27 July 2018

Risk appetite and internal audit
Chartered Institute of Internal Auditors

This guidance looks at the nature of risk appetite and how it has come to the fore following the financial crisis as a key component of governance and risk management.

We consider definitions and terminology, recent developments around risk appetite including the relationship to wider corporate governance, how to establish a risk appetite and the roles that internal audit can play.

This is an introduction to the subject orientated towards internal auditors and the provision of assurance and consultancy. Accordingly we have highlighted a range of additional material within the text to encourage wider reading and research.

Definitions
Terminology
Stakeholder expectations
Risk appetite and links to corporate governance
Establishing a risk appetite
Risk appetite statements
Risk appetite as a cornerstone to effective risk management
Risk appetite and internal audit
Risk maturity and internal audit consultancy
Risk culture and internal audit assurance
Risk appetite questions

Definitions

At the moment there is no accepted, single definition of risk appetite but the similarity among existing definitions indicates movement towards a consensus.

Risk appetite definitions
The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time (Orange Book, HMT 2004).

Risk appetite is the level of risk that is acceptable to the board or management. This may be set in relation to the organisation as a whole, for different groups of risks or at an individual risk level. (An Approach to Implementing Risk Based Auditing, IIA UK & Ireland 2005).

The amount and type of risk that an organisation is prepared to seek, accept or tolerate (ISO 31000, 2009).

The amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives (Risk Appetite and Tolerance; Guidance Paper, Institute of Risk Management 2011).
Risk appetite is the amount of risk, on a broad level an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so (ERM Understanding and Communicating Risk Appetite, COSO 2012).

It is clear from this short list of definitions that ideas around risk appetite continue to evolve and this means there is a danger that difference in risk terminology will cause some confusion, particularly when the same terms are used to describe different things.

However, a level of agreement is beginning to form based upon definitions contained within the Institute of Risk Management’s Risk Appetite and Risk Tolerance Guidance Paper. This document also helps to clarify some of the key phrases and the relationship between performance, risk appetite and risk tolerance in the following table and diagrams.

### Terminology

**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.

**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 capacity** - The resources, including financial, intangible and human, which an organisation is able to deploy in managing risk.

---

Expand this diagram
In this context risk tolerance has a wider scope than risk appetite as it represents the outer limits beyond which the organisation could not cope in terms of risk capacity or performance (how much the organisation is able to live with if things go wrong).

Whereas risk appetite is the bandwidth the organisation aims to work within to achieve its objectives.

In setting risk appetite and risk tolerance organisations should consider both the gross risk position and the residual risk position to appreciate the reliance on controls and other mitigation but also the cost of these control compared to the consequences of the risk materialising.

Such a discussion would also highlight the focus of assurance by internal audit and other assurance providers.

**Stakeholder expectations**

These definitions show risk appetite has been with us for some time. It has simply come forward as a subject of importance in the debate about effective risk management following the financial crisis.

For instance, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has said one of the major problems that led to the financial crisis was that although objectives had been created there was no articulation of risk appetite or clarity of those who were responsible for various risk areas.

The focus upon risk appetite has therefore led to specific inclusions or changes to corporate governance codes and raised expectations of stakeholders, particularly sector regulators.

For example the Financial Reporting Council (FRC), the UK’s independent regulator responsible for promoting high quality corporate governance, expanded Section C: Accountability of the UK Corporate Governance Code in 2012 to introduce the concept of risk appetite.

Section C2, retained in the September 2014 update of the Governance Code now states 'The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives'. In other words boards must state their risk appetite for principal risks and consider their overall exposure to risk.

In addition to the updated code the FRC has also issued Guidance on Risk Management, Internal Control and Related Financial Business Reporting to bring together elements of best practice for risk management. This includes as Appendix C a set of questions for the board to consider upon risk appetite and risk culture.

The regulators in the financial services sector now insist that organisations define their risk appetite and require that appetite to be understood and owned by the board.

In a letter on governance for retail firms, the UK Financial Services Authority stressed the importance of risk appetite statements and the need for them to be clear and easy to understand and to inform strategic decisions.

They noted that ‘risk appetite statements may need to contain a mixture of qualitative and quantitative elements’ and that ‘If a firm sets granular risk appetites at business unit level, these
should be clearly linked to the firm's overall risk appetite statement."

In the Republic of Ireland the Corporate Governance Code for Credit Institutions and Insurance Undertakings published by the Central Bank of Ireland in 2010 requires financial organisations to have a risk appetite statement (RAS) and recently reviewed a sample.

It concluded in December 2011 statements were not to an acceptable standard and identified the following improvements:

- The Risk Appetite Statement must be approved by the Board.
- It is important to include all material risks in the Risk Appetite Statement. Some companies failed to document the firms risk appetite with respect to material risks such as underwriting and market risk.
- The RAS needs to express risk appetite in quantitative measures as well as qualitative terms. Risk appetite should be measurable and quantifiable. A Risk Appetite Statement written solely in the context of current solvency capital requirements is not acceptable.
- The statement should separately address risk appetite over short, medium and long term horizons (e.g. over the cycle). Most of the statements reviewed did not make any reference to risk appetite over a number of time horizons, as required.
- There must be clear trigger levels for each material risk. As well as material breach limits, statements need to include interim limits which when breached will require remedial action.
- There needs to be a clearly documented and communicated escalation procedure in place. The statement should outline both internal and external escalation procedures as well as identifying what constitutes a material breach.
- The statement must identify who is responsible for monitoring and escalation.
- The statement must be communicated to all relevant staff, including those responsible for producing, monitoring or using the risk measures on a regular basis.

Risk appetite and links to corporate governance

The higher profile assigned to risk appetite is an indication risk management is widely regarded as essential to good governance and sustaining the long-term future of the organisation.

In this context risk appetite at an overall level becomes the framework that joins an organisation's risk management process to its business goals providing managers at all levels with a consistent view of how to respond to risks.

The challenge facing most organisations is to develop a risk management approach and application of risk appetite that is meaningful and embedded in the day to day activity of the organisation.

A dialogue between executive management and the board about risk appetite is important especially as this is an iterative process to arrive at the real risks the organisation is prepared to take.

The discussion should take into account the risk culture of an organisation in terms of the direction and tone at the top but also the risks that managers are really taking to be successful.

Rather than embarking upon designing a risk management process and preparing risk registers organisations should establish expectations about risk management, including a common understanding or attitude towards risk and how much risk people are allowed to take.
Developing clarity about risk appetite is an important way of supporting a robust risk culture, particularly as risk appetite and tolerances will constantly evolve. The diagram below summarises how the iterative cycle needs to operate:

HM Treasury's *Orange Book* (2004) states 'The concept of a risk appetite is the key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed.

The concept may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity.

The *Orange Book* goes on to say that in either case the risk appetite will best be expressed as a series of boundaries, appropriately authorised by management, which give each level of the organisation clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it.

The agreed corporate risk appetite can then be used as a starting point for cascading levels of tolerance down the organisation, agreeing risk appetite in different levels of the organisation.

**Establishing a risk appetite**
It can be difficult to arrive at a consensus given the range of attitudes that may exist towards risk taking.

Defining a risk appetite also assumes there is a clear understanding of what success looks like for the organisation, which may not be immediately apparent or universally recognised and agreed.

As a starting point it may be worth considering the diversity of attitudes towards risk when management considers a major issue such as upgrading a computer system, development of a new product line, acquisition, or joint ventures.

Boards and management of organisations with a lower risk appetite will usually react differently to acquisition, expansion, competition, and market volatility than will peers with a higher risk appetite.

In essence boards and executive managers need to discuss and agree some basic questions - how much risk shall we take and how much risk would be too much risk?

Risk appetite statements

The financial services sector has chosen to tackle this issue through risk appetite statements, an approach that other sectors may find useful.

The most effective risk appetite statements are those that are clear and easy to understand.

For example the statement should clarify the risks the organisation is actively pursuing and avoiding. Here is a list of reference points or objectives to guide discussions and the initial formation of a risk statement.

• Establish direct links to the organisation’s objectives.
• Recognises the organisation has a portfolio of objectives and projects.
• Align people, processes and infrastructure.
• Ensure clarity and precision to enable communication throughout the organisation.
• Set acceptable tolerances and parameters for risk.
• Recognise the need to regularly review and update the statement as risks change.
• Establish monitoring and assurance to ensure application.

However, risk appetite statements need not be developed purely from the top down. It is also important to understand and factor in how different divisions, subsidiaries, departments and units already apply boundaries or limits, which will enable risk appetite statements to be made more explicit based on current practice, and then debated and agreed.

Understanding the localised approach to risk taking is needed to ensure overall alignment and to ensure the organisation has a balanced profile or portfolio of risk.

Risk appetite should therefore be descriptive enough to guide strategic and every day decisions and actions across the organisation.

To achieve this risk appetite statements often start out broad and become more precise establishing risk targets and risk limits as they cascade into departments and operations across the organisation.
According to the Committee of Sponsoring Organizations (COSO) of the Treadway Commission a risk appetite statement should effectively set the tone for risk management. Their document Understanding and Communicating Risk Appetite particularly stresses the importance of effective communication and monitoring.

They conclude that to be effective risk appetite must be specific enough to be monitored by management and suggest three alternative forms of expressing risk appetite depending on complexity:

1. An overall, broad risk statement,
2. A risk appetite for each major class of organisational objective, and/or
3. A risk appetite for each category of risk.

**Risk appetite as a cornerstone to effective risk management**

Whilst risk appetite must be meaningful at a practical operational level, having an overall top down view has various advantages and benefits. A clearly articulated risk appetite will provide:

- A starting point to drive the implementation of risk management
- A focus upon strategic objectives within risk management.
- A common purpose - to manage residual risk within risk appetite.
- An understanding of where risks should be removed or transferred.
- Transparency and consistency of critical decisions.
- A basis for effective monitoring of risks.
- A basis for questioning whether risks are properly identified and managed.
- Foundations for further discussion of risk appetite as strategies and objectives change.

Without a clear expression of risk appetite it is not possible to be clear on the objectives of the risk management process.

Once appetite is defined it is possible to establish those internal controls and other measures necessary to ensure that residual risk (which is the level of risk remaining after the inherent risk has been mitigated by internal controls) falls within the risk appetite.

In this way measures of risk appetite can be used as a metric to measure the success of the risk management process.
Having a clear expression of the appetite makes it easier for board members, managers and employees to share in a common view on acceptable risk. It also demonstrates how each separate part of the organisation contributes to the overall strategy of risk management.

This shared understanding can then be embedded within planning and operational activity, leading to an overall more risk aware, more risk mature culture.

Regulators and potential investors are likely to want to know that risks are being managed. They will have their own appetite for risk and will be able to compare it with that of the organisation where it has been defined and communicated.

In summary strategy, risk management and risk appetite are intertwined. They do not exist in isolation and should therefore be considered together.

**Risk appetite and internal audit**

Risk appetite falls within the remit and scope of internal audit. It forms part of internal audit’s role to 'evaluate the effectiveness and contribute to the improvement of risk management processes' (Standard 2120). This is relevant:
• Where internal audit is required to provide an annual report and opinion to support the board’s overall statement on the organisation’s risk management and control systems.
• If internal audit carries out a wider review of risk management
• In relation to individual audit assignments where the overall aim is to ensure significant risks are identified and assessed with an appropriate risk response that is aligned with the organisation’s risk appetite.

The approach taken by internal audit will depend on the organisation’s risk management maturity including whether risk appetite is fully defined, communicated and understood at all levels of the organisation.

If this is true in your organisation then internal audit’s focus of attention should be upon application and update of risk appetite. This can be done on an audit by audit basis or through an organisation wide review of risk management.

However some organisations are just beginning their risk management journey and for this reason a specific review of risk appetite, either on an assurance or consultancy basis, may be a timely and a useful thing to do.

Taking a view on the risk maturity of the organisation is therefore a good place to start.

**Risk maturity and internal audit consultancy**

The IIA’s approach to implementing risk based internal auditing provides a simple and effective system of classification to help determine the maturity of risk management.

The model, which is as summarised in the chart form below highlights risk appetite as a key factor in maturity indicating that organisations tend to be Risk-defined before risk appetite is expressed with sufficient detail.

**Risk management maturity timeline**
In organisations where risk management is regarded as Risk-naive or Risk-aware internal audit will be more effective providing an annual opinion upon the state of risk maturity and offering advice and consultancy upon the development of a more effective process.

However, it is important that audit retains its role as the third line of defence, so that it does not lose its independence and objectivity.

The key points in our guidance and the list of improvements required to risk appetite statements offered by the Central Bank of Ireland presented earlier provide a list of features and questions that internal auditors can use to help their organisation develop a more effective approach to developing risk appetite. We have brought these together below.

Second, for some operations within organisations it can be difficult to define a meaningful risk appetite resulting in vague general statements that are either very difficult to monitor or impossible to achieve because they imply zero tolerance levels.

This could apply to areas such as incidents of fraud, errors effecting customers, accidents in the workplace etc. and we all know that completely fool proof processes are extremely expensive, if not impractical to achieve.

As independent observers internal audit are in a position to provide a view upon whether there have been realistic attempts to define risk appetites across the business and to highlight areas where more clarity, monitoring and/or research is needed.

Recognising that it is challenging to define some risk appetites is a normal part a developing risk maturity but this should not be an excuse not to try to define and implement something meaningful at point in the journey. Internal audit can highlight where these weak points exist in support of the
Risk culture and internal audit assurance

As discussed earlier the ability to establish, manage and monitor a risk appetite will be influenced by the risk culture within the organisation.

The tone at the top and the commitment to effective risk management from the organisation’s leaders will largely determine the success of the organisation’s approach to implementing risk appetite.

Symptoms of a strong functioning risk culture include:

• Leadership sending consistent and clear messages on acceptable levels of risk.
• Risk and risk appetite discussions as part of key strategic decisions.
• Considering what might go wrong and deciding upon appropriate tolerance levels when considering targets and performance.
• Adequate risk reporting, monitoring and incident reporting based upon clearly defined risk appetite.
• A system of accountability with sanctions for those taking inappropriate levels of risk.
• Appropriate levels of resource to address risks

Even where risk management is quite mature there may well be a difference between the ‘espoused’ risk culture and actual risk taking. Either in terms of taking too much risk outside defined parameters or not taking any risk at all and failing to grasp opportunities.

Likewise the risk appetite understood (or not understood) by different levels of managers and employees will reflect the risk culture and also inform it.

For example the board and senior executives may agree on the defined appetite of the organisation but individuals will vary in their tendencies to be either a risk taker or a risk avoider. This will influence their perceived level of risk as being acceptable or not depending on how it matches with personal risk appetite.

The board and senior executives therefore need independent assurance to understand the true risk culture/appetite of the organisation, comparing what is expected in relation to risk appetite to what is actually happening. This is particularly important in sectors where regulators are taking a close interest in risk appetite statements and censure those organisations who fail to ensure adequate implementation.

Internal audit therefor has an important role in highlighting the specific elements of the real risk culture and the root causes of any variations to provide a meaningful insight to the people leading the organisation.

Reviewing the way risk appetite has been communicated and monitored in the organisation will provide a useful insight into the risk culture in the organisation.

Internal audit’s role in relation to assurance is effectively summarised by Ken Doughty in the following figure provided in volume 5, 2011 of the ISACA Journal, which draws together how the three lines of defence model operates with regard to risk appetite.
There are two aspects to communication that are important. The first is quite simple; risk appetite must be clear and descriptive so that it is easily communicated to managers and employees.

While high level of statements can be quite broad with progressively more detail as they are cascaded down the organisation they all need to be understandable and capable of being monitored.

Second, risk appetite needs constant reinforcement through training, instruction, policy and guidance documents so that it becomes a normal part of daily routines and decision making. The HM Treasury guide Managing your risk appetite: Good practice examples provides some suggestions for communicating risk appetite effectively:

- Make it clear that risk appetite isn’t an optional extra – when it’s properly understood, it can help staff to be more confident about taking a particular risk, and more capable of managing it.
- Try to explain it using practical examples – you need to show how it can be applied on a day to day basis.
- Get buy in from the senior managers – if they understand risk appetite, then they’ll be able to apply it to their particular business area.
• Keep communications with staff short, sweet and simple – use relevant practical examples instead of reams of theory.

The point is that each organisation should determine the best way to communicate risk appetite to operational leaders in a specific enough manner that the organisation can monitor whether risks are being managed within that appetite.

Internal auditors can look at the approaches and the level of detail applied. For example the extent to which risk appetite is expressed and understood in relation to:

• Overall risk appetite using broad statements.
• Risk appetite for each major class of organisational objectives.
• Risk appetite for different categories of risk.

In doing so internal audit should provide assurance upon the knowledge and understanding people have of risk appetite. In other words what it means to individuals and their attitude towards application.

This can be done through one to one interviews, workshops and surveys with the aim of identifying areas where the attitude to risk appetite is different to that set out by the organisation and gaining an appreciation as to why this is so.

Assuming risk appetite is adequately communicated senior management, with board support, need to revisit and reinforce it. Risk appetite cannot be set once and then left alone.

Rather, it should be reviewed in relation to how the organisation operates, especially if the business model and risk tolerance/capacity changes.
Management cannot just assume that responsible individuals will implement risk management within the appropriate risk appetite. Therefore, some organisations will review the application of risk appetite through a series of monitoring activities.

Management should monitor the organisation’s activities for consistency with risk appetite through the specifics identified with risk tolerances. Most organisations have key performance risk metrics that they use to measure performance.

It is therefore possible to integrate risk tolerances into the monitoring process used to evaluate performance.

Internal auditing can provide independent insight on the effectiveness of such processes reviewing their effectiveness but also the extent of their reliability. In addition internal can support management in this monitoring by independently testing whether risks are being contained within risk appetite and risk tolerance levels.

Priority should be given to high inherent risks and high residual risks to determine whether risk responses are actually containing risks to acceptable residual risk levels. Controls and mitigating action should therefore be judged in terms of their ability to maintain risks within tolerance levels.

Controls that fail to do so are either unnecessary because they have little use or are ineffective. This is important as the International Standards (performance Standard 2600) require the head of internal audit to discuss with senior management any “accepted level of residual risks that may be unacceptable to the organisation”.

Furthermore, ‘If the chief audit executive determines that the matter has not been resolved the chief audit executive must communicate the matter to the board’.

**Risk appetite questions**

1. How does the organisation know and have agreement on what success looks like in terms of strategic and operational objectives as a basis for a risk appetite and risk tolerances?

2. What framework or structure exists to assign responsibility for establishing a risk appetite – is one needed?

3. How has the organisation articulated how much risk it is willing to take - its overall attitude to risk leading to some form of Risk Appetite Statement (RAS)?

4. To what extent is the RAS aligned to and consistent with the declared values of the organisation?

5. How does the RAS take into account the consultation and expectations of external stakeholders?

6. How does the RAS reflect the ability to grasp opportunities as well things that may go wrong?

7. To what extent has the board and senior executive reviewed the capabilities of the organisation to manage the totality of risks it faces – its risk capacity?
8. How does the risk appetite process incorporate review and update of risk appetite levels?

9. Does the range of risk appetites cover all material risks and/or categories of risk such as regulatory compliance, major changes, new products/services and projects?

10. Does the RAS address risk appetite over short, medium and long term horizons?

11. Does the RAS express risk appetite in quantitative measures as well as qualitative terms?

12. What is the rational for quantitative measures of risk appetite?

13. Is risk appetite measurable and quantifiable – is unacceptable risk taking made clear?

14. What are the lead indicators of risk that support retrospective measures of risk?

15. What are the arrangements to ensure senior executives get involved in risk appetite and set expectations?

16. How does the organisation know managers understand how much risk they can take and how they will be held accountable?

17. To what extent is risk appetite aligned to the reward mechanism – are people incentivised to work within or outside risk appetite?

18. Has the RAS been approved by the Board (Risk and/or Audit Committee)?

19. How effective is the RAS communication process, including those responsible for producing, monitoring or using the risk measures on a regular basis?

20. To what extent has responsibility been assigned for monitoring and escalation?

21. Should there be an early warning system to alert the board and senior executives that the organisation may breach key tolerance levels?

22. Are breaches adequately identified and reported?

23. How do the board and senior executive compare residual risk to risk appetite levels?

24. To what extent are risk aggregated and compared against the overall risk appetite?

25. Should performance against key risk indicators be included in dashboards and scorecards?

26. Are controls generally orientated towards maintaining risks within defined risk tolerances?

27. Is there evidence of how risk appetite is built into business as usual processes?

28. Is there evidence that the organisation has implemented risk appetite effectively?

29. Is independent assurance provided upon the application of risk appetite and risk tolerance?