each of which has several elements:

- **Strategy:** does the organisation focus primarily on the likelihood of the risk or on the impact by improving the resilience of the organisation?
- **People:** does the organisation expect nominated individuals to be responsible for a given risk, or is it about everyone in a team, department or organisation managing the risk?
- **Detail:** is the organisation focussed on a very specific risk, or is there a generic range of risks?
- **Tasks:** does the organisation collect information that underpins the way in which it addresses the control of a risk? Does it plan how to exercise control and what actions does it take?
- **Drivers:** is control driven by the managers of the organisation, by regulators or the various cultures that exist inside the organisation?

## Dimensions of control

These five dimensions and the elements of control are shown in the diagram below. Harsher control mechanisms will take a different route through this model than more enabling control mechanisms. This model provides one way for an organisation to consider how it can change its propensity to exercise control by changing its control journey through the Dimensional Control model.



## Measurement

318 We think that there is a need to develop a realistic measurement approach that will enable boards and managers alike to understand the ramifications of their risk appetite and whether breaches are material to the strategic direction of the company. We consider that there will be different approaches to measurement when it is considered at each of the three levels referred to above: strategic, tactical and operational.

## Strategic

319 At a strategic level we are suggesting that a model of shareholder value might be an appropriate measurement tool (Black, Wright and Bachman, 2000). The underlying shareholder value model we have adopted is shown below. The model is based on the hypothesis that shareholder value is calculated as the cashflow from operations, discounted by the weighted average cost of capital, less the value of debt.



Figure 5 - Shareholder Value Model (1)

320 Our proposition is that risks, which are normally associated in most ERM programmes to objectives, need also to be linked to the underlying shareholder value drivers as follows:

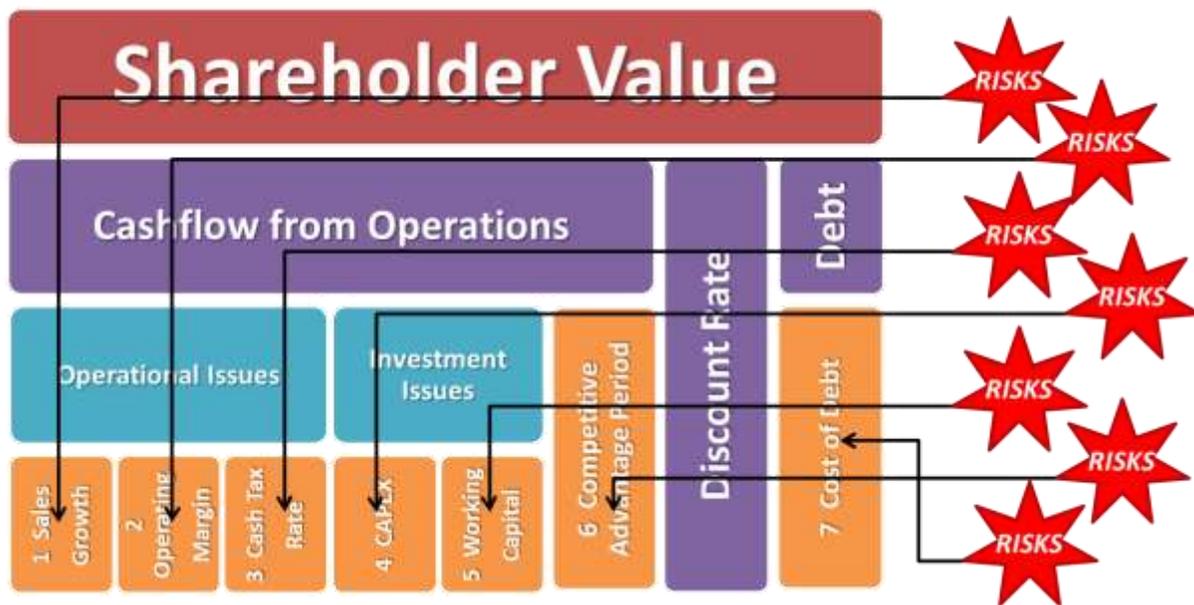


Figure 6 - Shareholder Value Model (2)

321 Although in practice, most risks will impact on several drivers as follows:

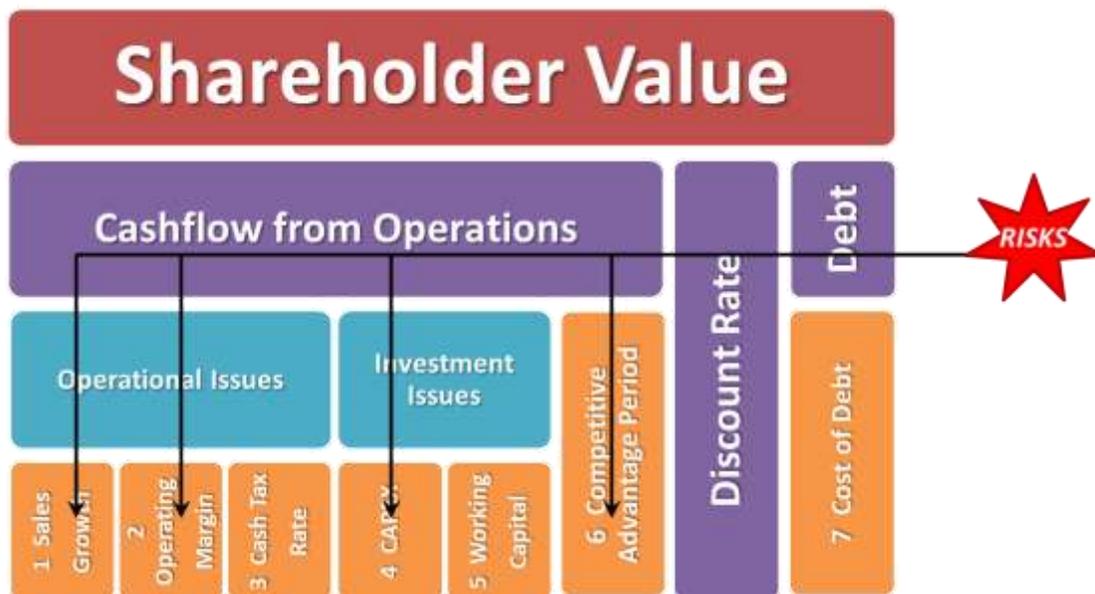


Figure 7 - Shareholder Value Model (3)

322 We think that testing risks against a model such as this will enable organisations to have a much better understanding of which risks are important at an early stage so that there is the maximum “wriggle room” in dealing with them. For example it might be that risk appetites could be expressed in terms of an acceptable deviation from the expected level of any one of the key value drivers. This might be expressed in terms of say, accepting a risk or series of risks which in aggregate might result in a decline in sales volumes of x%.

323 Shareholder value or (if organisations prefer) something like Economic Value Added (“EVA”) or economic capital, may be more sophisticated than is necessary for less mature organisations, and is clearly not appropriate in the context of public sector or some third sector organisations. We acknowledge that additional work may well be needed to identify public sector models that would be equally valid, but we do not think that this represents a significant shortcoming in the proposed model. We also recognise that this particular model may not be appropriate for many financial services organisations. However, the point is not the exact model, but rather the pursuit of underlying value drivers which need to be understood either for value creation or for value protection.

### **Tactical and operational**

324 We recommend that organisations should develop a series of key risk indicators (“KRI’s”) and key control indicators (“KCI’s”) to measure tactical and operational risks and controls. The concept of KRI’s and KCI’s is widely understood, although implementation is at best patchy. They should be relatively easy to implement in many organisations which already use key performance indicators (“KPI’s”) as part of their balanced scorecard management reporting information.

### **Data**

325 The approach to risk appetite has to become a data-driven exercise. Much of what currently passes for risk management is often a data-free or at best data-lite zone. Organisations that manage risk in this way will not be able to manage according to a pre-determined risk appetite. Accordingly we recommend that organisations should identify the relevant sources of data that will be required and ensure that there are appropriate levels of governance over those data sources to ensure that they are sufficiently robust to form the basis of a decision-influencing and report generating management tool.

326 All forms of measurement need to be tailored and appropriate to the environment within which they are being used. It is not our intention to recommend undue levels of complexity. However, as part of the regular reporting of risk appetite to senior management and boards, we believe that organisations need to develop the same level of rigour in reporting this information as they do in reporting periodic management accounts.

## **QUESTIONS FOR THE BOARDROOM**

1. What are the business, regulatory or other factors that will influence the relative importance of the organisation’s propensity to take risk and its propensity to exercise control at strategic, tactical and operational levels?
2. Does the organisation employ helpful risk taxonomies that facilitate the identification and responsibility for managing risk as well as providing insight on how to manage risks?
3. Does the organisation understand clearly why and how it engages with risks?
4. Is the organisation addressing all relevant risks or only those that can be captured in risk management processes?
5. Does the organisation have a framework for responding to risks?
6. What approach has the organisation taken to measuring and quantifying risks?

## IV Implementing a risk appetite

401 In this section of the booklet we are turning to the development of a risk appetite. We set out in Figure 8 below the seven stages of development for a risk appetite in an organisation:



Figure 8 - Stages of Development of Risk Appetite

402 The table below provides an overview of the seven-stage approach:

Stage	Main components
1. Sketch	Enough to engage with stakeholders
2. Stakeholder engagement	Engage with a full range of stakeholders
3. Develop	Using the risk appetite model set out in this paper
4. Approve	Approval from both the board and the risk oversight committee as appropriate
5. Implement	Ensure the metrics are right, communicate with those who need to work with the appetite and embed it into the fabric of the organisation
6. Report	Both internally and externally
7. Review	What worked well? What failed? What needs to be done differently next time?

## Sketch

403 Sketching a risk appetite framework is likely to require a reasonable degree of knowledge. For example, it would not be unreasonable to expect that an organisation:

- Should have defined and clearly articulated its core strategy;
- Would know its principal risks and the approach taken in managing them; and
- Would be able to describe with reasonable certainty the main features of its risk management maturity.

404 Ensuring that this detail is in place will enable a constructive statement of risk appetite to be developed using the main facets of the model described in Sections II and III of this paper.

## Stakeholder engagement

405 For some the “business of business is business” (attributed to Milton Friedman) and they will see no need to consult stakeholders apart from shareholders. For others who see a broader construct of the impact of business and government (and the third sector) on society, there may well need to be a broader range of consultation. For example, it might make sense to engage with others in the value chain, with (some) customers, and with others on whom your organisation depends. For some organisations, it will also make sense to engage with broader societal groups. For example, drilling oil wells offshore is likely now to raise deep concerns and being clear with residents and businesses about resilience in the event of oil spills would make considerable sense. For other organisations, it may well be that they wish to engage buy-side analysts engaged in the debate about risk appetite.

406 The purpose of engaging with stakeholders, however described and however broadly or narrowly defined, is to ensure that both the risk taking and the control activities are broadly aligned with others, or that potential divergences are identified early.

## Develop

407 The development of the risk appetite approach should now be well-informed by the background work, the preliminary sketch and the dialogue with relevant stakeholders. The amount of detail that is required will vary organisation to organisation. Of course, the detail needs to be tailored and proportionate to the organisation.

## Approve

408 If we are right in thinking that the development of risk appetite thinking in organisations has the potential to change the way that organisations are run, then it goes without doubt that boards, and in the event that they exist, risk oversight committees should review and approve the risk appetite document.

## Implement

409 Implementation is going to take some time. It is unlikely that an organisation will be able to get the risk appetite statement right first time. In particular the cultural aspects, the data gathering and the ramifications of divergences from the statement will need to be worked through.

## Report

410 We envisage that reporting against risk appetite statements will broadly take two forms:

- **Internal:** this will require reporting on a frequency similar to regular internal management reporting; and
- **External:** this will require annual reporting to relevant stakeholders, including (where they exist) shareholders, and perhaps others included in the stakeholder engagement stage above.

## Review

411 At the end of each reporting cycle, and before the risk appetite statement is re-sketches, there should be a review, perhaps undertaken by the board or the risk oversight committee into what worked well, what failed, and what needs to be done differently next time. Learning the lessons, especially in the early days of implementing a risk appetite statement will be critically important.

### QUESTIONS FOR THE BOARDROOM

1. Has the organisation followed a robust approach to developing a risk appetite?
2. Who are the key external stakeholders and have sufficient soundings been taken of their views? Are those views dealt with appropriately in the final documentation?
3. Is the risk appetite tailored and proportionate to the organisation?
4. Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?
5. What is the evidence that the organisation has implemented the risk appetite effectively?

## V Governing a risk appetite

501 The third strand of thinking that we want to touch on in this paper is the governance over a risk appetite statement. If a risk appetite is to be of any use to an organisation, it is essential that it is subject to good governance. We believe that there are four critical elements to the governance that need to be clearly articulated as set out in Figure 9 below:

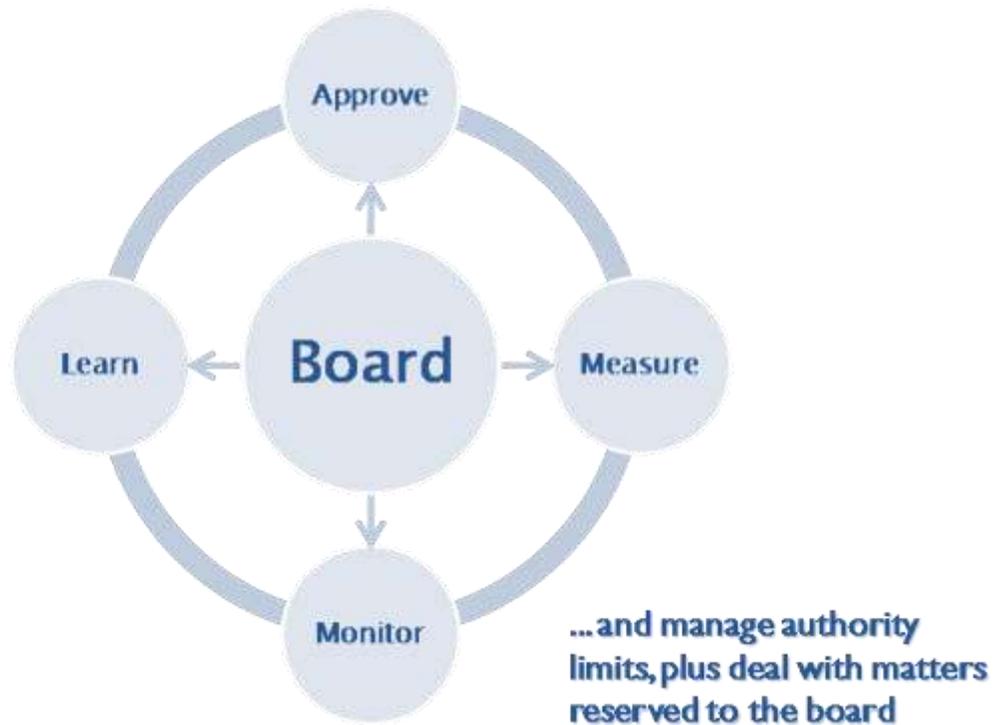


Figure 9 - Governing a Risk Appetite

Area for governance	Main components
1. Approve	Oversight of setting process
2. Measure	Measure and assess risk appetite to identify impact on business performance
3. Monitor	Identify breaches of, or tensions arising from risk appetite on a regular basis
4. Learn	What was good? What needs doing better? What needs changing

502 Our expectation is that the risk appetite document will be at the heart of the organisation. It will be informed by the vision of the company, and in turn will inform the way in which the operation will be managed as shown in the following diagram:

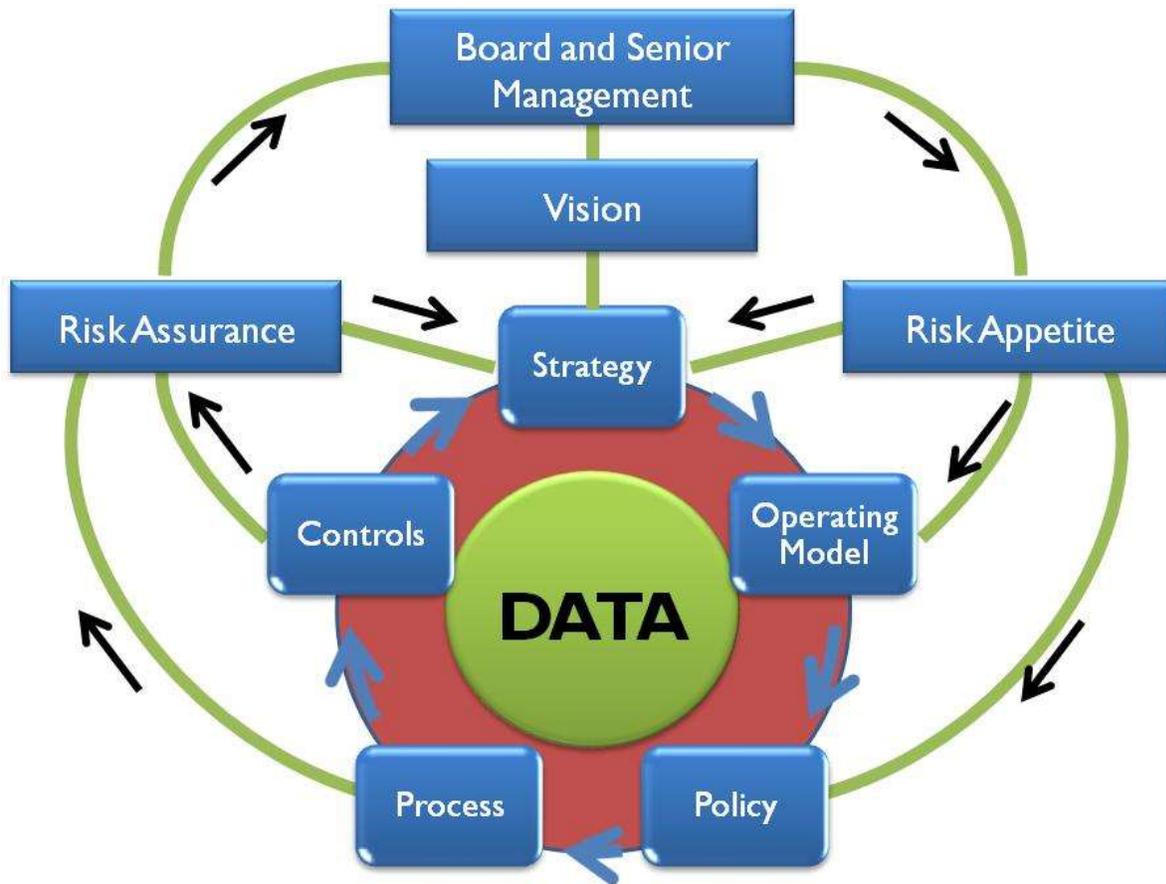


Figure 10 - Risk Appetite In the Organisation

503 With this in mind, we believe that it is of the utmost importance that the board (or risk oversight committee if it exists) should retain governance over the model at four key points:

- **Approval:** as discussed in the development of the risk appetite statement;
- **Measurement:** there needs to be regular and consistent measurement against the model and demonstration that the model is used in real life;
- **Monitoring:** the board will need to deal with breaches of the appetite, or tensions that arise from its implementation. If there are no breaches and no tensions then the likelihood is that it has not been properly developed.
- **Learn:** as discussed in the development section, the board needs to ensure that the organisation learns from the implementation of the risk appetite model so that it becomes more embedded into the organisation.

504 All of this needs to be carried out with the basic precept in mind that risk appetite can and will change over time as, for example, the economy shifts from boom to bust, or as cash reserves fall. In other words, breaches of risk appetite may well reflect a need to reconsider risk appetite part way through a reporting cycle as well as a more regular review on an annual cycle. Rapid changes in circumstances, for example as were witnessed during the financial crisis in 2008/9, would certainly indicate a need for an organisation to re-appraise its risk appetite.

### **QUESTIONS FOR THE BOARDROOM**

1. Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?
2. To what extent did the board identify tensions arising from the implementation of the risk appetite?
3. How much resource has it taken to develop and implement risk appetite? Was this level of resource appropriate? Does it need to be amended going forward?

## VI The journey is not over

601 It is our strong belief that the opportunity provided by the FRC for the development of risk appetite will potentially have enormous ramifications for the way in which organisations are run and for the development of assurance programmes. We have sought to fill a gap in the current guidance for directors and others in the development of risk appetite statements and we have included, as an Appendix to this report, a summary of how, in practical terms, a board might go about determining the risks it is willing to take. However there are a number of issues that we think are worth keeping in mind. In particular, risk appetite:

- Is as much about “enabling” risk taking as “constraining” adverse risks;
- Is a management tool as well as a governance requirement;
- Requires active “stakeholder” engagement;
- Needs to be built into “business as usual” processes;
- Should be approved by the board (or non-executive board risk committee)
- Has to be actively monitored by management
- Has to be reviewed regularly by the board; and
- Needs measurement tools and techniques.

602 But equally there are some substantial benefits. Risk appetite can help in:

- Safeguarding the organisation;
- Creating a framework for better decision making;
- Identifying issues at an early stage (allowing more wriggle room to deal with risks);
- Providing a framework for reducing surprises;
- Developing a model for structured thinking;
- Facilitating better achievement of long term objectives while respecting stakeholder views; and
- Bringing sense to the risk process.

603 Within IRM it is our intention to work with companies, boards, risk professionals, regulators and others to develop the thinking around risk appetite. For us the immediate next steps include:

- Developing a consensus as to what risk appetite means: this paper is just a first step in the discussion;
- Working with interested parties to develop appropriate mechanisms for measurement, including understanding:
  - the data sources that will be needed;
  - the impact on operational frameworks; and
  - the new data architecture and data governance models that will be required;
- The communications campaign that will include addressing the needs of boards and individual board members.

604 Above all, we want to hear from you. Please tell us what you think is good or bad about this paper, what needs to change, where you need further information or guidance and above all how we

can act as a support to boards and those that advise them in this important area of corporate governance.

### **QUESTIONS FOR THE BOARDROOM**

1. What needs to change for next time round?
2. Does the organisation have sufficient and appropriate resources and systems?
3. What difference did the process make and how would we like it to have an impact next time round?

## Bibliography

Adams, J. (2001). *Risk*. Routledge.

Black, Wright and Bachman. (2000). *In Search of Shareholder Value: Managing the Drivers of Performance*. Financial Times/Prentice Hall.

British Standards. (2008). BS31000 Risk Management Principles and Guidelines.

COSO. (1992). *Internal Control - Integrated Framework*. The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Financial Reporting Council. (2010, June). UK Corporate Governance Code.

Hindson, A. (2010, December). Developing a Risk Culture. *Risk Management Professional* .

ISO. (2002). Guide 73 Risk Management Vocabulary.

ISO. (2009). ISO 31000 Risk Management Principles and Guidelines.

Richard Anderson & Associates. (2009). *Risk Management and Corporate Governance*. OECD.

Smith, K. (2010). An introduction to risk clockspeed. *Institute of Risk Management Professional Development Forum*.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the express permission of the copyright owner.

©The Institute of Risk Management 2011

## Appendix: Determining the risks the board is willing to take

### Responsibilities for risk taking

1. The board of directors is responsible for the company's risk appetite and attitude to risk taking. It should do this by reference to the risk appetite that has been established for the company. The risk appetite may be defined by a series of risk criteria for the different types of risks faced by the company. Establishing the risk appetite and / or risk criteria will enable the board to determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board is responsible for monitoring compliance with the requirements of the risk appetite statement.
2. The risk appetite statement should be a driver of strategy at the most senior level. It should help with the development of plans for the implementation of strategy. It should also be used as a planning tool to develop tactics and plan change. Although the board cannot delegate responsibility for risk taking, a sub-committee of the board may have delegated authority for producing the risk appetite statement for board approval.
3. Management of the company at all levels is responsible for operating within the constraints established by the risk appetite statement. Management is responsible for ensuring that employees obey the rules regarding risk taking and operate within the limits of authority established by the risk appetite statement and the requirements of any Delegation of Authority arrangements. Management is also responsible for ensuring that the company operates a system of risk escalation when any specific risk exposure approaches the maximum level that the company is willing to tolerate.

### Process for managing risk taking

4. When establishing the risk appetite, there is a need to pay regard to the size, nature and complexity of the company and the business sector within which it operates. When determining the nature and extent of the risks that it is willing to take, the board's deliberations should include consideration of the following factors:
  - nature and extent of the risks facing the company;
  - extent and categories of risk it regards as acceptable for the company to bear;
  - likelihood of the risks concerned materialising;
  - company's ability to reduce the incidence and impact on the business of risks that do materialise; and
  - costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.
5. A risk appetite statement should be seen within the context of the risk management process. In particular, this statement is most relevant to the risk assessment stage. During risk assessments, a company will identify the significant risks it faces, analyse those risks and undertake an evaluation of the likely impact of each significant risk. The analysis of each risk will involve a consideration of how likely the risk is to materialise and the impact that would result.

6. Risk evaluation requires the company to compare the results of the risk analysis with a set of risk criteria that have already been established. These criteria will represent the risk appetite of the company, so that the risks the board is willing to take can be established. Application of the risk criteria should enable the company to develop and sustain:
  - efficient operations and activities
  - effective processes to deliver stakeholder expectations
  - strategic objectives capable of delivering the required outcomes
7. When developing the approach to the risks that it is willing to take, a company should have established procedures. These procedures will include establishing a risk appetite statement that clearly sets out the risk criteria that should be applied. In order to establish such a risk appetite statement, the following stages will be required:
  - undertake an assessment of the risks that the organisation is currently facing
  - report to the board the nature of the risks that are embedded within existing strategy, processes and operations
  - confirm that the risks that are currently being taken are within the risk appetite of the board and within the risk capacity of the company
  - use this analysis to develop and record the risk criteria that will form the basis of the risk appetite statement for the company
8. A company can develop criteria for the different categories of risks it faces and this will align with the willingness of the company to take those types of risks. If the risks are evaluated and analysed at the current or residual level, it is important that the critical controls applied to these risks are identified. Testing of those controls to ensure that they are efficient and effective will need to be undertaken.
9. When determining the nature and extent of the risks that it is willing to take, the company should pay regard to the:
  - current overall exposure of the company to risk
  - capacity of the organisation to take risk
  - limits of authorisation are in place for management
  - maximum risk exposure that the board is willing to tolerate in relation to any specific risk or category of risk
10. When developing the processes for developing a risk appetite statement and monitoring risk taking, the company should be aware that risk appetite can apply on three different levels, depending on the size, nature and complexity of the company and the business sector within which it operates:
  - risk appetite may be seen as a strategic driver for companies, especially if they operate in the financial sector
  - risk appetite or risk criteria establish a series of planning guidance to be used when determining tactics for the implementation of strategy, including decisions on the projects and programmes of work that will be undertaken
  - risk appetite also determines the operating limits and constraints (often expressed as the limits of authority for operational management) that apply to routine operations and may be established in a Delegation of Authority document