The Institute of Risk Management

Risk Appetite & Tolerance Guidance Paper

Crowe Horwath

Crowe Horwath Global Risk Consulting
Member Crowe Horwath International

irm

Leading the risk profession

Foreword

Leading the risk profession

Risk appetite today is a core consideration in any enterprise risk management approach.

As well as meeting the requirements imposed by corporate governance standards, organisations in all sectors are increasingly being asked by key stakeholders, including investors, analysts and the public, to express clearly the extent of their willingness to take risk in order to meet their strategic objectives.

The Institute of Risk Management, now in its 25th year, has a key role to play in establishing sound practices in this area and building consensus in what has, for too long, been a nebulous subject.

By providing practical advice on how to approach the development and implementation of a risk appetite framework we believe we will be helping boards and senior management teams both to manage their organisations better and to discharge their corporate governance responsibilities more effectively.

We are particularly pleased that a large number of professional bodies are supporting this work – risk is everyone's business and a common understanding and approach helps us work together to address this challenging area.

Alex Hindson
Chairman
The Institute of Risk Management

Crowe Horwath

Crowe Horwath Global Risk Consulting
Member Crowe Horwath International

While the Financial Reporting Council has kick-started the debate on risk appetite and risk tolerance in the UK, it is a debate that resonates around the world. As an integrated global risk consulting business, I can testify to the fact that our clients are debating risk appetite. That is why we are pleased to support the work of the Institute of Risk Management in moving this debate forward. We look forward to actively engaging with IRM and others in promoting this thought-provoking document and turning risk appetite into a day-by-day reality for boards and risk management professionals around the world.

Larry Rieger
CEO, Crowe Horwath
Global Risk Consulting

Chartered Institute of Internal Auditors

The Chartered Institute of Internal Auditors welcomes this contribution from the Institute of Risk Management to the debate on risk appetite and risk tolerance. In theory, the idea of deciding how much risk of different types the organisation wishes to take and accept sounds easy. In practice, it is difficult and needs ongoing effort both from those responsible for governance in agreeing what is acceptable and from all levels of management in communicating how much risk they wish to take and in monitoring how much they are actually taking. Anything that stimulates debate on the practical challenges of risk management is to be welcomed.

Jackie Cain
Policy Director
Chartered Institute of Internal Auditors

CIMA
Chartered Institute of Management Accountants

All successful organisations need to be clear about their willingness to accept risk in pursuit of their goals. Armed with this clarity, boards and management can make meaningful decisions about what actions to take at all levels of the organisation and the extent to which they must deal with the associated risks. But defining and implementing risk appetite is work in progress for many. CIMA therefore warmly welcomes this new guidance from the Institute of Risk Management as a sound foundation for developing best practice on this critical topic.

Gillian Lees
Head of Corporate Governance
Chartered Institute of Management Accountants (CIMA)

icsa. CHARTERED SECRETARIES

This document is an important contribution to a key area of board activity and helpfully addresses one of the issues highlighted in the Financial Reporting Council's Guidance on Board Effectiveness. ICSA is pleased to support the work started here by IRM, and looks forward to a well-informed debate and some useful conclusions.

Seamus Gillen
Director of Policy
Institute of Chartered Secretaries and Administrators (ICSA)

alarm
THE PUBLIC RISK MANAGEMENT ASSOCIATION

This paper will be helpful to senior managers in public service organisations who are trying to understand risk appetite in the context of their own strategic and operational decision making. In its recently published Core Competencies in Public Service Risk Management, Alarm identified the need to understand the organisation's risk appetite and risk tolerance, as part of the key function of identifying, analysing, evaluating and responding to risk. The 'questions for the boardroom', set out in this paper, could easily be translated into 'questions for the public organisation's senior executive committee' and as such may be of value to many Alarm members and their organisations.

Dr Lynn T Drennan
Chief Executive
Alarm, the public risk management association

CIPFA The Chartered Institute of Public Finance & Accountancy

CIPFA is pleased to endorse this work by IRM on risk appetite and tolerance which provides welcome leadership on a challenging subject for both the public and private sectors. We look forward to taking the debate further with our membership in pursuit of our commitment to sound financial management and good governance.

Diana Melville
Governance Adviser
Chartered Institute of Public Finance and Accountancy

Charterhouse Risk Management

This paper sends out a clear statement that the principle of risk appetite emanating from the board is the only effective way to initiate an ERM implementation. Charterhouse Risk Management is delighted to be associated with the launch of this paper after contributing to the consultation process. Our own experience with clients confirms that this approach is not only critical, but that the whole process must be undertaken with a practical rather than theoretical vigour. This is an essential ingredient of our delivery capability. References to 'appetite' and 'hunger' only reinforce the living nature of the required approach.

Neil Mockett
CTO
Charterhouse Risk Management

Introduction

This guidance 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 supplemented by much virtual debate 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 circulated an early draft of this paper to in excess of fifty individuals. We have also exposed it for a much wider consultation from which we received many responses (see list of people and organisations responding in Appendix B).

From this development process, we are confident that we are dealing with a topic that is relevant to many people in many organisations of different types in all sectors and that there is sufficient consensus on issues and approaches emerging to be able to publish this guidance. 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 to assist in boards' deliberations on the subject of risk appetite and tolerance. The paper consists of an executive summary, which is designed to provide an overview on the subject for general use, particularly by board members, and a more detailed document which is primarily designed to assist those whose task it is to advise boards on these matters.

The full version of this document is available for free download from the website of the IRM and from partner organisations. Printed versions of the executive summary are also available.

The original intent of this paper was 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, feedback from the consultation process has shown that there is considerable interest in this topic in the public sector as well as the private sector and beyond the UK. While some specifics might differ, the underlying principles hold true for all sectors and all geographical locations.

We have found that the approach contained in here has far reaching resonance with anyone who is interested in the subject of risk appetite and tolerance. This is not a subject with an untarnished history: most UK banks would have been expected to define their risk appetite, but 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. We are now poised to move beyond that thinking. 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 serious attention. One of the purposes of this document is to begin to provide a common vocabulary for people who wish to discuss this subject both within their organisations, and also in comparing organisations.

Members of the Working Group

Richard Anderson, deputy chairman of IRM and managing director of Crowe Horwath Global Risk Consulting

Bill Aujla, CRO at Etisalat

Gemma Clatworthy, senior risk consultant at Nationwide Building Society

Roger Garrini, audit manager at Selex Galileo

Paul Hopkin, director of IRM and technical director of AIRMIC

Steven Shackleford, senior academic in audit and risk management at Birmingham City University

John Summers, chief advisor – risk at Rio Tinto

Carolyn Williams, head of thought leadership at IRM

In writing this paper, we are conscious that we may appear to have come at this originally from a UK, quoted company-centric perspective and that this is counter to IRM's broad sectoral appeal and international ethos. In fact, while this guidance was originally written with the UK Corporate Governance Code in mind, comments and revisions arising from the consultation process mean that it is applicable to all sectors in all geographies. We continue to welcome feedback from readers in this regard.

Our objective in writing this document has been to give:

1. A theoretical underpinning to the subject of risk appetite; but
2. More importantly, to provide 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 organisation is run.

This guidance is not definitive: we do not think that we have written 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 should be a fundamental business concept that could 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 approach of the new UK Corporate Governance Code 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. I am, of course, particularly pleased that other professional bodies of considerable repute agree sufficiently with our approach to put their names also to this document.

Richard Anderson

Deputy Chairman
The Institute of Risk Management
September 2011

About IRM

The **Institute of Risk Management** (IRM) is the world's leading enterprise risk management 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 board level 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 in the private, third and public sectors.

About the Author

Richard Anderson, the principal author of this booklet, is Deputy Chairman of IRM. Richard is also Managing Director of Crowe Horwath Global Risk Consulting in the UK. A Chartered Accountant, and formerly a partner at a big-4 practice, 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 and 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.

Contents

Table of Figures

Executive Summary

Principles and approach

The following key principles have underpinned our work on risk appetite:

1. Risk appetite can be **complex**. Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it.
2. Risk appetite needs to be **measurable**. Otherwise there is a risk that any statements become empty and vacuous. We are not promoting any individual measurement approach but fundamentally it is important that directors should understand how their performance drivers are impacted by risk. Shareholder value may be an appropriate starting point for some private organisations, stakeholder value or 'Economic Value Added' may be appropriate for others. We also anticipate more use of key risk indicators and key control indicators which should be readily available inside or from outside the organisation. Relevant and accurate data is vital for this process and we urge directors to ensure that there is the same level of **data governance** over these indicators as there would be over routine accounting data.
3. Risk appetite is **not a single, fixed concept**. There will be a range of appetites for different risks which need to align and these appetites may well vary over time: the temporal aspect of risk appetite is a key attribute to this whole development.
4. Risk appetite should be developed in the context of an organisation's **risk management capability**, which is a function of **risk capacity** and **risk management maturity**. 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 to their systems and processes, and partly due to the nature of their business. However, until an organisation has a clear view of both its risk capacity and its risk management maturity it cannot be clear as to what approach would work or how it should be implemented.
5. Risk appetite must take into account differing views at a **strategic**, **tactical** and **operational** level. 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.
6. Risk appetite must be **integrated** with the control culture of the organisation. Our framework explores this by looking at both the **propensity to take risk** and the **propensity to exercise control**. The framework 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.

"It is often said that no company can make a profit without taking a risk. The same is true for all organisations: no organisation, whether in the private, public or third sector can achieve its objectives without taking risk. The only question is how much risk do they need to take? 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 latest UK Corporate Governance Code issued by the Financial Reporting Council in 2010."

Risk and control

We think that this dual focus on taking risk and exercising control is both innovative and critical to a proper understanding of risk appetite and risk tolerance. The innovation is not in looking at risk and control – all boards do that.

The innovation is in looking at the interaction of risk and control as part of determining risk appetite. 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 pre-occupation of many risk management programmes, which is the avoidance of harm.

Risk appetite and Performance

Our view is that both risk appetite and risk tolerance are inextricably linked to performance over time. We believe that while risk appetite is about the pursuit of risk, risk tolerance is about what you can allow the organisation to deal with.

Organisations have to take some risks and they have to avoid others. The big question that all organisations have to ask themselves is: just what does successful performance look like? This question might be easier to answer for a listed company than for a government department, but can usefully be asked by boards in all sectors.

The illustrations on these pages show the relationship between risk appetite, tolerance and performance. Diagram 1 shows the expected direction of performance over the coming period. Diagram 2 illustrates the range of performance depending on whether risks (or opportunities) materialise. The remaining diagrams demonstrate the difference between:

- all the risks that the organisation might face (the "risk universe"- diagram 3)
- those that, if push comes to shove, they might just be able to put up with (the "risk tolerance" - diagram 4) and
- those risks that they actively wish to engage with (the "risk appetite" - diagram 5).

We believe that the appetite will be smaller than the tolerance in the vast majority of cases, and that in turn will be smaller than the risk universe, which in any case will include "unknown unknowns".

Risk tolerance can be expressed in terms of absolutes, for example "we will not expose more than x% of our capital to losses in a certain line of business" or "we will not deal with certain types of customer ".

Risk appetite, by contrast is about what the organisation does want to do and how it goes about it. It therefore becomes the board's responsibility to define this all-important part of the risk management system and to ensure that the exercise of risk management throughout the organisation is consistent with that appetite, which needs to remain within the outer boundaries of the risk tolerance. Different boards, in different circumstances, will take different views on the relative importance of appetite and tolerance.

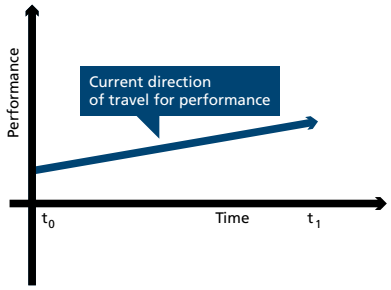


Diagram 1

Diagram 2

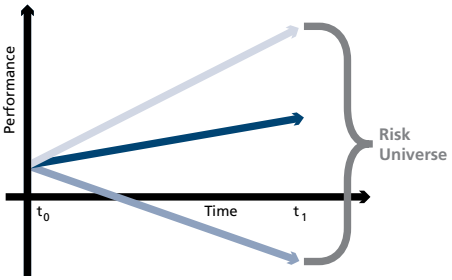


Diagram 3

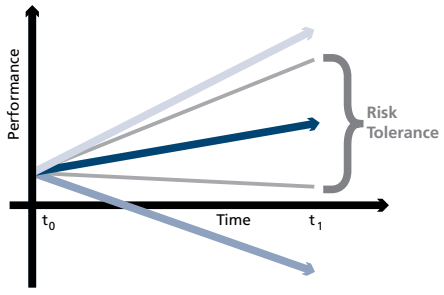


Diagram 4

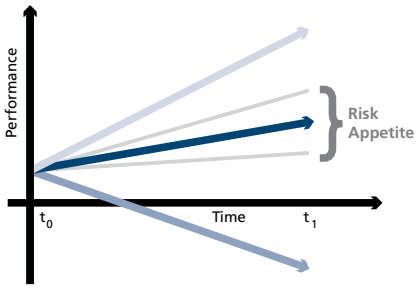


Diagram 5

Putting it into practice

We have sought to develop an approach to risk appetite that:

- is theoretically sound (but the theory can quickly disappear into the background)
- is 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
- will make a difference.

Boardroom debate - we suspect that in the early days particularly, a successful approach to reviewing risk appetite and risk tolerance in the boardroom 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 will diminish into a mere tick-box activity – and nobody needs any more of those in the board room. It is essential that 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 not a one-size-fits-all approach.

Consultation - in our paper we have set out an illustrative process for the development of an approach to risk appetite. This includes appropriate consultation with those 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.

Risk Committees - in his 2009 *Review of Corporate Governance in UK Banks and Other Financial Industry Entities,* Sir David Walker recommended that financial services organisations should make use of board risk committees. The Economic Affairs Committee of the House of Lords recently suggested that large organisations in other sectors should also consider creating such committees. We think that the creation and monitoring of approaches to risk appetite and risk tolerance should be high on the agenda of these committees. In the detailed document, we have included a brief section on the role of the board or risk committee: we are suggesting that governance needs to be exercised over the framework at four key points: approval, measurement, monitoring and learning.

Flexibility - 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, might also indicate a need for an organisation to re-appraise its risk appetite. In a fast changing economic climate, it is especially important for firms to have not only a clearly defined strategy, but also a clearly articulated risk appetite framework so that they are able to react quickly to the challenges and opportunities presented during such times.

Five tests for risk appetite frameworks

"The risk appetite statement is generally considered the hardest part of any Enterprise Risk Management implementation. However, without clearly defined, measurable tolerances the whole risk cycle and any risk framework is arguably at a halt."

Jill Douglas, Head of Risk, Charterhouse Risk Management

In summary, there are five tests that Directors should apply in reviewing their organisation's risk appetite statement:

1. Do the managers making decisions understand the degree to which they (individually) are permitted to expose the organisation to the consequences of an event or situation? Any risk appetite statement needs to be practical, guiding managers to make risk-intelligent decisions.
1. Do the executives understand their aggregated and interlinked level of risk so they can determine whether it is acceptable or not?
2. Do the board and executive leadership understand the aggregated and interlinked level of risk for the organisation as a whole?
3. Are both managers and executives clear that risk appetite is not constant? It changes as the environment and business conditions change. Anything approved by the board must have some flexibility built in.
4. Are risk decisions made with full consideration of reward? The risk appetite framework needs to help managers and executives take an appropriate level of risk for the business, given the potential for reward.

We believe that by following the guidance set out in detail in our document, directors will be able to be confident that they can pass all of those five tests.

Questions for the boardroom

Below we set out some questions that we think boards may want to consider, as part of an iterative process over time, as they develop their approaches to risk appetite and which will enable them to remain at the forefront of the discussion. One clear outcome from our consultation exercise was that, despite the expected variation in views on the technical aspects of risk appetite, there was a common acceptance of these questions as a useful starting point for board discussion.

Background

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

Designing a risk appetite

6. Has the board and management team reviewed the capabilities of the organisation to manage the risks that it faces?
7. What are the main features of the organisation's risk culture in terms of tone at the top? Governance? Competency? Decision making?
8. Does an understanding of risk permeate the organisation and its culture?
9. Is management incentivised for good risk management?
10. How much does the organisation spend on risk management each year? How much does it need to spend?
11. 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?

Constructing a risk appetite

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?

Implementing a risk appetite

15. 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?
16. Has the organisation followed a robust approach to developing its risk appetite?
17. Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?
18. Is the risk appetite tailored and proportionate to the organisation?
19. What is the evidence that the organisation has implemented the risk appetite effectively?

Governing a risk appetite

20. Is the board satisfied with the arrangements for data governance pertaining to risk management data and information?
21. Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?
22. Does the board have, or does it need, a risk committee to, inter alia, oversee the development and monitoring of the risk appetite framework?

The journey is not over - final thoughts

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

Hungry for risk?

The word "appetite" brings connotations of food, hunger and satisfying one's needs. We think that this metaphor is not always helpful in understanding the phrase "risk appetite". When those two words appear together we think it is more appropriate to think in terms of 'fight or flight' responses to perceived risks. Most animals, including human beings, have a 'fight or flight' response to risk. In humans this can be over-ruled by our cognitive processes. Our interpretation of risk appetite is that it represents a corporate version of exactly the same instincts and cognitive processes. However, since these instincts are not "hardwired" in our corporate "nervous and sensory" systems we use risk management as a surrogate.

I Background

"What is this all about?"

101 In recent years we have witnessed some major risk events ranging from the global financial crisis to the more recent sovereign debt crisis and a large number of natural and meteorological events with major consequential damage and knock-on effects. But the financial crisis of 2008 had many consequences, and raised many questions, 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 tolerance by any other name.

102 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 of this document look at a proposed new framework 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
- Appendix A 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

103 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...

104 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.

105 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 we might infer that 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" might lead the reader to surmise that the risk appetite element is one of the reasons that organisations require risk systems. Overall this is a radical new departure for the FRC and introduces a new concept for many directors and boards of non-financial services organisations.

106 As an aside, it seems that the terms "risk appetite" and "risk tolerance" have deep associations with the financial services industry in some minds, and attempts to move non-financial services organisations in that direction might have been difficult. However these words can be seen, for all intents and purposes, as being indistinguishable from the previous phrases. While many commentators see them as inseparable phrases, 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 and tolerance.

How has "risk appetite" been used before?

107 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 work that was undertaken in writing 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. Some people prefer other terms such as risk attitude or risk capacity. As far as we are concerned there is nothing fundamentally wrong in using any of these terms. Suffice it to say that in writing this guidance we are taking a very pragmatic view: risk appetite is the most common phrase that we have come across, it is the one that was used by the FRC in the context of the draft Corporate Governance Code and therefore we would prefer to define this term in a way that begins to make sense for as many people as possible.

108 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[1] (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." Some people argue that ISO31000 is silent on the subject of because it is neither a useful phrase not a meaningful concept. They therefore focus more on risk criteria. On the other hand, we believe that there is a benefit from exploring what we think is turning out to be a useful and meaningful concept.

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

[1] At the time of writing, this document is undergoing revision. Nevertheless the approach in the 2008 document has proved most useful for this discussion.

109 The original BS31100 contained more detail. It defined 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 went 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".

110 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.

111 We are concerned that this focus treats risk in an unduly negative way, something which we are challenging in this booklet in the sense that there should be a maximum tolerance for risk taking as well as risk avoidance.

112 While neither standard is very informative, it is instructive to see how the "appetite" word or similar words were used in the original 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:

1. "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
2. "The organisation's risk appetite should be established and/or approved by the board (or equivalent) and effectively communicated throughout the organisation

113 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. It is interesting to note that the revised version of BS31100 has substantially removed references to risk appetite to bring it in line with ISO31000. This leaves something of a vacuum on the subject, which this guidance seeks to fill.

Risk "appetite" and risk "tolerance"

114 Before we started on this project, it was our belief that we, and more importantly directors and risk professionals, could easily distinguish between risk appetite and risk tolerance and that the former was the more complicated concept. In practice we have found that in many instances these terms are used inter-changeably. We think that is conceptually wrong: there is a clear difference between the two. It is also 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 allow the organisation to deal with. Without a doubt there will be occasions where an organisation can deal with more risk than it is thought prudent to pursue.

115 The difference can be illustrated in the diagrams on the bottom of this page.

116 Figure 1 shows performance from the current time (t_0) to sometime in the future (t_1). The line **AB** shows the current expected direction of travel in terms of performance. Figure 2 shows that in practice this is subject to risks which, should they materialise, could result in performance along the line **AC**, or to opportunities (positive risks) which could result in performance along the line **AD**. The potential risk universe or the total risk exposure is shown by the difference between **C** and **D**. (see Figure 3)

117 What is clear is that following line **AC** is not desirable. Less clear is that it might also be undesirable to follow line **AD** because pursuing it might throw up substantial additional risks. Consequently, there are some risk outcomes for which there is no tolerance, and moreover no tolerance for taking those risks. Moreover, since we are using the generally accepted concept of risk as being potentially positive as well as negative, that suggests that there is a range shown by the triangle **AXY** (See Figure 4), outside of which the organisation will not tolerate exposure. This is the **risk tolerance.**

118 On the other hand, our "appetite" for risk is likely to be shown by a narrower band of performance outcomes shown by the triangle **AMN**.

119 Risk tolerance can therefore be expressed in terms of absolutes: for example "we will not expose more that x% of our capital to losses in a certain line of business", or "we will not deal with a certain type of customer". Risk tolerance statements become "lines in the sand" beyond which the organisation will not move without prior board approval.

120 Risk appetite on the other hand is about what the organisation **does** want to do and how it goes about it. It therefore becomes the board's responsibility to define this all important part of the risk management system and to ensure that the exercise of risk management and all that entails is consistent with that appetite, which needs to remain within the outer boundaries of the risk tolerance.

121 While we have focused primarily on risk appetite, some entities (such as Government departments) may be more focused on risk tolerance. This in itself becomes a more complicated issue where the risk of insolvency (the ultimate determination of failure for corporates) is absent. Defining success and failure is therefore very important. This is an area where we believe further work is required. 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.

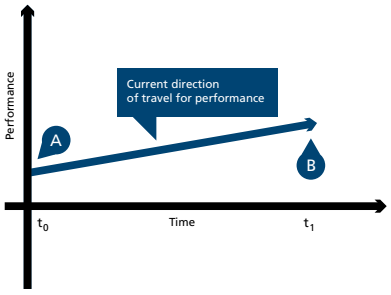


Figure 1 - Performance over time

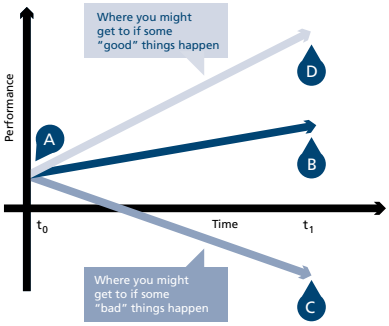


Figure 2 - Possible outcomes

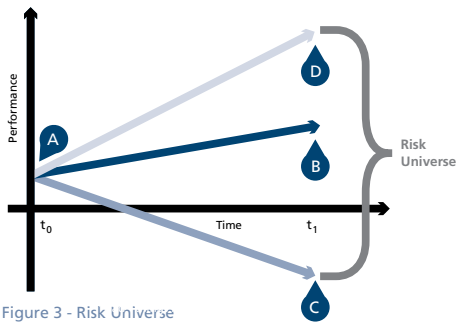


Figure 3 - Risk Universe

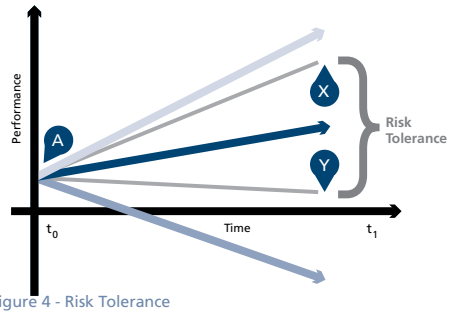


Figure 4 - Risk Tolerance

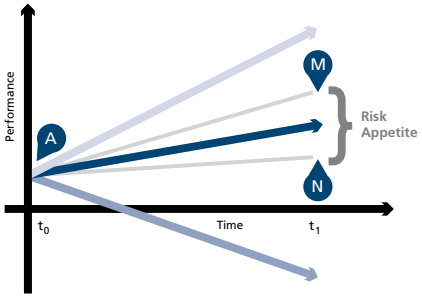


Figure 5 - Risk Appetite

A word of caution

122 The word "appetite" brings connotations of food, hunger and satisfying one's needs. We think that this metaphor is not always helpful in understanding the phrase "risk appetite". When those two words appear together we think it is more appropriate to think in terms of "fight or flight" responses to perceived risks.

Most animals, including human beings have a "fight or flight" response to risk. In humans this can be over-ruled by our cognitive processes. Our interpretation of risk appetite is that it represents a corporate version of exactly the same instincts and cognitive processes. Except of course, as a legal fiction(as opposed to biological reality) organisations do not have their own brains, nervous systems, sensory organs and instincts. They 'borrow' these from members of their boards and from their employees.

These systems have to be created in terms of interactions of people, data systems and management information which enable people in the organisation to act as if they were parts of the same physical organism.

Conclusion

123 There are four early conclusions that we have drawn from the work we have undertaken in preparing this guidance:

- The first is that we would benefit from a renewed focus on defining the terms that we are using. We have therefore developed glossaries of key terms and phrases which appear throughout this guidance.
- The second 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 third 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 fourth 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.

Key Terms and Phrases

124 In this section we have used three key terms which we will continue to use throughout the document. In the absence of helpful definitions elsewhere, we are defining them as set out here:

Phrase	Meaning
Risk appetite	The amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives.
Risk tolerance	The boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives.
Risk universe	The full range of risks which could impact, either positively or negatively, on the ability of the organisation to achieve its long term objectives.

125 It is our expectation that for most organisations, the risk appetite will be smaller than the boundaries depicted by its risk tolerance.

The rest of this document

126 We have set out a route through this topic of risk appetite in the rest of this document as follows 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

Section VI: The journey is not over

In **Section VI** we explore some of the issues that we will need to explore as we develop this concept as a boardroom topic over the coming years.

Background - Questions for the Boardroom

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

II Designing a risk appetite

"The Building Blocks"

201 In developing a possible framework 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 is a broad consensus that there is no single risk appetite, but rather **a range of appetites** for different types of risk and this range of appetites needs to align under, and be consistent with, an overall risk appetite framework. 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. Risk appetite is not something that can be written in tablets of stone and then ignored for the rest of the year. Equally, the risk appetite for tomorrow may be very different to the risk appetite for a period ten or twenty years hence.
- 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 appears repeatedly in BS31100: organisations should develop a tailored and proportionate response. We have defined this in terms of **risk capability**, which is a function of **risk capacity** and **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. Recognising where your organisation sits on this spectrum is an important first step in developing and articulating risk appetite.

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 framework is depicted in the diagram below:

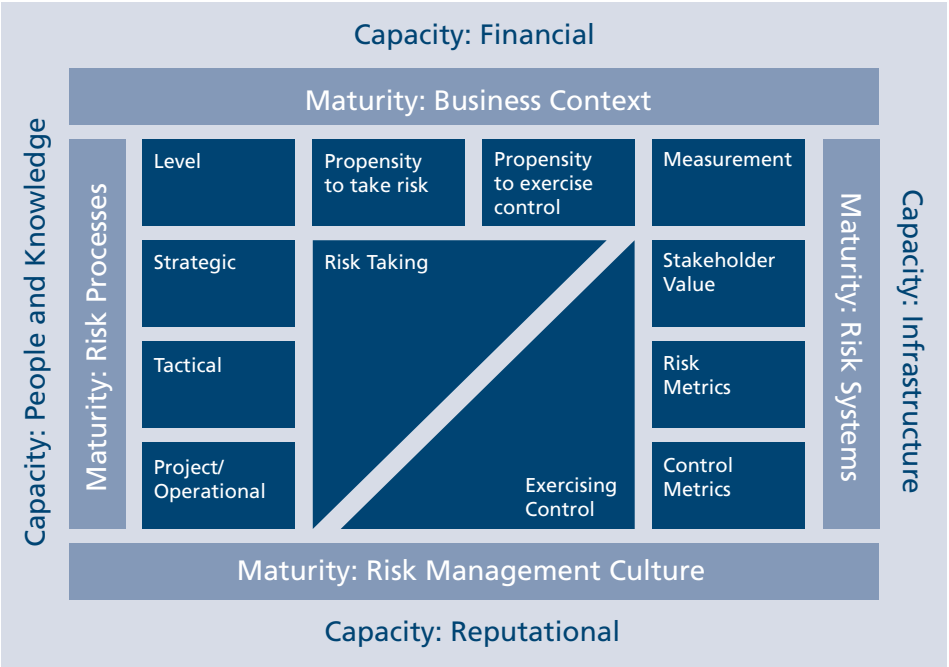


Figure 6 - Risk Appetite in Context

203 This framework has several key features:

1. It is our view that risk appetite should be established in the context of what we are calling the risk capability of the organisation. Risk capability is a function of risk capacity: the ability to carry risks, and the risk management maturity to manage them.

a. Risk capacity might be defined in terms of items such as, for example, assets and liabilities, reputation, liquidity or political capital.

b. On the other hand, while an organisation might have the capacity it equally needs to have the risk management or organisational maturity to manage risks, which we are calling the risk management maturity of the organisation. 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" framework 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:

a. Business context

b. Risk management culture

c. Risk management processes

d. Risk management systems

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 framework explores this by looking at both the propensity to take risk and the propensity to exercise control. The framework 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 framework 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.

Risk Capacity

204 There is little advantage in having a substantial appetite, or indeed tolerance for risk, unless the capacity to manage it also exists. In traditional terms, risk capacity is a concept which has been closely associated with the insurance industry: at what level of deductible does a policy need to kick-in in order to protect the balance sheet or (in more limited circumstances) the income statement of the organisation? What is the maximum extent of insurance cover that is required? And so on. In this document, we are extending this concept beyond the direct financial consequences. We see capacity as being an enabler of risk taking as well as a cushion for risk loss-events. We also see it as having non-financial dimensions, which might include items such as:

a. **Reputation:** an organisation needs to have the wherewithal from a reputational perspective both to achieve its objectives and withstand pressures as they arise.

b. **Political:** in some cases an organisation may require political space in order to achieve its objectives. Equally, it may require political tolerance in the event of adverse effects from risk events materialising.

c. **Infrastructure**: an organisation must have sufficient infrastructure to take certain risks. This might be in terms of physical assets, IT systems or network partners.

d. **People**: an organisation will need to assess whether or not they have sufficient, appropriately trained and skilled individuals to undertake some risks.

e. **Knowledge**: in many cases the management of risk requires specific knowledge either within, or available to, an organisation.

An Example

In the nineties, GEC came under new management, who undertook a wholesale re-shaping of the portfolio of businesses. With a change of name to Marconi, they moved increasingly away from their traditional manufacturing and defence businesses towards telecoms and internet businesses. It might well be argued, given the subsequent failure of the group, that they lacked the risk capacity to move into new strategic areas about which some of the management team had little knowledge.

205 It might be argued that understanding risk capacity reflects the level of maturity of an organisation's skills in strategic and business planning. In a fast changing economic climate, it is especially important for firms to have a clear, defined strategy and risk appetite framework so that they can react quickly to the challenges and opportunities presented in such times.

Three Illustrative Examples of Risk Capacity

	Financial Services Organisation	**FMCG Organisation**	**Public Sector Organisation**
Illustrative situation	Developing new product for rapid launch	Building new factory to serve new market	Implementing new policy initiative
Financial	Does the firm have sufficient capital to support the product?	Can the firm afford the development and how will it remit funds back to the ultimate holding company?	What is the impact on public sector costs? Are there any taxation or borrowing implications?
Reputation	Will the product be acceptable to the relevant customer base? Does the firm have a history of product innovation in this sector to this group of consumers?	Are there any ethical, environmental or social issues in building the factory in this location and which could have an adverse impact on indigenous populations?	What is the track record of the department in rolling out such policy initiatives?
Political	How does this product innovation stack up against government policy? Is there likely to be any political antagonism towards the product?	What is the impact on employment, taxation and so on in the "home" territory and the "host" territory? Does the company have a record of bringing such projects to fruition?	What are the voter ramifications of success and failure?
Infrastructure	Does the firm have the necessary capability in terms of marketing, sales, complaints handling, processing etc?	Does the group have the wherewithal to get manufactured product from the plant to end customers? Is any new infrastructure required, eg roads, railways, port facilities?	How quickly (or slowly) does the policy implementation need to be rolled out from inception, through trial to full implementation?
People and Knowledge	How many new people will be required? How will they be trained? What skills do they need?	How can knowledge be transferred to the new work force? What management skills are required?	Does this require major recruitment? What are the implications for public sector spending?

Risk Management Maturity

206 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.

207 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:** This includes understanding the state of development of the business, its size, industry sector, geographical spread and the complexity of the business model. 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 engaging with and how much more it might wish to engage with in the future.
- **Risk management culture:** This addresses 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. 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:** This refers to the extent to which there are processes for identifying, assessing, responding to and reporting on risks and risk responses within the organisation. 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:** This means the extent to which there are appropriate IT and other systems to support the risk management processes. 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.

208 It is our view that risk management data and its subsequent processing to generate actionable management information must be subject to the same rigour in terms of data governance as is applied to the data and information that is used in accounting and reporting systems.

Area of focus	Factors to consider
Business context	• Nature of business • Size of business • Geographical spread of operations • Degree of virtualisation • Complexity of value chain • Interdependencies with other partners • Political climate • Regulatory environment • Competitive environment • Risk clockspeed (see page xx)
Risk management culture	• Tone from the top • Attitudes to governance in the organisation • Attitudes to the management of risk • Attitudes to control • Attitudes to regulation • Attitudes to innovation • Competencies and capabilities
Risk management processes	• Identification processes • Assessment processes • Monitoring and reporting processes • Common language • Extent of common processes • Delegations of authority • Integration with strategy and business planning • Integration with regular periodic reporting • Escalation procedures
Risk management systems	• Extent of organisational structure to facilitate the management of risk • Risk management strategy and policy defined • IT support systems • Enterprise data warehouse for risk data • Risk reporting
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

209 We believe that it is almost impossible to encapsulate risk appetite for a business as a whole 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.

210 The framework that we have depicted in Figure 6 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 framework 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 framework 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

211 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.

212 To meet the criteria of embedding risk management it is important for remuneration to be directly linked to good control of risks. It is recognised that not all risk appetites and thresholds will be quantitative, but where they are they can be directly linked to bonus payments. In this way when thresholds are breached the business unit and associated team members will be able to see the impact of decisions taken. Conversely, good risk management can be evidenced and appropriately rewarded.

Key terms and phrases

213 In this section we have introduced five key phrases, which we are defining as set out in the following table:

Phrase	Meaning
Risk capability	A function of the risk capacity and risk management maturity which, when taken together, enable an organisation to manage risk in the pursuit of its long term objectives.
Risk capacity	The resources, including financial, intangible and human, which an organisation is able to deploy in managing risk.
Risk management maturity	The level of skills, knowledge and attitudes displayed by people in the organisation, combined with the level of sophistication of risk management processes and systems in managing risk within the organisation.
Propensity to take risk	The extent to which people in the organisation are predisposed to undertaking activities the impact, timing and likelihood of which are unknown, and which is influenced by financial, cultural, performance and ethical considerations.
Propensity to exercise control	The extent to which people in the organisation are predisposed to take steps to change the likelihood, timing or impact of risks, influenced by financial, cultural, performance and ethical considerations.

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:

Risk Culture Diagnostic	
Tone at the Top Risk Leadership Responding to bad news	**Governance** Risk governance Risk tranparency
Competency Risk resources Risk competence	**Decision Making** Risk decisions Rewarding appropriate risk taking

Figure 7 - 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.

Designing a Risk Appetite - Questions for the Boardroom

- Has the board and management team reviewed the capabilities of the organisation to manage the risks that it faces?
- What capacity does the organisation have in terms of its ability to manage risks? Are there any particular issues of which the board should be aware?
- 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?
- What specific factors should the risk appetite take into account in terms of the business context? Risk Processes? Risk Systems? Risk management maturity?
- At which levels would it be appropriate for the board to consider risk appetite?
- What are the main features of the organisations risk culture in terms of tone at the top? Governance? Competency? Decision making?
- How much does the organisation spend on risk management each year? How much does it need to spend?
- Does an understanding of risk permeate the organisation and its culture?
- Does each individual understand their role and responsibility for managing risk?
- At a managerial level, do you know what level of risk you should take? Do you know who the risk owners are? Do they have systems in place for measuring and monitoring risk?
- Is management incentivised for good risk management?

III Constructing a risk appetite
"Managing the right levers"

301 In Section II of this paper we explored the main issues in designing the risk appetite framework: in this section, we look at each of the main elements in the middle of the framework in more detail.

302 At the heart of the risk appetite framework, once an organisation understands their capability to manage risk, 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:

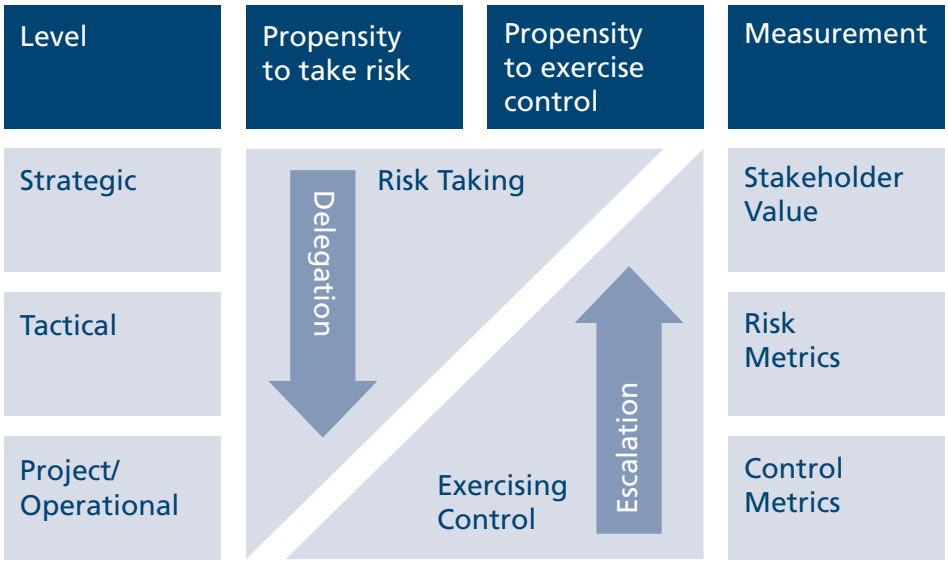


Figure 8 - Risk appetite - Main Issues

Levels of risk appetite

Strategic

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

304 At a strategic level, risk appetite is predominantly about the risks or types of risks that an organisation has a comparative advantage in managing (or indeed knowing that they can neither manage nor mitigate). These 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:

- Risks in connection with decisions about outsourcing or maintaining processes and competencies in-house.
- Risks concerning new product developments, such as new innovations, R&D, new product lines.
- Risks concerning new sources of finance, such as the optimal debt:equity ratio, banking covenants, headroom and liquidity.
- Risks concerning acquisitions or disposals including the likelihood of achieving organisational objectives or destroying shareholder value.

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 will 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 risk avoidance.

306 Figure 8 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.

Risk Taxonomies

There are many 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
Classification	• Directly Discernible • Visible through Science • Virtual	• Head office • Department A (eg marketing) • Department B (eg Finance) • Geography X • Geography y	• Strategic • Operational • Compliance • Process • Reputational • Change
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.

Tactical

308 Many organisations struggle to implement their strategy, regardless of how finely developed and well-honed it 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 framework 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 Most 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.

Operational Examples

Different sales departments could have a different focus depending on how their specific unit relates to the defined strategy. Specific sales units might be directed to take increased risk to exploit the market in order to support a new product initiative. Sales units might have defined margin requirements

The IT department might need to focus on cost savings and increased efficiencies to support a strategic product launch.

The legal or policy department might need to focus on controls to reduce the number of errors.

The finance team might be required to manage the debtor balances and to ensure sufficient unencumbered funds in the event of a worst case scenario.

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 a single one word label. Risk-averse companies have little or no future, while risk-reckless organisations can expect a rapid exit from business. This is not to deny that in practice, at the simplest level, the propensity to take **any given risk** can be defined by single word labels. Although this then needs to be weighed against the way in which control is exercised in the relevant area. 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 self-defeating:

- 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.

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 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.

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.

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.

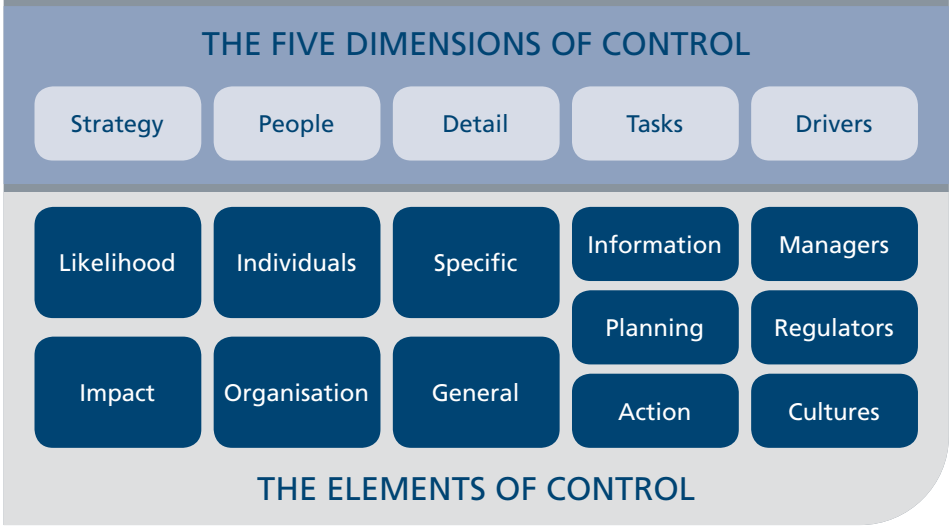
317 In conclusion, the propensity to exercise control is an important counter-weight to the propensity to take risk. Taking risk cannot be considered without also contemplating control mechanisms. There is a range of possible approaches from the simple single-word definitions, through traditional accounting 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.

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?

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. At this stage we are not recommending any individual approach to measurement, although we have included some illustrative ideas.

An example of a valuation model: shareholder value

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.

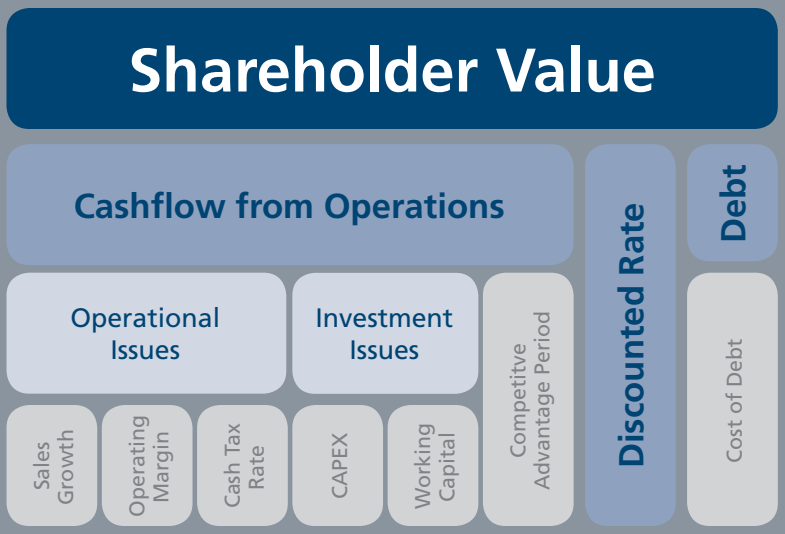


Figure 9 - Shareholder Value Model (1)

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

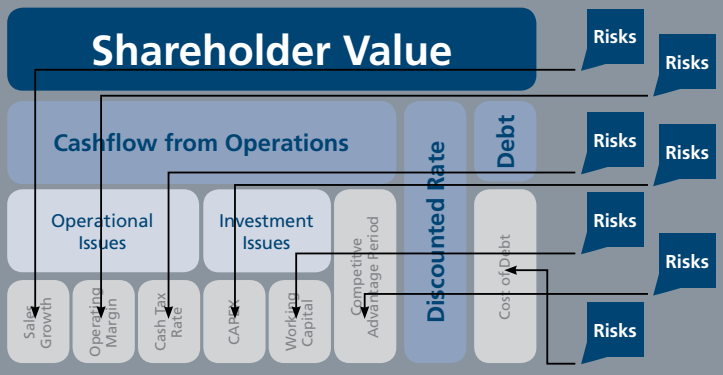


Figure 10 - Shareholder Value Model (2)

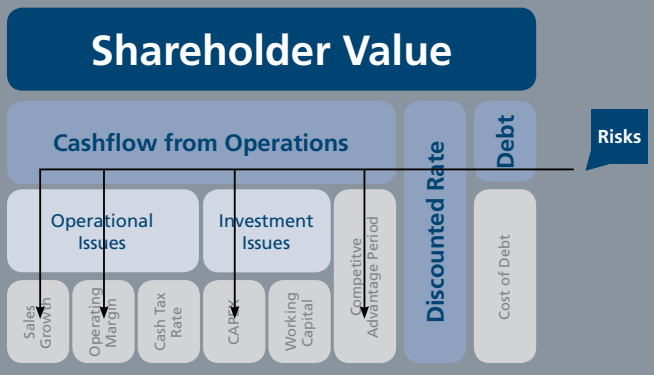


Figure 11 - Shareholder Value Model (3)

We think that testing risks against models such as these will enable organisations to have a much better understanding of which risks are important at a much earlier stage.

Strategic

319 At a strategic level we are suggesting that a variety of high level models might be used including:

- Shareholder value for private sector organisations. See the box above for more information on one possible approach. (Black, Wright and Bachman, 2000)
- Stakeholder value might be a more appropriate measure for not-for-profit organisations
- Economic Value Added ("EVA") has been commonly used in many organisations.

320 The important issue here is not so much the precise model that is selected, but rather that it is appropriate for the nature of the organisation. One of the key attributes of using models such as these is that there is a focus on translating strategy to the underlying value drivers and, of paramount importance, a need to identify key assumptions and therefore key risks.

321 Such models may be more sophisticated than is necessary for less mature organisations and it is clearly not appropriate to implement a shareholder value approach in the context of the public sector or some third sector organisations. We acknowledge that additional work is still required to identify other models that would be equally valid in the public sector but we do not think that this represents a significant shortcoming in the proposed framework.

Tactical and operational

322 We recommend that organisations should develop a series of risk metrics and control metrics to measure tactical and operational risks and controls. The concept of risk and control metrics is widely referred to in risk management literature, normally as KRI's and KCI's, although implementation is at best patchy. There are many practical approaches to identifying key indicators. However, in implementing them, management should ensure that they are readily understood and are drawn from appropriate information systems and reliable data-sources which are subject to proper governance procedures. For organisations that already use KPI's as part of their balanced scorecard management reporting information, both risk and control indicators should be relatively easy to implement.

Data

323 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

324 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, including appropriate governance over the data and information systems employed.

Constructing a risk appetite - questions for the boardroom

- 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?
- 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?
- Does the organisation understand clearly why and how it engages with risks?
- Is the organisation addressing all relevant risks or only those that can be captured in risk management processes?
- Does the organisation have a framework for responding to risks?
- What approach has the organisation taken to measuring and quantifying risks?

IV Implementing a risk appetite

"Execution is everything"

401 In this section of the booklet we are turning to the development of a risk appetite. We set out in Figure 12 below the seven stages of development for a risk appetite in an organisation:

Figure 12 - Stages of Development of Risk Appetite

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

Stage	Main components
Sketch	Enough to engage with stakeholders
Stakeholder engagement	Engage with a full range of stakeholders
Develop	Using the risk appetite framework set out in this paper
Approve	Approval from both the board and the risk oversight committee as appropriate
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
Report	Both internally and externally
Review	What worked well? What failed? What needs to be done differently next time?

Sketch

403 Risk appetite should be evolved from and support the strategic planning and business objectives of the organisation. It needs to become a central component of the business planning cycle. The risk appetite framework helps to articulate the risks to the business that could potentially impact on the achievement of strategic goals (positively or negatively). It will reflect the extent to which the organisation is prepared to tolerate risks described by limits, indicators and process controls.

404 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 capability, both in terms of capacity and maturity.

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

Stakeholder engagement

406 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.

407 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.

A fuller extract from Friedman's own writings illustrates a rather wider perspective to the relevance of wider stakeholders on business than is sometimes attributed to him: "A corporate executive… has direct responsibility to his employers… to conduct the business in accordance with their desires, which generally will be to make as much money as possible while conforming to their basic rules of society, both those embodied in law and those embodied in ethical custom." (Friedman, 1970)

Develop

408 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 from organisation to organisation. Of course, the detail needs to be tailored and proportionate to the organisation.

Approve

409 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

410 Implementation is going to take some time. It is unlikely that an organisation will be able to get the risk appetite framework 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.

411 There is little point in defining an appetite without clearly articulating consequences. Further, it is important the organisation is seen to take action in conjunction with the appetite. For example, some Boards and senior management state they have a zero tolerance risk appetite regarding any compliance or regulatory breaches. All well and good, but the organisation's staff policy handbook must clearly follow the same lines and one would expect that once proved, disciplinary proceedings for the staff responsible would be automatic. For the risk appetite statement to be taken seriously throughout the firm it cannot be defined in isolation to the rest of the organisation.

Report

412 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

413 At the end of each reporting cycle, and before the risk appetite statement is re-sketched, 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.

Implementing a risk appetite - questions for the boardroom

- Has the organisation followed a robust approach to developing a risk appetite?
- 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?
- Is the risk appetite tailored and proportionate to the organisation?
- Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?
- What is the evidence that the organisation has implemented the risk appetite effectively?

V Governing a risk appetite
"Making sure it fits"

501 The final 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 13 below:

502 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 framework 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 framework and demonstration that the framework 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, and
- **Learning**: as discussed in the development section, the board needs to ensure that the organisation learns from the implementation of the risk appetite framework so that it becomes more embedded into the organisation.

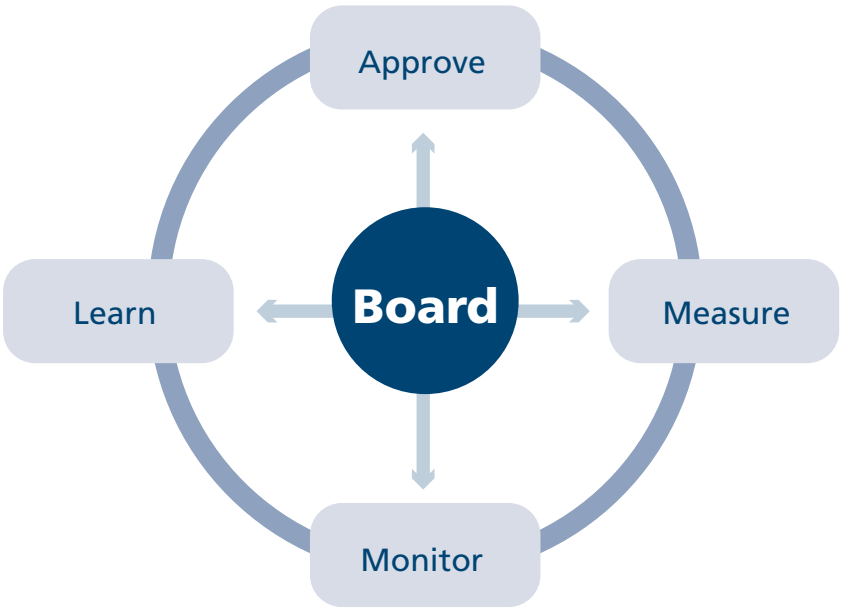


Figure 13 - Governing a Risk Appetite

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

503 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.

504 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 Figure 14.

505 This view of the criticality of data supporting information flows in the organisation also underpins the importance of developing actionable management information. Traditionally the data and information used in most organisations is oriented to accounting and reporting. It is our view that data governance from a risk management perspective is becoming a key issue underpinning the development of relevant and effective risk appetite frameworks. Measurement will only work where the underlying data sets are reliable, accurate, complete and timely with minimal off-line manipulation. Exactly like those used for accounting and reporting systems.

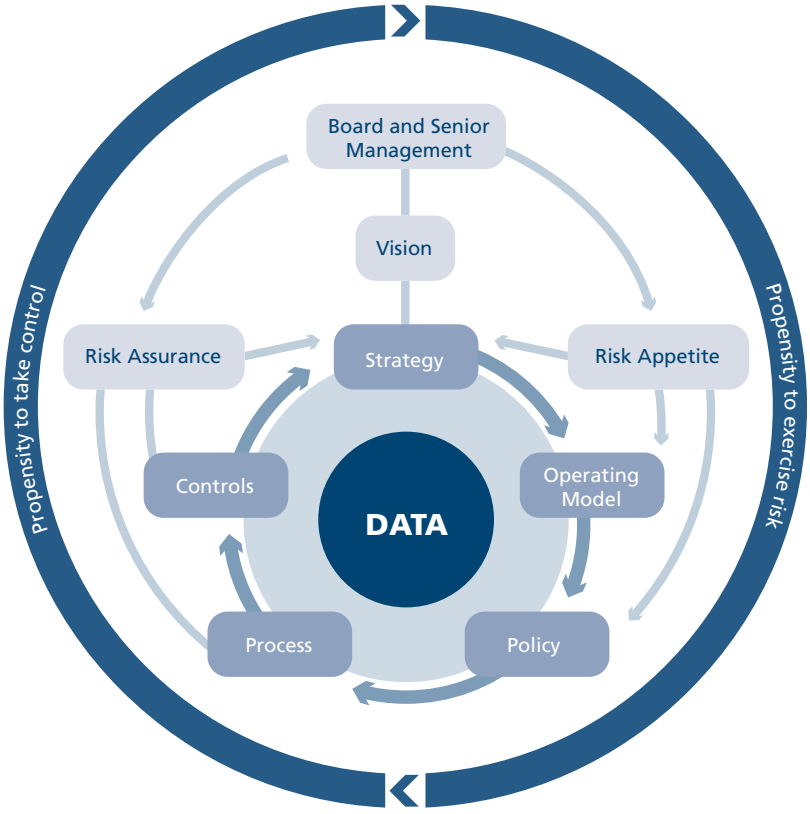


Figure14 - Risk Appetite In the Organisation

506 This is a new area of endeavour for many organisations and their boards. The House of Lords Economic Affairs Committee addressed a recommendation made by Sir David Walker in his review of governance of banks and other financial institutions. It is neither the purpose nor the remit of this paper to comment on this, except to the extent that if a board institutes such a committee, we believe that risk appetite and risk tolerance should be high on their agenda

> "We strongly support the development of separate risk committees in banks and major financial institutions. Other large companies should institute them where appropriate. Such committees will increasingly require specialist skills and external advice. This advice should not be provided by the firm which is the company's auditor."
>
> Source: House of Lords, Economic Affairs Committee. Second Report: "Auditors: Market concentration and their role".

Governing a risk appetite - questions for the boardroom

- Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?
- To what extent did the board identify tensions arising from the implementation of the risk appetite?
- 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?
- Does the board have, or does it need, a risk committee to, inter alia, oversee the development and monitoring of the risk appetite framework?
- Is the board satisfied with the arrangements for data governance pertaining to risk management data and information?

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 could 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, as a cornerstone in a risk management programme, can help in:

- Safeguarding the organisation
- Creating a framework for better decision making
- Identifying issues at an early stage
- Providing a framework for reducing surprises
- Developing a framework 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 frameworks 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.

The journey is not yet over - final questions for the boardroom

- What needs to change for next time round?
- Does the organisation have sufficient and appropriate resources and systems?
- 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.

Baldwin, R. Harnessing the Power of Risk Management. Corporate Risk Group

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.

Financial Reporting Council (2011, March). Guidance on Board Effectiveness

Financial Reporting Council (2011, September). Boards and Risk

Financial Reporting Council (2011, September). Effective Company Stewardship

National Audit Office (June 2011) Managing Risks in Government

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

House of Lords Economic Affairs Committee. (2011). *Second Report - Auditors: Market concentration and their role.*

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.*

Walker, D. (2009). *A review of corporate governance in UK Banks and other Financial Industry Entities.*

Appendix A: 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, risk tolerance and attitude to risk taking. It should do this by reference to a risk appetite framework the establishment of which the board should oversee. The risk appetite framework of the organisation should be established in the context of the capacity of the organisation to manage the risks and its ability to exercise the appropriate management disciplines.
2. The risk appetite framework 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 framework.
3. The risk appetite framework should inform the development of strategy for the organisation. 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 should retain responsibility for strategic risk taking, a committee of the board may have delegated authority for overseeing the production of the risk appetite framework for board approval.
4. Management of the company at all levels is responsible for operating within the constraints established by the risk appetite and risk tolerance framework. Management is responsible for ensuring that employees follow the policy with regard to risk taking and operate within the limits of authority established by the risk appetite framework 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 risk exposure approaches the maximum level that the company is willing to tolerate.
5. Management is responsible for ensuring that appropriate disciplines are in place over risk management data and risk management information. The board (or a committee thereof) should satisfy itself that appropriate data architecture and data governance disciplines are in place.

Process for managing risk taking

6. When establishing the risk appetite framework, there is a need to pay regard to the size, nature and complexity of the company and both the business sector and geographical locations 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:

- The strategic objectives of the organisation, including an understanding of the parameters of success and failure, and the underlying performance (or value) drivers
- Nature and extent of the risks facing the company
- The capability of the organisation to manage the risks it faces, both in terms of capacity (financial, intangible, infrastructure and human aspects) and organisational maturity (skills, knowledge, attitudes of people and the level of sophistication of risk management processes and systems)
- Extent and categories of risk it regards as acceptable for the company to bear
- Likelihood of the risks concerned materialising
- The organisation'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.

7. A risk appetite framework should be seen within the context of the overall management of the business as well as the risk management process. The risk appetite framework will inform more detailed risk assessments, when an organisation 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.

8. In evaluating their risks, an organisation will compare the results of the risk analysis with a set of risk criteria. These criteria will be derived from and form part of the risk appetite framework of the company, so that the risks the board is willing to take can be established. Application of the risk appetite framework should enable the company to develop and sustain:

- Strategic objectives capable of delivering the required outcomes
- Effective processes and the development of an organisational culture to deliver stakeholder expectations, and
- Efficient operations and activities.

9. An organisation 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. It is important that critical controls applied in the management of risks are understood and identified. The risk appetite framework will form the foundation for developing risk based assurance mechanisms, including internal audit.

10. 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 organisation to risk
- Capacity of the organisation to take risk
- Limits of authorisation that are in place for management, and
- The maximum risk exposure that the board is willing to tolerate in relation to any specific risk or category of risk.

11. When developing the processes for developing a risk appetite framework 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 both the business sector and geographical locations within which it operates:

- Risk appetite may be seen as a strategic driver for companies
- 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; and
- 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 under Delegations of Authority.

Appendix B: List of respondents to consultation

We are grateful to the following who took the time to respond to the formal consultation request on the draft document. Some made formal representations; others responded through e-mail correspondence or other more informal channels. In most cases, unless the name of the organisation is in the first column, responses were in a private capacity and do not necessarily reflect the views of the organisation for whom the individuals listed work. Given the very diverse nature of the responses, we have not necessarily been able to reflect everyone's comments, but they have all been reviewed and considered in formulating the final document.

Individual or Organisation Responding	Affiliation
Adrianus Darmawan	Financial Service Risk Management, Ernst & Young, Indonesia
Alarm	The public risk management association
Alpaslan Menevse	Sekerbank, Turkey
Alyson Pepperill	Client Projects Director, Oval Insurance Broking
Andrea Simmons	Simmons Professional Services
Andrew Black	BVA Ltd
Andy Garlick	Private
Annemie Pelletier	Private
Association of Corporate Treasurers	N/A
Brian Martin	FSCS
Brian Roylett	RMIA
Bruce Widdowson	Private
Chris Greaves	Zurich Risk Engineering
Chris Hodge	FRC
Chris MacDonald Bradley	Engineering Council
Chris Pierce	Visiting Professor of Corporate Governance, City University
Claude Patrick	Arcelor Mittal
Craig Percival	Corporate Risk Manager, United Utilities
Dan Clayton	Chan Healthcare Auditors, Missouri, US
Dan Roberts	RAAS Consulting
Darren Tomlins	New Zealand Customs Service
David Clayton	DWP
David Hillson & Ruth Murray Webster	Risk Doctor & Lucidus Consulting
Dennis Cox	Risk Reward Ltd
DNV	N/A
Duncan Stephenson	Head of Group Risk, Yorkshire Building Society

Individual or Organisation Responding	Affiliation
Gillian Lees	Chartered Institute of Management Accountants
Graham Dalzell	Engineering Council
IoSH	N/A
Jackie Cain	Chartered Institute of Internal Auditors
Jake Storey	VP Finance, Gearbulk
Jean Paul Louisot	CARM Institute, France
Jeff Smith	Head of Risk Management & Internal Audit, James Brearley & Sons
Jill Douglas	Head of Risk, Charterhouse Risk Management
Jo Howey	Policy Advisor on Risk Management and Internal Audit, Financial Management and Reporting Group, HM Treasury
John Thirlwell	Private
Keith Smith	Private
Malcolm Kemp	UK Actuarial Profession Enterprise Risk Management Practice Executive Committee
Marina Basova	Finance Manager, Basic Element Company, Moscow
Michael Parkinson	KPMG, Australia
Nicola Crawford	Private
Norman Marks	Honorary Fellow of the IRM, Vice President, Evangelist, SAP
Paul Taylor	Director of Risk Assurance, The Morgan Crucible Company
Pauline Bird	BDO LLP
Pesh Framjee	Crowe Clark Whitehill
Peter Bonisch	Paradigm Risk
Reno Fanucci	Head of Risk, P4
Richard Archer	Wellcome Trust
Richard Baker	Caerus Consulting, on behalf of the UK Policy Governance Association
Robert Chanon	Charterhouse Risk Management
Sally Coates	Senior Auditor & Senior Risk Management Advisor, Gloucester County Council
Seamus Gillen	Institute of Chartered Secretaries and Administrators
Sheila Boyce	Metropolitan Housing Partnership
Stephen Ward	School of Management, University of Southampton
Steven Shackleford	Birmingham City University
Thomas Reardon	Private. Falls Church, Virginia, USA
Tom Maher	Private
Trevor Llanwarne	UK Government Actuary
Trevor Williams	Magique Galileo
UK Actuarial Profession Enterprise Risk Management Practice Committee	
Vaughan Cole	Private
William Wong	Private

Crowe Horwath Global Risk Consulting
Contact: Richard Anderson
E richard.anderson@crowehorwathgrc.net

Charterhouse Risk Management Ltd
Contact: Andy Jenkinson
E andy.jenkinson@charterhouse-group.com

The Institute of Risk Management
6 Lloyd's Avenue
London EC3N 3AX

T +44(0)20 7709 9808
E enquiries@theirm.org
W www.theirm.org

Leading the risk profession