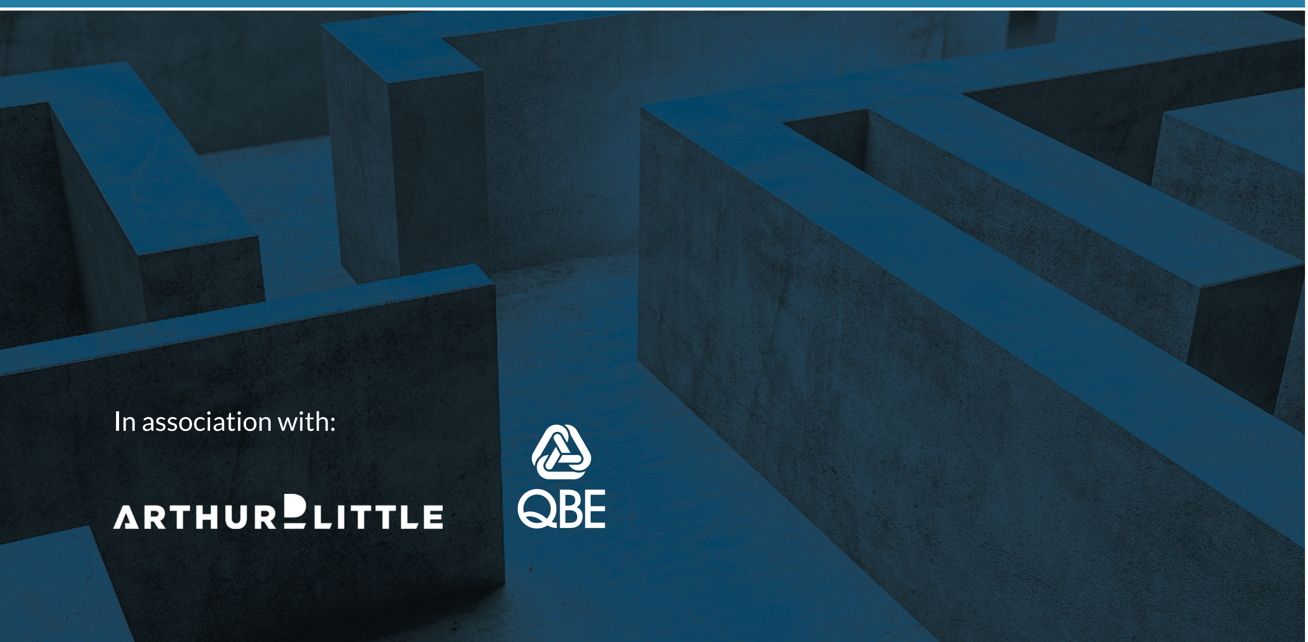
airmic

Risk Appetite **EXPLAINED** Guide

RISK APPETITE EXPLAINED GUIDE



In association with:

ARTHUR D LITTLE

QBE

Acknowledgements

About Arthur D. Little
Arthur D. Little is the first management consulting firm in the world and has always remained focused on innovation. Arthur D. Little's deep industry knowledge, linked to their strong expertise in strategy, innovation, and transformation, helps them solve clients' most complex business issues while delivering sustainable results to their businesses. For over a century Arthur D. Little has been a pioneer in many aspects of risk management - highlighted by numerous landmark assignments leveraging proven capability and the ability to develop deep and meaningful insights.

About QBE European Operations
As a business insurance specialist, QBE European Operations offers a range of insurance products from the standard suite of property, casualty and motor to the specialist financial lines, marine and energy. All are tailored to the individual needs of our small, medium and large client base. We work hard with our broker partners to understand clients' businesses so that we offer insurance solutions that meet their needs – from complex programmes to e-trading solutions – and support them in minimising their risk exposures.

About Airmic
The leading UK association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 1,900 individual members. Individual members are from all sectors and include company secretaries, finance directors, and internal auditors, as well as risk and insurance professionals. Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com

CONTENTS

1. INTRODUCTION

Risk appetite is an inherent part of human decision-making and, in an organisational context, should be considered explicitly when comparing the potential outcomes of decision alternatives. It also plays a key role in the way reasonable assurance over the adequacy of risk management is formed and communicated to the Board – with emphasis on balanced risk-taking within agreed limits.

Risk appetite is a key component of enterprise risk management; it refers to the amount and type of risk that an organisation is willing to pursue or retain. Willingness to bear risk can be defined in two ways:

- An organisation's desire or aversion to pursue opportunities in an uncertain business environment
- How much volatility around an expected outcome is tolerable in terms capacity, regulatory compliance, ethics, reputation and alternative costs for the business.

Defining and implementing risk appetite (increasingly referred to as a *risk attitude*) is a strategic activity that involves the Board and top management, as it must be aligned with strategic objectives and requires consensus and engagement from organisation leadership.

"The Board should determine and continuously assess the nature and extent of the principal risks that the organisation is exposed to and is willing to take to achieve its objectives – its risk appetite – and ensure that planning and decision-making reflects this assessment. Effective risk management should support informed decision-making in line with this risk appetite, ensure confidence in the response to risks and ensure transparency over the principal risks faced and how these are managed."

- The Orange Book: Management of Risk – Principles and Concepts, and Risk Appetite Guidance Note (HM Government)

"The Board has responsibility for an organisation's overall approach to risk management and internal control (including)...determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite')."

- Financial Reporting Council (FRC)

Risk appetite varies between industry sectors, between organisations within those sectors, and by geographies and types of risk. The level of regulation and capital intensity of an organisation will influence its perception of acceptable risk in relation to potential opportunities. Organisations and the context in which they operate are dynamic, and an approach of continuous improvement should be adopted to ensure that lessons learned are taken on board and risk appetite is regularly reviewed, updated and signed off by key stakeholders, including the Board.

This guide sets out an introduction to the concept of risk appetite, with the intention of providing individuals, who may not be risk management specialists, with a high-level overview of:

- What risk appetite is and why it is important
- How risk appetite can be used to support decision-making
- The role of culture in risk management
- The practical challenges of applying the concepts of risk appetite.

The approach described in this guide is aimed at ensuring that an organisation effectively implements a mechanism for understanding how much risk it should take in relation to strategic objective setting, value creation and best value delivery, business model changes and investment decisions.

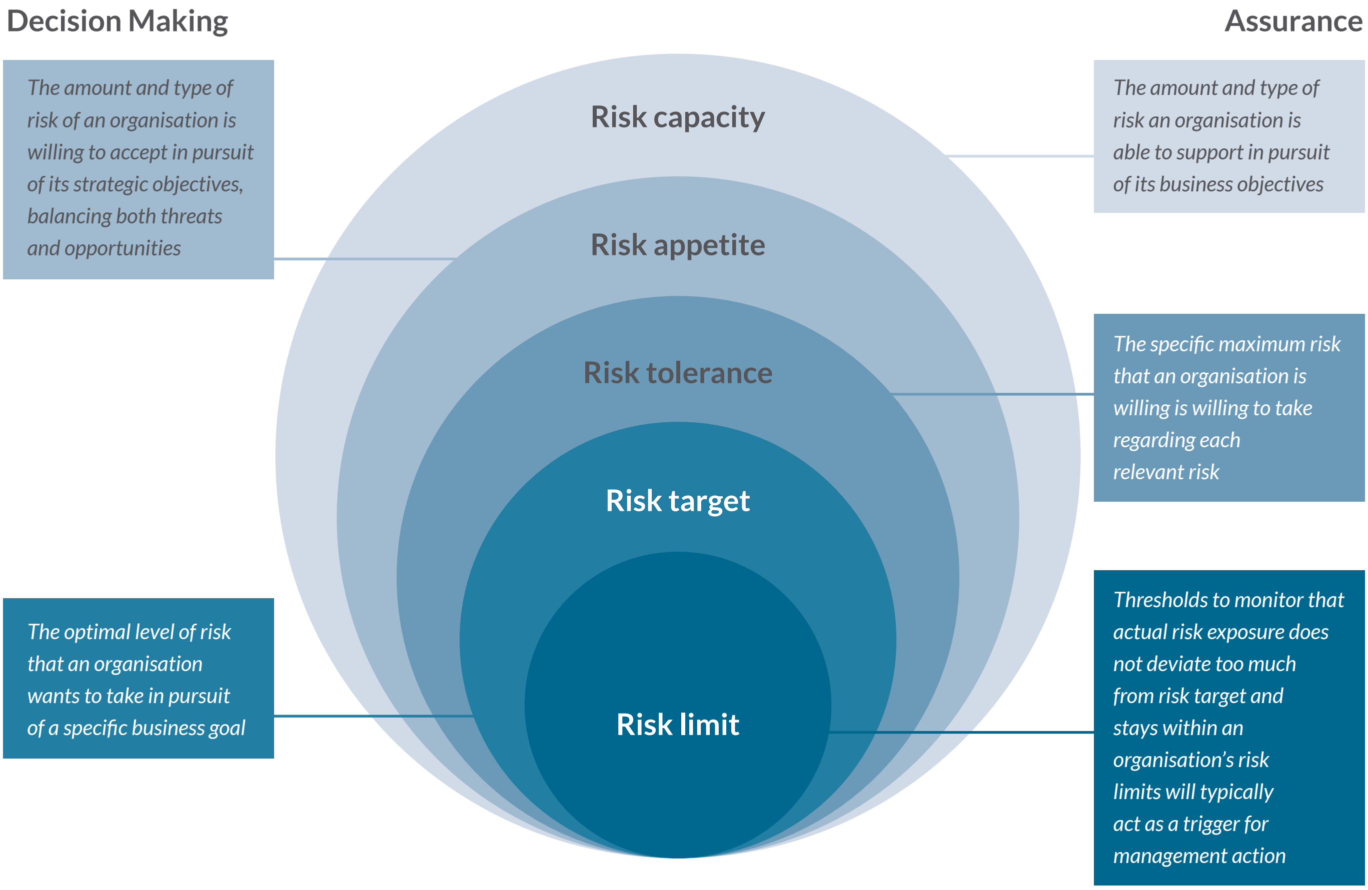
2. THE IMPORTANCE OF RISK APPETITE

An optimal balance must be achieved between risk retention, mitigation and transfer to support long-term growth, or sustainable service delivery, in the current business environment. In essence, an organisation should take risk on a controlled and informed basis in pursuit of its business objectives.

2.1 Why does risk appetite matter?

How much risk an organisation can and may wish to bear will depend on a number of factors, including the environment it operates in, its stakeholders' expectations, the nature and culture of its business, and the capacity it has to cope with absorbing risk without negatively impacting its objectives, otherwise known as its 'risk capacity'. Understanding clearly the differences between the two sides of risk – threat and opportunity – is a key enabler for organisations.

Figure 1: Key concepts associated with risk appetite



An organisation's risk appetite should be:

- **Comprehensive**: It should have the appropriate breadth, reflecting coverage of the risk landscape
- **Measurable**, practical and achievable: Risks should be quantified and compared to risk tolerances. For risks difficult to quantify, qualitative boundaries should be established
- **Consistent and coherent:** Tolerances throughout the organisation need to form a balanced system of relative boundaries, avoiding excessive allowance in some areas and excessive restrictions in others, and should align with the business model of the organisation.

"The Board is fully engaged in risk appetite as this underpins our business model and licences to operate."

- Head of Risk, Major Insurance Organisation

2.2 How is risk appetite used?

Organisations must articulate how much risk they are prepared to bear using a format that can be understood by the organisation as a whole. This format will vary considerably between different business environments, depending on objectives, size, complexities and maturity of the entities in question. There is no one-size-fits-all approach. For example, an organisation operating in a highly regulated environment may have its approach to risk-taking defined through its processes and procedures, and make very little reference to a stand-alone framework document.

The critical factor is how the framework is designed and how guidelines are used to drive improved planning and decision-making. This in turn drives performance and supports the achievement of strategic objectives.

Providing assurance to senior stakeholders that risk is being taken within specified limits is important. Supporting improved decision-making by clearly articulating risk appetite against future risk scenarios is a real driver of reducing future uncertainty and financial volatility. Establishing clear links between strategies, performance indicators and risk limits will facilitate this reduction in uncertainty.

2.3 How does risk appetite support decision-making?

Whilst risk appetite statements have already become a standard part of risk management frameworks across industries, many consider their practical implementation an area that requires further development, especially outside of the financial services industry. To apply the concept of risk appetite effectively, there are six key steps to follow:

- Identify business objectives and review overall strategy
- Understand baseline risk management maturity
- Define risk appetite, considering current risk management maturity and organisational culture
- Integrate risk appetite into decision-making through performance targets
- Specify monitoring, reporting and review processes
- Implement continuous improvement processes, including regular review of risk appetite, cultural maturity and changes in strategy. A summary of one continuous improvement process is given in Figure 2.

The risk appetite statement should consider culture, strategy and objectives, and risk capacity in setting the type and amount of risk that the organisation is willing to accept (see Figure 3).

Figure 2: Example of continuous improvement process for risk appetite setting

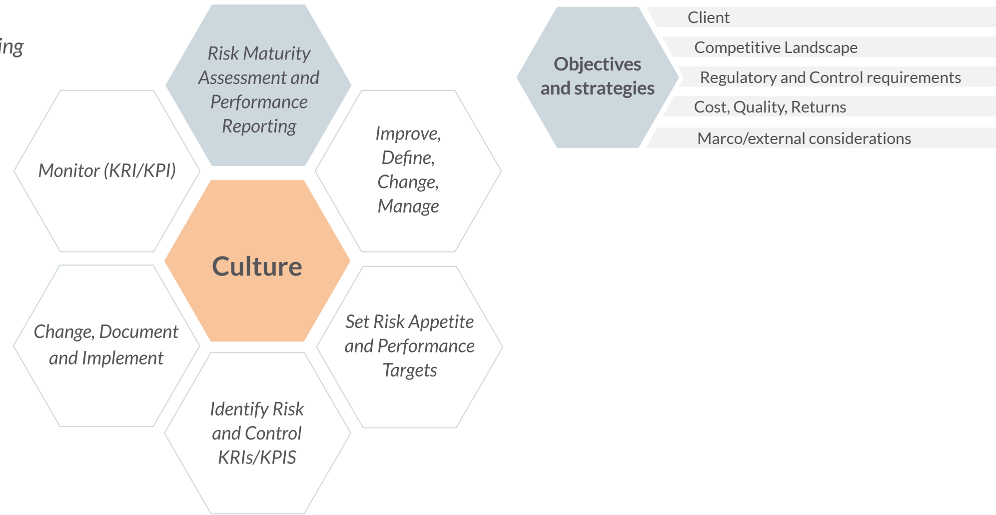
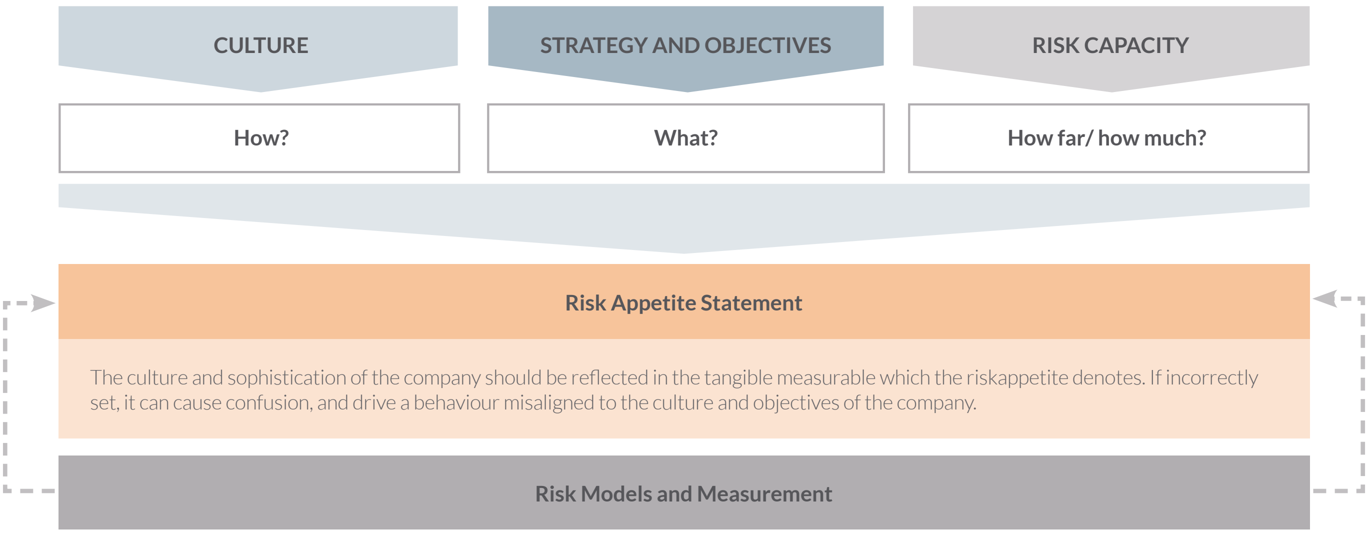


Figure 3: An approach to setting a risk appetite statement



2.3.1 Strategic drivers

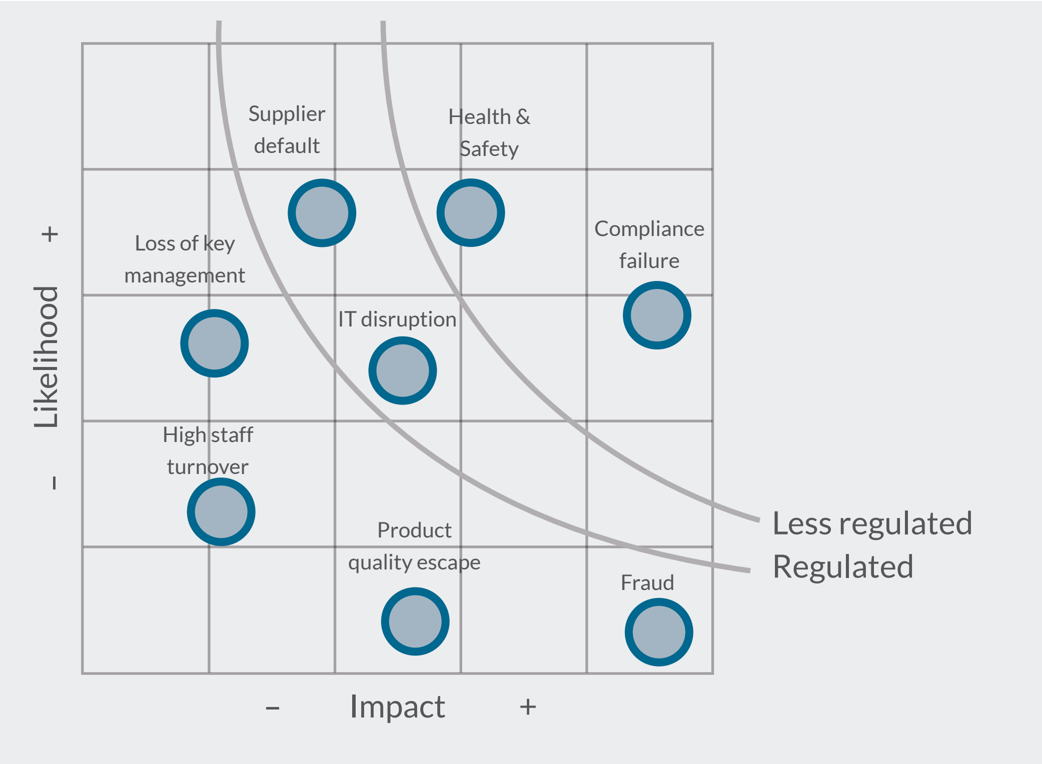
For risk appetite to be meaningful, it needs to be based on clear business drivers. These drivers can be both external and internal, as well as mandatory and voluntary in nature. Examples include:

- Economic cycles
- Competitor actions
- Capital availability
- Terms and conditions of borrowed capital
- Diversification opportunities
- Insurance market conditions
- Active investors
- Safety regulation and other compliance requirements
- Regulation such as Basel II and Solvency II
- Corporate Governance Codes
- Organisation's own return on investment (ROI) targets and minimum capital requirements
- Stakeholder and societal demands.

Alignment of these business drivers, an organisation's current level of risk management maturity, and the types and materiality of relevant risks with the final risk appetite statement is critical for success – what is appropriate for organisations will vary significantly.

As shown in Figure 4, the boundary between acceptable and unacceptable risks will vary by industry. Heavily regulated industries and public sector organisations are generally likely to be more risk averse due to stringent oversight and potential reputational damage. This will influence culture throughout these organisations and must be considered when setting the risk appetite.

Figure 4: The impact of industry and associated regulations on risk-taking



2.3.2 Defining risk appetite

Having formed an understanding of the key business drivers as requirements for risk-taking and risk avoidance, an organisation should be well placed to articulate its risk appetite. Ideally, this would happen through a collaborative process between senior decision-makers, including the Board, as well as those responsible for risk management acting as facilitators.

To engage the Board, some companies have found workshop-based approaches useful, alongside training sessions on the causes and effects underlying principal risks, and how they relate to the business model.

Note: There is no one-size-fits-all formula for risk appetite statements, and it would be dangerous to even propose one, but there are good practices that can be applied in most business contexts, such as:

Defining:

- Scope and objectives of the risk appetite statement
- Principles of governance – which roles and bodies are involved and how their inputs are utilised (ideally, formally approved by the Board)
- Review intervals
- **Clearly linking** the risk appetite statement to objectives, strategies and KPIs
- **Explicitly stating** how its content should be used when making business decisions
- **Use of language** appropriate to the organisation (not introducing too many technical terms or acronyms
- Ensuring the use of **key terminology is consistent** between the risk appetite statement and other policies and risk management guidance
- **Use of case studies** to avoid the perception that the statement is a 'theoretical' document.

Qualitative statements may include the following:

We have a low appetite for risk

We have a high appetite for development in merging markets

We have no appetite for fraud or financial crime risk

We have zero tolerant for regulatory breaches

We will seek to introduce new innovative products in growth markets

We committed to protecting environment

We wish to avoid negative press coverage

Such statements demonstrate an organisation's attitude or philosophy towards upside and downside risks, which may be difficult to quantify numerically, at least initially. Quantitative statements might include the following:

We will maintain a credit rating of AA

We will maintain service supply during core demand hours

We will maintain our market share of 40% irrespective of profit margin

We will maintain a dividend cover of 4x earnings

We will maintain spend in community and leisure services as 10% of our budget

We will reduce energy consumption per unit produced by 50% in 10 years

We will maintain customer satisfaction levels at 95% or above

Note: These types of high-level statements should be cascaded into specific risk tolerances and risk limits – it is important to note that organisations can have multiple risk appetites and it may not be possible to balance all risks optimally at all times. Organisations should be aware of connected risk – the systematic exposure of organisations and their stakeholders to cumulative cascading financial, operational and reputational vulnerabilities.

"Within local authorities, the risk appetite within each service area will vary greatly. What is an acceptable level of risk within waste services may look very different to that of children's services. We encourage local authorities to not be dismayed by the complexity as there is so much value to be gained in having the conversation, raising the issues and shaping their views around risk appetite and tolerance within the organisation."

- Risk Control Director, Risk Management Partners

"Risk appetite and related tolerances need to be calibrated at different levels of the business, as well as across different corporate functions."

- Head of Risk, Major Utilities Company

"Having a low to minimal tolerance of risk can thwart innovation, whereas the opposite approach can leave organisations open to unhealable damage. BCI research has shown that the pandemic has resulted in organisations not only taking a more critical view of their risk appetite, but also ensuring clear flows of information are created and more collaborative working policies are fostered. This means risks are openly discussed with input from all necessary stakeholders and a universally agreed appetite for risk in each area. Indeed, good practice in organisational resilience helps to ensure a universally agreed appetite for risk can be achieved."

- Head of Thought Leadership, The BCI

2.3.3 Role of risk appetite in setting objectives and strategies

Risk appetite should ideally cover the desired organisational behaviours around risk-taking in terms of both threats ('downside risk') and opportunities ('upside risk'). Whilst in the absence of threats the upside appetite would be unlimited, it is the ability to balance the two that separates the most successful organisations from the rest.

Accepting a certain level of risk is a precondition for staying in business, and this minimum level of risk-taking varies between industries and market conditions. Being able to improve an organisation's competitive position in a rapidly changing business environment requires insights into risks and the organisation's ability to manage them at a differentiating level and in varying conditions.

An organisation's appetite for growth and profitability is reflected in its objectives (grow x% over y years, decrease debt by x% over y years) and in the strategies it decides to pursue.

Whilst objectives influence the overall view on risk vs reward, each strategic alternative will come with a different risk profile and hence will influence the way an organisation can cope with unknown future scenarios (alternative futures) as it seeks to fulfil its vision.

“All businesses need a degree of risk to achieve the greater returns expected from equities compared to the virtually risk-free investments such as bonds. We have accepted greater risk in the more strategic areas with a lower to near zero tolerance for compliance issues.”

- Head of Risk, FTSE 250 Aerospace and Defence Organisation

2.3.4 Integration with decision-making

Many businesses are starting to integrate risk into elements of key decisions, often referred to as ‘risk-based decision-making’. The application of this can vary from qualitative awareness of risk themes associated with a ‘go or no go’ decision to a highly systematic decision analysis approach that forces, initially, the establishment of clear decision alternatives and, secondly, the evaluation of these against various alternative futures, driving ranges in their expected net present value (NPV), payback periods and internal rate of return (IRR).

Key to this process is incorporating risk appetite consideration into the evaluation criteria to compare individual decision alternatives. In this way, risk appetite becomes an integral part of how an organisation and the key stakeholders consider the ‘preferences’ of alternative ways forward.

To ensure appropriate accountability and assurance, the Board should require management to present it with acceptable worst-case scenarios for each of the decision alternatives in question and demonstrate a robust analysis of their financial, reputational, legal and organisational consequences to allow the Board to be well informed of the potential outcomes of the decision. The alternative costs associated with the decision should also be explicitly covered.

For the risk appetite consideration not to become a roadblock for agile decision-making, or even a source of bias in itself, simple-point estimations of worst cases should be avoided. A more balanced view on uncertainty around objectives and business cases should be sought by looking at a full range of uncertainty or at least by establishing plausible three-point estimates (e.g. base/expected case, pessimistic case, optimistic case).

In order to support efficient decision-making, limits and escalation protocols that relate to the risk appetite need to be determined across the organisation and the various relevant risk categories.

“The group looks at the competitive position and growth profile of each of its businesses when considering where to allocate capital. We are prepared to take risks in areas of core competence, but will seek to minimise risk outside of those areas.”

- Head of Risk, Major Education Organisation

“Where decisions are required that are potentially outside of our risk appetite, this becomes a topic for Board discussion and approval.”

- Head of Risk, FTSE 250 Aerospace and Defence Organisation

3. PRACTICAL STEPS TO DESIGNING AND IMPLEMENTING RISK APPETITE

Implementing risk appetite within an organisation is a task that extends far beyond simply understanding its conceptual framework. While the concept of risk appetite is familiar to most organisations – outlining the levels and types of risk an entity is willing to pursue or tolerate to achieve its objectives – its practical application across a complex organisation presents significant challenges. These challenges arise from the need to integrate risk appetite into the fabric of the organisation's decision-making processes, align it with diverse operational realities and ensure it is responsive to an ever-changing risk landscape.

The process of designing and embedding risk appetite requires a structured and iterative approach that engages key stakeholders across the organisation and remains closely aligned with the broader enterprise risk management (ERM) ecosystem. It is not just about setting thresholds and limits; it is about ensuring that these thresholds are understood, respected and utilised at every level of the organisation. This requires a concerted effort to communicate the organisation's risk appetite, provide the necessary training, and establish robust monitoring and reporting mechanisms. The steps outlined in the visual below provide a practical guide to achieving this, illustrating how risk appetite can be effectively implemented to support organisational resilience and strategic success.

Figure 5: The process of designing and implementing risk appetite (Source: Arthur D. Little)

Step	Description	Stakeholders	ERM Touch point
1 Establish Governance and leadership Commitment	The first involves securing commitment from the organisation leadership and establishing a governance frame to guide appetite process. This includes roles, responsibilities, and oversight structures.	- Board of Directors - Executive Leadership - CRO	• Align risk appetite with strategic goals and ERM priorities
2 Identify and Define Risk Categories	Identify the types of risk the organisation faces across different categories, such as strategic, operational, financial, compliance, and reputational risks. Define what each category means in the context of the organisation operations.	- Executive Leadership - Business Unit Leader - Risk Management Team	• Review existing risk categories from the ERM framework
3 Set Risk Appetite Statement	Develop clear and concise risk appetite statements for each risk category. These statements should articulate the level and type of risk the organisation is willing to accept to achieve its objectives	- Executive Leadership - CRO - Risk Management Team	• Ensure consistency with strategic direction and organisational culture
4 Quantify Risk Tolerances	Quantify the organisation risk tolerances, where possible, by setting specific thresholds and limits that align with the risk appetite statements. These may include financial metrics, KPIs, or qualitative boundaries.	- CFO and CRO - Business Unite Leaders - Risk Management Team	• Align with ERM-tracked KPIs and performance metrics
5 Integrate Risk Appetite into Decision-Making Processes	Embed the risk appetite into organisation's decision-making processes, ensuring that strategic decision, business planning, and day-to-day operations are informed by the risk appetite framework.	- HR and Training Teams - Communication Team - All Employees	• Regularly review decision against risk appetite tolerances
6 Communicate and Train	Develop a communication plan to ensure that all employees and stakeholders understand the organisation's risk appetite and how it applies to their roles. Conduct training sessions to reinforce this understanding.	- HR and Training Teams - Communication Team - All Employees	• Integrate risk appetite into broader ERM training material
7 Monitor and Report	Establish mechanisms to monitor the organisation's adherence to its risk appetite, using metrics and reporting structures to track performance. Regularly report findings to the board and adjust the risk appetite as needed.	- CRO - Risk Management Team - Internal Audit	• Automate monitoring against risk appetite across broader ERM
8 Review and Revise	Periodically review and revise the risk appetite framework to ensure it remains relevant in the face of changing internal and external conditions. This should be an iterative process informed by feedback and lessons learned.	- Executive Leadership - Business Unit Leaders - Risk Management Team	• Conduct frequent review and challenge the existing risk appetite

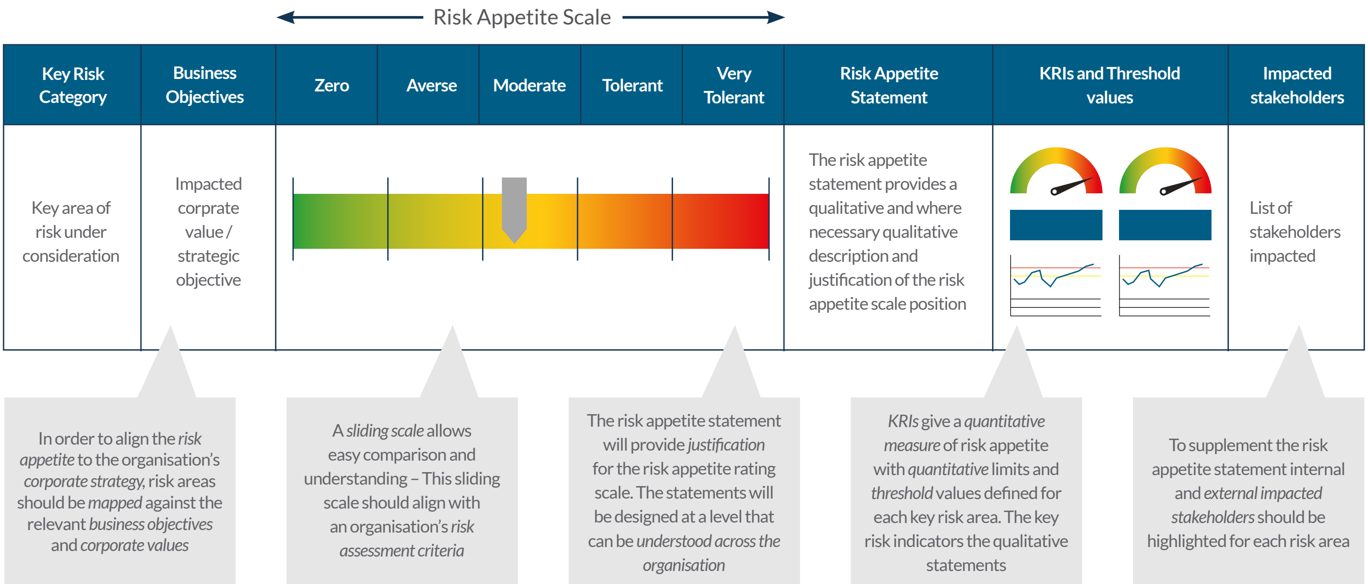
In practice, the successful implementation of risk appetite is an evolution rather than a revolution. It necessitates regular review and adjustment to reflect changes in the internal and external environments. Moreover, the risk appetite framework must be sufficiently flexible to adapt to evolving risks and opportunities while maintaining alignment with the organisation's strategic objectives. By embedding risk appetite into the decision-making processes and ensuring continuous engagement with the ERM framework, organisations can not only safeguard against potential threats but also capitalise on opportunities in a controlled and informed manner.

3.1 High-level design of risk appetite

While risk appetite statements typically share common elements such as risk categories, tolerance levels and key performance indicators, there is no universal structure that applies to all organisations. The uniqueness of each organisation's strategic objectives, risk landscape and corporate culture necessitates a customised approach to developing risk appetite statements. This customisation ensures that the risk appetite is aligned with the organisation's goals, values and operational realities, thereby providing meaningful guidance for decision-making.

Organisations must consider their specific context when defining and articulating their risk appetite. For instance, a risk appetite statement for a financial institution might emphasise risk tolerance in credit and market risk, while a manufacturing company may focus more on operational and supply chain risks. Furthermore, the language and presentation of the risk appetite statement should resonate with the organisation's culture, ensuring that it is easily understood and consistently applied across all levels of the organisation. This tailored approach not only enhances the relevance and effectiveness of the risk appetite statement but also facilitates its integration into the broader enterprise risk management (ERM) framework. The following graphic outlines a high-level structure of a risk appetite statement:

Figure 6: High-level structure of a risk appetite statement (Source: Arthur D. Little)



An overview of the core components is outlined below:

- **Key Risk Category:** Identifies relevant primary risk areas (e.g. financial, operational) that require ongoing monitoring and management, normally derived from the organisation's ERM framework
- **Business Objectives:** Connects identified risks to specific corporate values or strategic objectives, ensuring that risk management supports broader organisational goals
- **Risk Appetite Scale:** A sliding scale (e.g. from zero to very tolerant) that visually represents the organisation's willingness to accept risk; it is important this is aligned with ERM risk assessment and prioritisation criteria
- **Risk Appetite Statement:** A qualitative and, where necessary, quantitative justification for the position on the risk appetite scale, informed by the organisation's risk capacity and tolerance
- **Key Risk Indicators (KRIs) and Threshold Values:** Quantitative measures and limits that provide a clear indication of acceptable risk levels, closely linked with ERM-tracked metrics
- **Impacted Stakeholders:** Identifies internal and external stakeholders affected by the risk appetite, ensuring effective communication and understanding across relevant groups as well as potential severity due to types and number of stakeholders involved.

Ultimately, the structure of a risk appetite statement should be one that resonates with individuals at all organisational levels, supporting enhanced, risk-based decision-making. It is essential that the chosen structure is not only aligned with the organisation's strategic objectives but also with its culture and operational nuances. By ensuring that the risk appetite framework is accessible and meaningful to all stakeholders, organisations can embed a risk-aware culture that drives both resilience and strategic success.

Case study – A South American Oil and Gas Company

A South American national oil company, undergoing a significant shift in corporate strategy and expanding into non-core business areas such as offshore operations, sought to develop a comprehensive risk appetite statement. The primary goal was to provide the Board and stakeholders with a clear understanding of the organisation's risk categories and establish a coherent framework to assess their tolerance for risk across these categories. This project was particularly crucial as the organisation was also in the process of enhancing its broader enterprise risk management (ERM) landscape, making the alignment on risk appetite an essential step in ensuring strategic coherence.

To address these needs, a thorough review of the organisation's risk profile was conducted, followed by extensive interviews with subject matter experts. This process identified eight key risk categories, around which the risk appetite statement was structured. Alongside the risk appetite statement, Key Risk Indicators (KRIs) were developed, complete with associated tolerances, limits and targets. This framework provided the Board with a robust mechanism to evaluate the organisation's financial exposure to each key risk, ensuring that decisions could be made with a clear understanding of the risk-reward balance aligned with the organisation's strategic objectives.

"The development of our risk appetite framework has been instrumental in aligning our Board's views on risk, especially during a time of significant strategic change. It has provided us with a clear, structured approach to assess and manage our risk exposure across new and existing operations." – Head of Risk, South American National Oil Company".

3.2 Cascade of risk appetite across complex organisations

When it comes to cascading risk appetite across complex organisations, two approaches could be applied, each with its own merits depending on the size, structure and risk profile of the organisation.

Single Corporate-Level Risk Appetite

The first approach is the establishment of a single, overarching risk appetite at the corporate level that applies uniformly across the entire organisation. This method is typically favoured by smaller or less complex organisations where the business units operate under a unified strategy and share common objectives and risks. A single risk appetite statement ensures consistency in how risk is perceived and managed across the organisation. It simplifies communication and monitoring, providing a clear, centralised view of the organisation's risk tolerance that can be easily understood by all stakeholders.

Multi-Level Risk Appetite Statements

However, as organisations grow in size and complexity, the limitations of a single corporate-level risk appetite become apparent. In larger organisations, business units often have diverse operational realities, strategic priorities and risk landscapes. To address these differences, there is a growing shift towards a multi-level risk appetite framework. In this approach, an overarching risk appetite is still established at the corporate level, providing a unified vision and setting general boundaries for risk tolerance. However, this is complemented by individual risk appetite statements at the business unit level. These unit-specific statements are designed to reflect the unique priorities, risks and operational nuances of each business unit.

Case study – A UK Construction Organisation

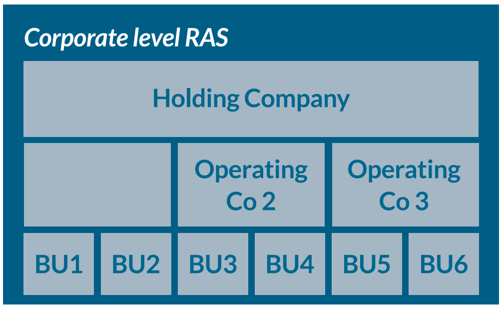
A leading UK construction business faced the challenge of aligning its risk management practices with the overarching group risk appetite. The organisation's diverse business units, including civil engineering, buildings, mechanical and electrical (M&E), ground engineering and home building, each had unique business models and markets. This diversity required a tailored risk appetite framework that could reflect the distinct strategic priorities of each unit while aligning with the group's overall risk management strategy. To address this, a bespoke risk appetite statement was developed at the organisational level, with specific entries for each business unit. This approach enabled the organisation to manage risks more effectively at the local level while ensuring that critical risk information was escalated to senior management in a timely and coherent manner.

The implementation of business unit-specific risk appetite statements led to significant improvements in how the organisation monitored and reported risks. The tailored approach provided better visibility across the organisation's operations, ensuring that relevant and high-quality risk data was communicated to the group level. This not only enhanced the decision-making process for senior managers and the executive committee but also fostered stronger engagement and accountability within each business unit.

> *"The tailored risk appetite framework has significantly improved our ability to manage and escalate risks across our diverse business units, ensuring that key issues are addressed promptly and effectively at the group level." – Managing Director, Major Construction Company".*

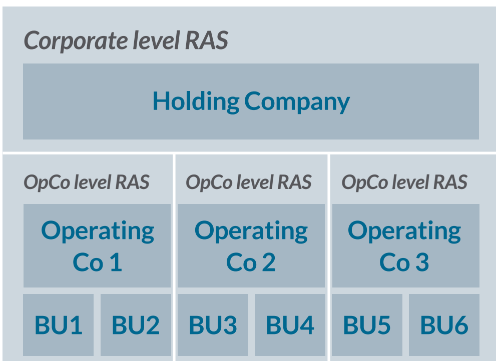
Holding level RAS Approach

- Traditionally, organisations have a single risk appetite statement that has intended to holistically cover an organisation and all its ***business units (BUs)***
- In times of heightened volatility and as organisation becomes more **complex,** one-size-fits-all ***RAS*** may fail to deliver effective, ***risk-based decision-making power***



Multiple RAS Approach

- As organisation becomes increasingly ***diversified*** and ***complex***, there is a case for organisations to define multiple risk appetite statements to support the decision-making of each ***operating company*** and ***business unit***
- The design and implementation of multiple risk appetite statement is ***complicated***, significant effects needs to be taken to ensure that individual RAS ***align*** with overall corporate strategy and cascade up through the organisation



The multi-level approach allows each business unit to define its own risk appetite in a way that aligns with its specific goals while still adhering to the broader corporate risk appetite. This alignment is crucial as it enables business units to manage their risks more effectively while contributing to the overall risk profile of the organisation. The risk appetites at the business unit level are then aggregated up to the corporate level, providing a more granular and accurate picture of the organisation's risk exposure. This method not only enhances risk management at the local level but also ensures that the corporate-level risk appetite is informed by the realities of individual business units, leading to more informed and strategic decision-making.

For larger, more complex organisations, this shift towards a multi-level risk appetite framework is increasingly becoming the norm. It allows for greater flexibility and adaptability, enabling the organisation to manage risks in a way that is both cohesive at the corporate level and responsive to the specific needs of its various business units.

4. THE ROLE OF CULTURE

An organisation's risk culture sets the tone for how it identifies, values, understands, discusses and monitors the risks that it faces. Risk culture is crucial for integrating risk into day-to-day decision-making across an organisation in order to support the achievement of organisation objectives.

4.1 Why culture matters in risk appetite

Setting risk appetite can be one of the most complicated steps in building a robust risk culture but it is worthwhile if implemented correctly. A risk appetite that speaks powerfully to those it serves cultivates improved knowledge and positive attitudes, thus empowering individuals to effectively manage risk. This ensures that decisions at an individual level are aligned to the wishes of the organisation.

"There are certain common foundational elements that support a sound risk culture within an institution, such as effective risk governance, effective risk appetite frameworks and compensation practices that promote appropriate risk-taking behaviour."

\- Financial Stability Board (FSB)

The relationship between appetite and culture is mutually supportive. A risk appetite sets expectations for consistency of approach, and therefore the foundations for risk culture. Conversely, a strong risk culture will increase the success of a risk appetite in practice because effective leadership, communications and governance systems incentives application of risk frameworks. Risk culture is influenced not only by internal forces, but also the industry (particularly those in heavily regulated sectors) and region it operates in.

"Those businesses with a stronger, more aware risk culture should, by their nature, have better processes to articulate and communicate their appetite for various risks. This awareness should then permeate down the organisation in a better way, so that all levels have an understanding of how to act and, if unsure, at least know to question things."

\- Head of Risk, Major Education Company

"We consider risk culture to simply be the business culture viewed through a risk lens. The third tier of risk appetite, the 'modus operandi' is a way for us to integrate risk appetite and tolerances into the day-to-day working of the business."

\- Head of Risk, Major Insurance Company

4.2 Risk culture elements

The risk culture across an organisation can be assessed both directly and indirectly, allowing areas of improvement to be identified. Airmic's seven drivers of risk culture, represented in Figure 8, provide a framework for assessing risk culture. These cultural factors can significantly influence the institution's attitude and acceptance towards risk. More information can be found in the Airmic guide on The importance of managing corporate culture.

The setting of risk appetite features under Section 4.2.1 on Leadership but each of the subsequent drivers can be considered as additional ways to embed risk appetite into the day-to-day activities and decision-making of the organisation, thus reinforcing the culture around the use of risk appetite.

Figure 8: Seven drivers of risk culture

4.2.1 Leadership

In order to effectively manage risk, there must be clear guidelines established and communicated by senior management and the Board of Directors, representing the 'tone at the top'. It is crucial that required behaviours are openly practised by senior management – leading by example in their own decision-making and choices. Individuals who witness consistent behaviours being demonstrated by their immediate leadership group including middle managers and team leaders are more likely to buy into a risk appetite framework.

Without a clearly defined risk appetite, decision-making will be left to personal judgement, inference and bias. People often accept risk based on their individual perceptions, leading to inconsistency in behaviours, which invariably leads to mistakes.

Additionally, setting the risk appetite can be challenging as each senior individual or Board member will have a unique perspective on which risks are acceptable. Setting risk appetite is a difficult part of the risk culture puzzle, so extensive dialogue is necessary. This is beneficial in itself to tease out risk appetite and tolerances in different areas of the organisation, as well as expectations for escalated decisions, before they are cascaded through the leadership structure.

4.2.2 People, Training and Development

Investing the time in ensuring a collective and clear understanding of risk appetite builds the shared attitudes and behaviours that underpin a robust risk culture. Well-trained staff will more consistently interpret the risk appetite statements and be better equipped to address any gaps that may arise in risk appetite application, and will take decisions and actions that are consistent with the spirit (rather than just the wording) of the risk appetite statement. They will also better identify and escalate unexpected risks that aren't covered by risk appetite statements. Poorly trained staff may attempt to exploit opportunities or accept risks that are not explicitly prohibited or attempt to find ways around boundaries designed to reinforce risk appetite in practice. Group training sessions allow teams to discuss how risk appetite is governed in practice specifically at their level in addition to facilitating a unified understanding of risk appetite.

Learning 'on-the-job', with regular informal feedback, reinforces the consistent application of risk appetite and use of processes such as escalation protocols. Taking time to reflect as part of supervisory situations – What made that a good (or bad) decision? Which elements made it ambiguous and in need of escalation? etc. – will serve to reinforce the culture around risk appetite and support the continuous improvement process linked to it.

4.2.3 Reward and Recognition

Encouraging strong risk culture can be achieved with appropriate reward, recognition and penalty mechanisms. Incentivising risk-aware behaviour has been found to be a significant factor across many sectors and can take many forms.

Incentives can include supporting actions such as voicing concerns about behaviours that are contrary to risk appetite and tolerances or identifying adverse trends in an area of the business through audit and oversight processes. For incentives to work, individuals must understand what is being asked of them, and how it links to objectives behind the requirements.

Incentives don't always have to be financial. Praising the right behaviours and recognising the success stories behind the events, not only rewards the individuals involved but can encourage others across the organisation to share in that success through similar behaviours.

Incentives also don't have to be ad hoc. Building consideration of risk behaviours into regular performance reviews provides another layer to recognise the right behaviours. More organisations are using a balanced scorecard approach for assessing performance, and where a formal risk appetite statement is in place, this can help to shape remuneration with the aim of preventing employees from taking unacceptable risks to achieve performance targets.

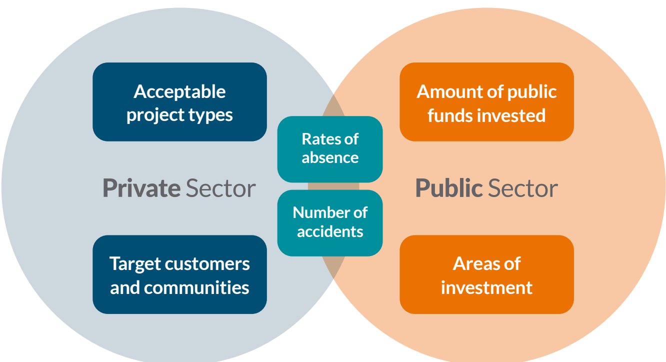
4.2.4 Communication

All individuals should be able to describe how risk appetite relates to their role, their performance objectives and the organisation's strategic aims. If a sufficient level of clarity and understanding is achieved across all functions, senior management can have confidence that the behaviour of employees will be consistent with their expectations and desires for the achievement of the organisation's goals.

> **Note:** In some cases, the phrase 'risk appetite' may not be used at all and communications will be based on describing acceptable and unacceptable risks.

There is no right or wrong way to communicate risk appetite, because organisations will have fundamentally unique objectives, different funding sources and values, and will operate in different sectors and regions, under different regulatory regimes, with different cultural dynamics. An example for private and public sector interests is shown below.

Figure 9: Example of the differences and similarities in appetite focus for public and private sectors



Aside from an all-encompassing framework or separate statements, risk appetite should be communicated through functional documents such as policies and procedures, job roles and performance reviews, control check-lists or programmes, performance targets and indicators. A layered approach that uses established channels that are relevant to role and context reinforces the message that risk appetite is part of normal routines and not an abstract concept involving technical risk jargon. Furthermore, this affords the opportunity to ensure risk appetite isn't considered in silos, which may result in conflict down the line.

The following should be considered when communicating risk appetite expectations:

- A mix of quantitative and qualitative statements including words, numbers, charts, heatmaps, etc. that are appropriate to the function
- Group discussions to avoid individual misinterpretation (similar to the training element in 4.2.2 People, training and development)
- Regular and ongoing communications around governance processes to embed risk appetite long term
- Internal aims aligned with external communications to avoid over promising or mis-selling expectations for projects, delivery, services, etc.
- Setting coherent expectations for acceptability, for example, what's easily green or red, and what falls to 'amber management'.

4.2.5 Performance Evaluation

Risk appetite will not become a meaningful part of an organisation's daily operations unless it is tied to the overall understanding of what risk exposure there is at any one point in time. This calls for the capability to monitor changes to risk, not just once or twice a year, but continually.

> ***"Procedures and processes should be in place to determine the amount of risk that a company is willing to accept in pursuit of its strategic objectives (risk appetite). The risk appetite is set in parallel with the company's strategy and objectives."***
>
> - Financial Reporting Council, Corporate Governance Code Guidance 2024

Strong risk cultures do not conceal bad news, meaning that deviations from agreed risk appetite should be reported through the management chain immediately as part of routine reporting processes. Building a regular review of risk appetite and associated metrics into oversight discussions can help ensure that personnel are taking the right risks to deliver on strategic plans, a risk-averse culture is avoided and the organisation keeps its strategic focus.

A key part of monitoring and reporting is the design and implementation of Key Risk Indicators (KRIs). KRIs form a holistic view of how risk exposure trends across the organisation compare to the organisation's risk tolerance.

KRIs should be used to monitor how closely aligned an organisation's actual risk exposure at any point in time is with its risk appetite. KRIs should help define the risk level, so that when deviations occur outside of the target range or tolerance boundaries, control levels should be investigated and rectified.

Figure 10: Benefits of KRI implementation

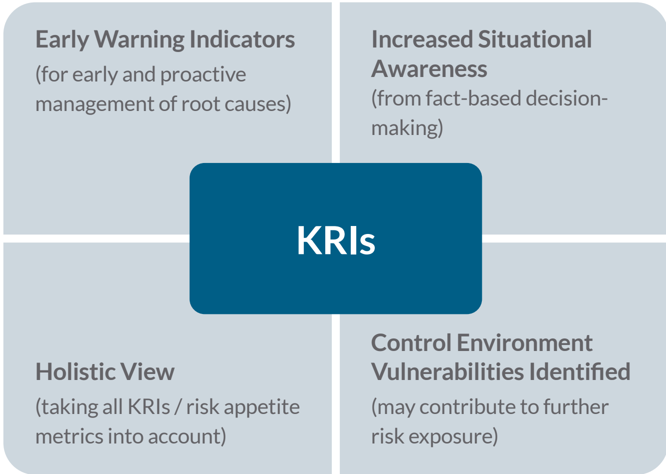


Figure 11: Changes in risk level over time

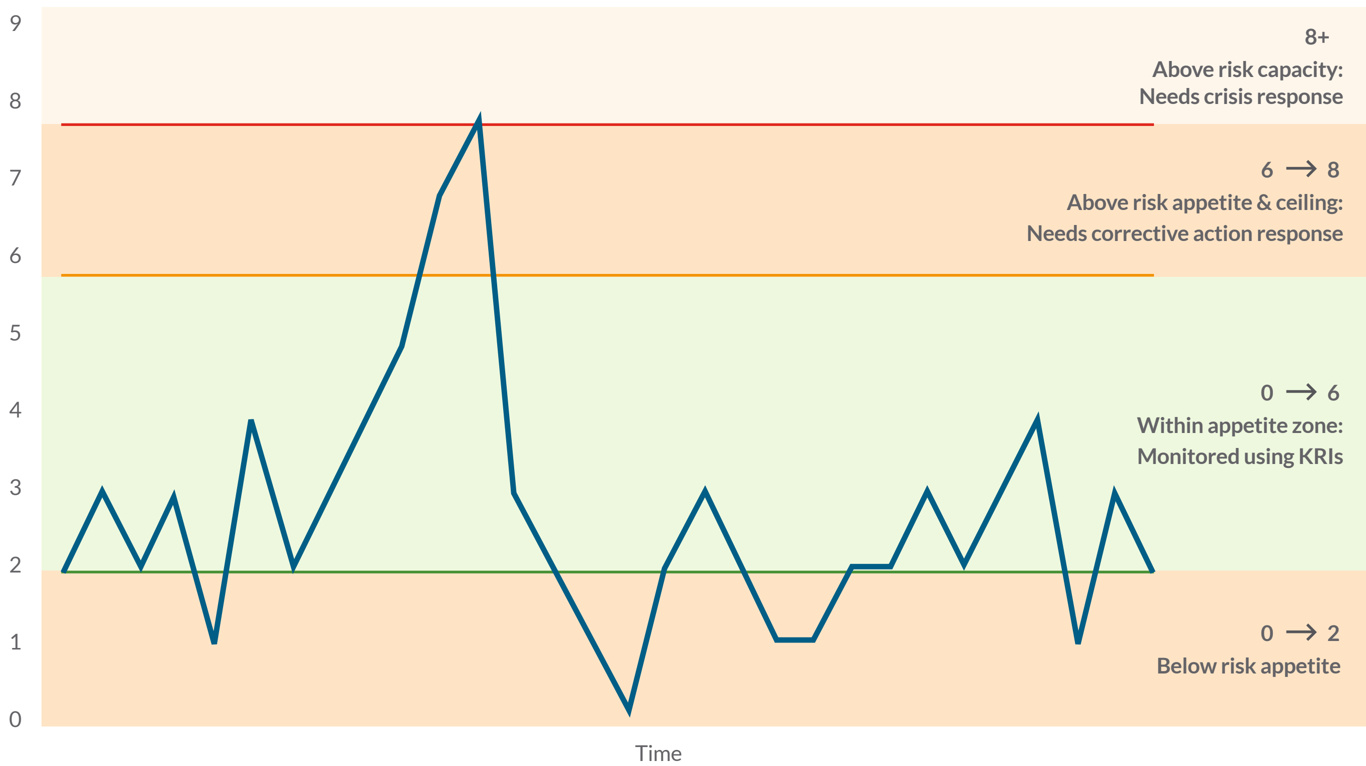


Figure 12: Examples of where consideration of risk appetite can be focused

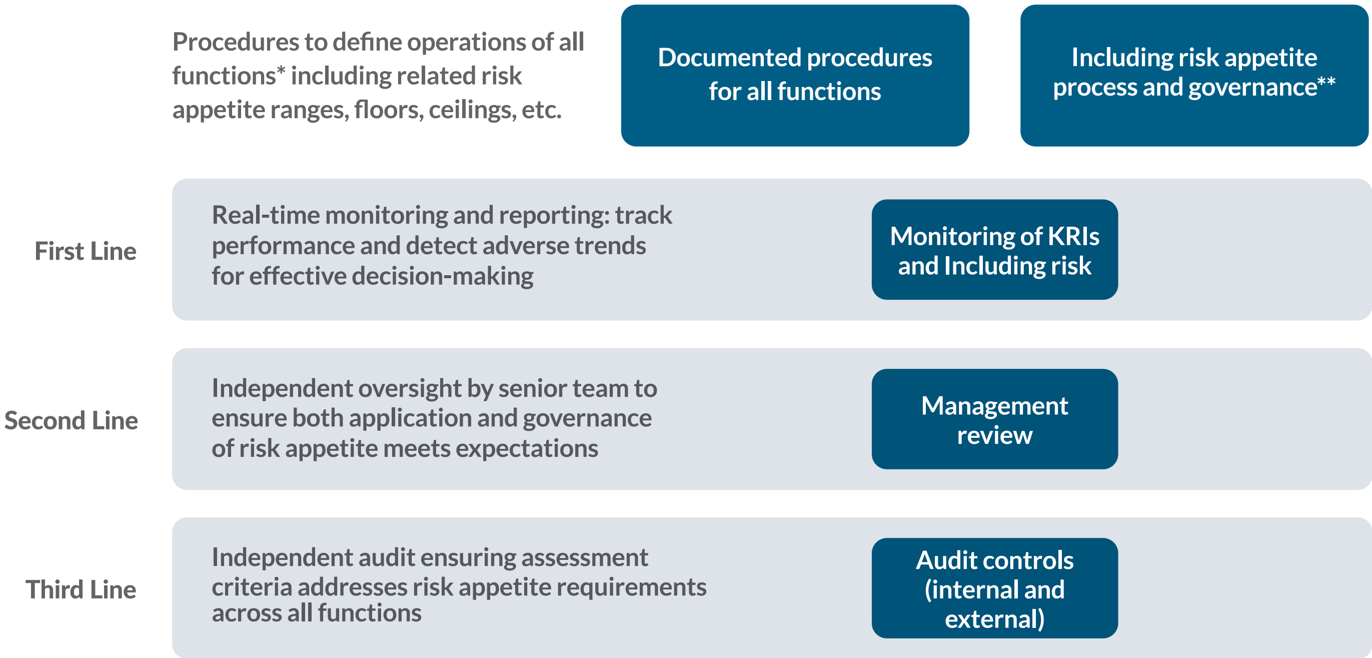
	Strategic	Financial	Operational
When risk appetite considered	• Innovation and development of new products and services • Community groups or markets to pursue, target or avoid • Activities likely to damage brand and reputation • High-profile acquisition, merger or recruitment • High-profile partnerships or investors	• Variations in financial performance, debtor levels, credit scores, etc. • Budgeted investment in specific areas with expected outcomes • Capital levels and expenditure • Variety of sector-specific financial ratios	• Research & Development investment • Health, safety and well-being goals • Quality targets • Customer feedback measures • Business interruption goals • Information and cyber security measures • Compliance breaches • Environmental, social & governance (ESG) targets
Aims	*"We have no appetite to partner with organisations that could tarnish our reputation."*	*"We have a low appetite for debt, want to reduce current borrowings and be clear of debt in 2 years."*	*"We want to maintain positive customer feedback for 90% of all transactions."*
KRIs	*Monitor due diligence information for supplier sign-off, new and ad-hoc payments, contract controls, referral sources, expenses, etc.*	*Overdraft levels, loan repayments, contracts agreed, expenditure and cash flow plans and reports, etc.*	*Levels of feedback sought, responses to structured feedback requests, complaints received and upheld, ad-hoc reviews, etc.*

For further guidance, please see the Appendix – Developing Effective Key Risk Indicators (KRIs)

4.2.6 Service Delivery and Operations Management

A strong risk culture will help integrate risk appetite throughout core processes and prevent it from being viewed as a standalone initiative. Risk appetite may be addressed through operational and governance controls established in assurance layers. Three layers have been defined in the Institute of Internal Auditors' (IIA) Three Lines Model. An adaptation is given in Figure 13.

Figure 13: The Three Lines Model (Adapted)



** Beware there are no 'black holes' or 'glass ceilings' where process controls and risk appetite parameters do not reach. Some functions such as those with sensitive information (finances, personnel) or creative processes (design, marketing) may prove more difficult to define, control and set metrics for, or managers may try to avoid the process controls applied in the core operations and service delivery. This would very likely have damaging knock-on effects including avoidance of monitoring, audit and reporting for management oversight, so it is important to map out all functions in your organisation as one connected management system to ensure nothing has been missed.*

*** Emphasised here to spotlight risk appetite, but in practice, it is likely to be both part of operating procedures and controls defined around the risk management/ERM overview itself.*

4.2.7 Continuous Improvement

Implementing a risk appetite statement is not a one-off activity. To ensure continuous improvement, organisations must view risk appetite frameworks as continually evolving benchmarks rather than static statements. As risk management maturity improves, strategies change and objectives may be revised. Risk appetite statements will need to be updated to align with these new views and remain useful benchmarks for considering opportunities for creating value and managing risk.

Defining and monitoring KPIs and KRIs provides necessary information on which management can base decisions for required changes. To identify gaps and confront challenges in upholding risk appetite, individuals responsible for implementing it in their day-to-day decisions should also contribute to feedback. Equally, management needs to be responsive to feedback, ensuring risk appetite is continually assessed as to whether or not the assumed risk is still aligned and proportionate.

Changes in market dynamics, the wider business environment, the supply chain, regulatory demands, as well as the organisation's long-term vision and strategic priorities can change over time, so it's important that there is an effective radar to detect these and that risk appetites adapt accordingly to stay relevant, as culture and perspective towards risk can shift. The baseline risk appetite framework should continue to serve as a benchmark to establish priorities, make cost-benefit assessments and measure tangible progress year on year.

As with any cultural improvement programme, the ability to share success stories can help breed further success as people see others around them role-modelling the desired behaviours. Recognising and publishing instances where the application of risk appetite principles has helped to achieve strategic goals is a useful way to ensure the cogs of continuous improvement continue to turn.

5. PRACTICAL CHALLENGES OF RISK APPETITE

There are wide-ranging interpretations of both how to understand risk appetite as well as how it should be implemented across organisations. This has led to various myths surrounding the topic, as well as a number of criticisms, especially from outside the financial services industry. These therefore are the key pitfalls to avoid.

5.1 Myths and criticisms

- **Too theoretical –** risk appetite is often referred as being a theoretical concept that exists mainly for assurance purposes.

  Implementation challenges – many organisations struggle to make risk appetite part of everyday management procedures.

  Stifling entrepreneurship – there is a view that defining risk appetite puts limits on entrepreneurialism, creating a 'straitjacket'.
- **Quantification challenges –** some believe that a qualitative approach is too simplistic, whilst others argue that a quantitative approach may be time-consuming and hard to determine accurately, if at all, especially outside of the financial services industry.
- **One-size-fits-all approach –** if the process of setting, implementing and maintaining the risk appetite is not specific to the organisation, the topic is not embraced by all employees and therefore becomes an inefficient and ineffective process.
- **Process is too simplistic or too complex –** if the risk appetite is too simplistic, or too many hoops have to be jumped through to comply, the topic of risk may remain isolated from key decisions.
- **Lack of business context –** risk appetite statements are not aligned to the functions and associated objectives and indicators of the organisational units.
- **Lack of commonly accepted terminology –** it has often been noted that there is confusion created by the terms risk appetite, risk tolerance and risk threshold.
- **Lack of buy-in from internal stakeholders –** if the process is completed in isolation at the top of the organisation, there is a danger that key inputs from all levels of the organisation will be missed, with the risk appetite therefore becoming inappropriate.
- **'Paralysis by analysis'** – if there are too many risk appetite metrics, often they are ignored in the context of decision-making.
- **Too rigid –** if risk appetite is cast in stone and fails to evolve in line with internal and external drivers, it will cease to be relevant and useful, and so will be ignored.
- **Not aligned to cultural incentives –** if renumeration or other incentives conflict with the application of agreed risk appetite, other personal drivers such as bonuses for reaching income targets may be put first.
- **Translation issues –** often, the translation of risk terminology into more meaningful languages causes confusion and misinterpretation. The approach to setting and managing risk appetite proposed in Section 3 on the Importance of Risk Appetite and sections 4.2.4 on Communication and 4.2.2 on People, Training and Development has attempted to address these issues, enabling risk managers and decision-makers to overcome related challenges with mature methods.

"Far too frequently, conversations about risk only happen at Board or senior management level, and information 'from those on the ground' who know the risks in their own areas is not inputted. Furthermore, if the process around understanding risks within the organisation is too complex, too rigid or is written in language which staff find difficult to understand, any conversations about risk appetite are likely to be devoid of many who could provide valuable input."

- Head of Thought Leadership, The BCI

The process described in Section 3 on the Importance of Risk Appetite, where risk appetite is both an integral part of strategy setting and based on organisation culture, helps to mitigate these criticisms. Risk appetite cannot be treated as an "add-on", it should provide a framework through which business processes can be used to exploit opportunities in a controlled manner. Section 4 on the Role of Culture also serves to address these criticisms, explaining practical ways in which the pitfalls can be avoided, particularly through consideration of the seven drivers of risk culture.

As described throughout, there is no single correct approach for setting and using the concept of risk appetite. It must consider the industry of an organisation, economic backdrop, risk materiality, organisational culture, leadership style and stakeholder expectations. The risk appetite statement for an investment bank will be very different to that for a large infrastructure construction contractor or that of a local authority. The types of risks, balance of qualitative and quantitative KPIs and KRIs, style of leadership and decision-making will all be different. A statement that is too complex or considered to address the wrong risks will be ignored.

As part of implementation, it is important that employees undergo training with regards to how risk appetite can and should be considered as part of the risk management and decision-making frameworks, and what the overall benefits of it are. This must be backed up by consistent leadership demonstration of the behaviours expected and by appropriate recognition and reward mechanisms that support the effective use of risk appetite in day-to-day activities.

Finally, risk appetite must not be allowed to become the sole responsibility of the risk management function. The risk management function should support and advise, with implementation of processes derived from the risk appetite statement owned by operational managers who are held to account on its use.

5.2 Why is the concept of risk appetite hard to apply?

Whilst risk appetite statements are becoming a standard part of risk management frameworks across many industrial sectors, some consider practical implementation to be an area that requires further development. Key challenges and considerations include:

- Risk appetite and related tolerances (qualitative and quantitative) need to be calibrated at different levels of the organisation, as well as across different units or functions
- Risk appetite can be used as an effective tool to arrive at a more optimum decision on the balance between risk retention, mitigation and transfer (risk transfer optimisation)
- Risk appetite and maturity models can be used to identify improvements, focus effort and foster a continuous improvement mentality
- Risk appetite statements must be formulated and developed in a way to avoid unintended constraints or artificial 'breaches'
- Whilst individual areas need to be considered when developing risk appetite statements/frameworks, they cannot be addressed in a siloed way that might lead to conflicts and unintended consequences. Their requirements need to be framed in a manner that enables management to allocate resources and understand risk/benefit trade-offs
- Risk appetite statements/frameworks need to speak to and serve all levels of management and front-line employees in a language that is meaningful to them and is consistent with other targets and goals
- Risk appetite frameworks and/or statements need to be kept under constant review to ensure they remain relevant despite shifts in the working environment and stakeholder expectations.

Risk appetite is also challenging to apply where an organisation's risk profile is not well understood. In the case of a poorly understood risk profile, this is also likely to be linked to a low level of maturity in risk management. Forming a better understanding of the risk profile will be a necessary initial step before the risk appetite can be set.

6. RISK APPETITE LINKAGES AND TOUCH POINTS

A sustainable risk appetite depends on alignment with an organisation's risk maturity and culture. Risk maturity reflects how an organisation functions relative to its risk appetite, since the appetite framework shapes decision-making, should build on culture and determines the capability of an organisation to approach risk in a balanced and well-informed way over the longer term.

6.1 Risk maturity

Risk maturity reflects how an organisation functions relative to its risk appetite, since the appetite framework shapes decision-making and determines the capability of an organisation to approach risk in a balanced and well-informed way.

Without a clear risk appetite framework and controls around review and escalation, decision-making will be subjective as boundaries are grey and individuals' personal risk drivers are allowed to become key factors in the decision-making process. This may result in some heroic wins when opportunities are taken that work out, but is more likely to lead to failure when resources are invested in areas that are not within the core competencies of the business.

A clear risk appetite establishes the boundaries and tolerances around expectations for behaviours, which is essential for consistent application of risk controls. In immature risk management cases, leadership will be unclear about appetite in many areas, systems of control will be poorly defined, skills, knowledge and incentive structures are likely to be misaligned, and mechanisms for measuring, monitoring and review of performance won't be fully effective.

At a commercial level, mature risk management cases with a clear risk appetite aligned to well-defined authority levels will effectively invest in pre-contract phases so that time and resources are allocated to the right areas. Being clear about what is acceptable and what is not, also makes for effective 'amber management' where escalation requirements become quickly obvious. Avoiding delay and indecision through the clarity provided around appetite and escalation means an organisation can grasp opportunities in the amber zone, succeeding where competitors may fail.

Care must be taken not to cast risk appetite statements in stone. Both internal drivers and external influences in the business environment can shift quickly or evolve imperceptibly over time. Poor resilience and failure to adapt can mean an organisation quickly loses ground against competitors or just fails to adapt to new opportunities for development.

There are a number of indicators of risk maturity including:

- The scope, objectives and implementation of the management of risk, how well these meet the external and internal drivers, address the specific context of the organisation and its value chain, and hence add value to key stakeholders
- How comprehensive, well-structured and fit-for-purpose the framework design is
- The nature and consistency of the organisation's risk culture and how the organisation's collective attitude and individual behaviours towards the application of its risk appetite are influenced by cultural factors (as described earlier)
- How well-embedded (integrated) the risk appetite framework is within the management processes and daily activities
- The efficiency and consistency of amber management processes when escalation is required on appetite-related decisions
- The mechanisms in place for resolving conflicts in appetite should they arise, for instance, in different functions or locations, recognising that risk appetite statements should not be drawn up in isolation or operated in silos
- How the reporting of risk information, including risk appetite conformance and exception, supports decision-making and the degree of alignment risk reporting has with other management and external reporting

How the risk management framework and its implementation are continuously improved to demonstrate measurable benefits to the organisation, including its responsiveness to changes in internal drivers and shifts in the external business environment.

Each of these risk management maturity factors not only influence the risk appetite of an organisation and its application in practice but are also reflections of it.

6.2 Sustainability

Whilst we cannot address fully the subject of sustainability in this guide (where the focus is squarely on risk appetite), it at least deserves a mention in terms of linkages. A key part of risk culture is driven by an understanding of the societal purpose as well as clear definition of the integrity and ethical values that the organisation represents. So, we cannot talk about risk appetite as a key feature for success and longevity of organisations in isolation, but must consider the growing sustainability movement which challenges capitalist models of shareholder wealth creation in favour of much wider stakeholder value, where results aren't just about generating profit but how the organisation impacts on people and the planet – the triple bottom line.

Typically, risk appetite statements are grouped and aligned to traditional risk categories such as operational, financial, strategic, etc. A different way could be to align risk appetite statements to environmental, social and governance (ESG) factors as three central tenets to drive a culture of sustainability. After all, sustainable continuity and success have to be the key indicators that risk has been managed effectively for the long term.

This may seem too narrow a set of criteria to address the whole of the organisation, but given that effective governance should set expectations and risk appetite for all areas and monitor performance accordingly, the Governance section of this approach can also be used to capture KPIs in areas such as finance, operations, innovation, etc.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the World Business Council for Sustainable Development (WBCSD) have collaborated to create a guide on Enterprise Risk Management – Applying enterprise risk management to environmental, social and governance-related risks. Risk appetite considerations can be applied when incorporating ESG risks into the wider risk management framework.

Clearly some of the above are already governed by minimum standards set by legislation and regulation, but risk appetite statements, and their effective implementation, can be used to drive a risk culture with sustainability clearly in view.

To drive a culture of sustainability and the long view on the management of risk, risk appetite statements may be set along following parameters as in Figure 14.

Figure 14 Summarising EDG factors from various sources including COSO's ERM-ESG guide (Referred to previously), the UN Global Compact, ISO 26000 and Global Reporting initiative (GRi), plus UK Government Guidance and the Principles for Sustainable Insurance.

Environmental

- Climate Emergency
- Greenhouse Gas Emissions
- Energy Efficiency
- Biodiversity
- Deforestation
- Pollution
- Resource Scarcity
- Waste and Water Management

Social

- Community Relations
- Human Rights
- Diversity and Inclusion
- Employee Engagement and Working Practices
- Customer Satisfaction
- Consumer Protection
- Public Policy Advocacy

Governance

- Board and Top Management Composition
- Conduct and Ethics
- Fair Remuneration
- Financial Crime
- Data Protection
- Whistleblowing
- Tax Transparency
- Procurement and Partnerships
- Investment Strategies
- Independent Audit

6.3 Insurance purchasing

What has been discussed in this guide applies fully to the buying of insurance. After all, it is an integral part of the risk management system and one of the risk response options an organisation can leverage to manage its risk exposure so that it aligns with its set risk appetite and tolerances. This section demonstrates the interconnectivity of risk and insurance management, highlighting the need for stronger engagement of those responsible for insurance purchasing in the risk appetite process.

Informed business decision-making, of which insurance purchasing is a part, benefits significantly from systematic consideration of risk information and from using risk information and risk appetite to frame and prioritise the decision alternatives. Some companies may speak with their broker about their key risks at a high level, but they often fail to make a full assessment of what the maximum probable loss is for their business and where their risk capacity is sufficient.

Whilst some companies understand that having well-informed insurance and mitigation strategies in place has a positive impact on the delivery of their organisation's short, medium and long-term ambitions, this is not commonplace. Risk appetite plays a key role in this as it is about understanding the art of the possible: setting risk tolerances and limits to risk exposures, and subsequently using insurance and other risk transfer methods as well as controls and mitigations to ensure that the maximum probable losses do not exceed these thresholds.

Understanding the potential for loss is a complex subject. Often, the use of statistical models, and other quantitative methods grounded in consensus assumptions, are necessary to model a range of scenarios. This way, consideration can be given to the full range of possible impacts. It is key to strike a balance when determining the appropriate level of insurance coverage. Too little insurance and the organisation is at risk of significant losses. Too much and the organisation is wasting money on coverage that it already has internal capacity for and that is unlikely be triggered. Hence, clarification over risk capacity and risk appetite is crucial.

A clearly articulated risk appetite will support the definition of realistic and cost-efficient insurance and retention requirements. Risk appetite could therefore directly impact the risk financing of an organisation, including risk transfer to the insurance market and consideration of deductibles as part of it.

Deductibles are an essential part of the insurance contract and therefore a component of an organisation's risk management strategy. They are typically used by insurers to deter the large number of claims that a policyholder can be reasonably expected to bear the cost of. By restricting its coverage to events that are significant enough to incur large costs, the insurer expects to pay out slightly smaller amounts much less frequently, incurring higher savings.

Understanding the role and consequences of deductibles is key to informed insurance purchasing, as the level of deductibles agreed will have a direct impact on insurance premium for the policyholder. Organisations with a mature understanding of both the nature of their insurable risks, and their tolerance for the impacts these risks may cause, have effectively leveraged this knowledge to purchase insurance policies that are more appropriate to their business model and more balanced in terms of retention and risk transfer. Moreover, the premium itself tends to be more reflective of the insurable risks faced, benefiting both policyholder and policy issuer. In conclusion, case studies have indicated that a greater transparency of the policyholder's risk-bearing capacity will support optimising the amount of risk transferred to the insurance market and, ultimately, drive business performance by reducing the Total Cost of Risk (TCOR).

7. CONCLUDING THOUGHTS

The pace at which industries, technology and global interrelations are changing is ever increasing, making it vital that organisations continuously review and update the risk appetite where and when necessary. In some sectors more than others, this applies to their regulatory environments as well. In many more, it applies to stakeholder and societal expectations of big business and organisations established to serve the population.

- As a result, the setting of appropriate risk appetites should not be a one-off, static process, but instead these risk appetites should be monitored and reflect changes in both the internal and external business context.
- This calls for a systematic process for updating the risk appetite, allowing sufficient flexibility to ensure that it does not become an administrative burden. To enable this, leading organisations have defined criteria to trigger risk appetite statement updates to complement review requirements, incorporating conditions including regulatory changes, cost of capital, activist investors, and supply and demand.
- Risk appetite and risk culture are mutually supportive, each being able to drive improvement in the other, so it is important that an appropriate risk culture is in place across the organisation. This will ensure that lessons learned can be openly discussed and implemented, and the necessary adjustments made to the risk appetite and applicable risk tolerances.
- To develop a risk culture that encourages continuous improvement, it is important to have an effective 'tone at the top' (the attitudes and behaviours demonstrated by senior management) within the organisation, but equally important is the capability and understanding of people at all levels, open communication and appropriate alignment of incentives.

APPENDIX – DEVELOPING EFFECTIVE KEY RISK INDICATORS (KRIs)

Introduction

Key Risk Indicators are used to measure the level of risk that a business is exposed to. Designed and used well, they can provide management with advance warning that a risk is increasing in its potential to materialise. As a result, they offer management an opportunity to investigate and, where needed, take action to prevent the risk from impacting the business.

It is worth exploring the relationship between a Key Risk Indicator (KRI) and a Key Performance Indicator (KPI).

Risk indicators and performance indicators are linked, and they can easily be confused and misunderstood.

All too often they are defined, recorded and monitored in isolation, but there are strong arguments to align them and consider them as part of the same ecosystem. Ultimately, they are both crucial to management's oversight of the business and how it is performing against its objectives.

For example, KPIs look at how the business is performing against its targets and goals. KRIs look at what might prevent the business from achieving those targets and goals.

This is why it is important to view KPIs and KRIs as part of the same ecosystem of management oversight, both looking at the performance of the business, just through a different lens. Viewing them in this way will also enable the identification of more effective KRIs, because they will be more likely to be aligned and relevant to the overall business objectives.

Principles of effective KRI development

To fully exploit the potential benefit from KRIs, there are some principles that are important to consider during their development and implementation. Where possible, they should be:

- **Relevant to the overall risk profile:**

They should help to quantify the risk, and as the business and risk profile changes, the KRIs can and should change with it

- **Aligned to the corporate strategic objectives:**

They should be informing management of the potential risk to their strategic objectives and whether these are within their appetite for the risk

- **Measurable and easy to obtain and report:**

They should be able to be quantified in a way that is measurable, with the methodology being reliable and consistent over time. This will enable comparisons to be made and trends identified

- **Leading or preventative in nature:**

Generally, the most effective KRIs are those that enable management to investigate and act before a risk has materialised. KRIs should where possible be 'leading' or 'preventative' so that they are providing management with a future view of risk rather than a retrospective one

- **Focusing on the root cause of the risk rather than the symptoms:**

KRIs that focus on the symptoms of a risk will only alert management that a risk is materialising and will reduce the time that management has available to act. The insight provided to management could be misleading and therefore any actions taken will likely have a short-term, delaying effect. KRIs that measure movements in the root causes of a risk will enable management to implement effective solutions before the risk materialises and impacts the business.

Steps to developing effective and relevant KRIs

Figure 15:

Step 1 Map and align corporate objectives with risks	**Step 2** Select the 'key' risks rather than all	**Step 3** Complete a RCA (Root Cause Analysis) of the key risks	**Step 4** Identify suitable metrics, both existing and potential	**Step 5** Assign tolerance levels aligned to risk appetite of the risk	**Step 6** Define frequency and audience of KRI monitoring
A mapping of corporate objectives may already exist, and this can be used as the starting point for KRI development. If not, complete an alignment of risks to the overarching corporate objectives. This exercise will ensure relevance of the resulting KRIs.	It is possible that there could be many risks identified. Developing and monitoring KRIs for all risks would likely be unsustainable. Therefore, it is important to identify the most critical indicators for the highest risks. The risk owners and other management stakeholders should be involved in this process.	To ensure that the KRIs will focus on measuring the root cause of the risks and not the symptoms, a root cause analysis (RCA) should be conducted against the highest risks identified. Several methods could be used for this purpose, including the '5 Whys Analysis' or the 'Fault Tree Diagram'. The principle is to target the root cause, so either these formalised methods or more informal approaches could be used.	It is likely that the business already gathers, reports and monitors hundreds of metrics and data points. Engage the risk owners and subject matter experts to identify if there are existing sources of data already used that could also be used for measuring the risk root causes identified in Step 3. Where there are gaps, look to identify suitable metrics that could be efficiently generated and reported.	According to, and in alignment with the risk appetite for the risks, assign tolerance levels (upper, lower and target) to each metric. This exercise is most effective if the risk owners and subject matter experts are again engaged to support the identification of these levels.	Align with the management team the frequency and audience for the review and monitoring of the KRIs. Develop a clear dashboard and reporting pack that can be circulated in advance of any review meetings to ensure that the team have an opportunity to review and ask questions before the review meeting.

Key Risk Indicator - A worked example

This example works through the steps suggested for the development of a Key Risk Indicator.

The diagram below (see Figure 16) shows the hierarchy and analysis of Steps 1 to 3 – identifying the strategic objectives, selecting the key risks that could impact achieving the objective and subsequently undertaking the Root Cause Analysis (RCA) to identify the root causes. This then drives the identification of relevant and effective Key Risk Indicators.

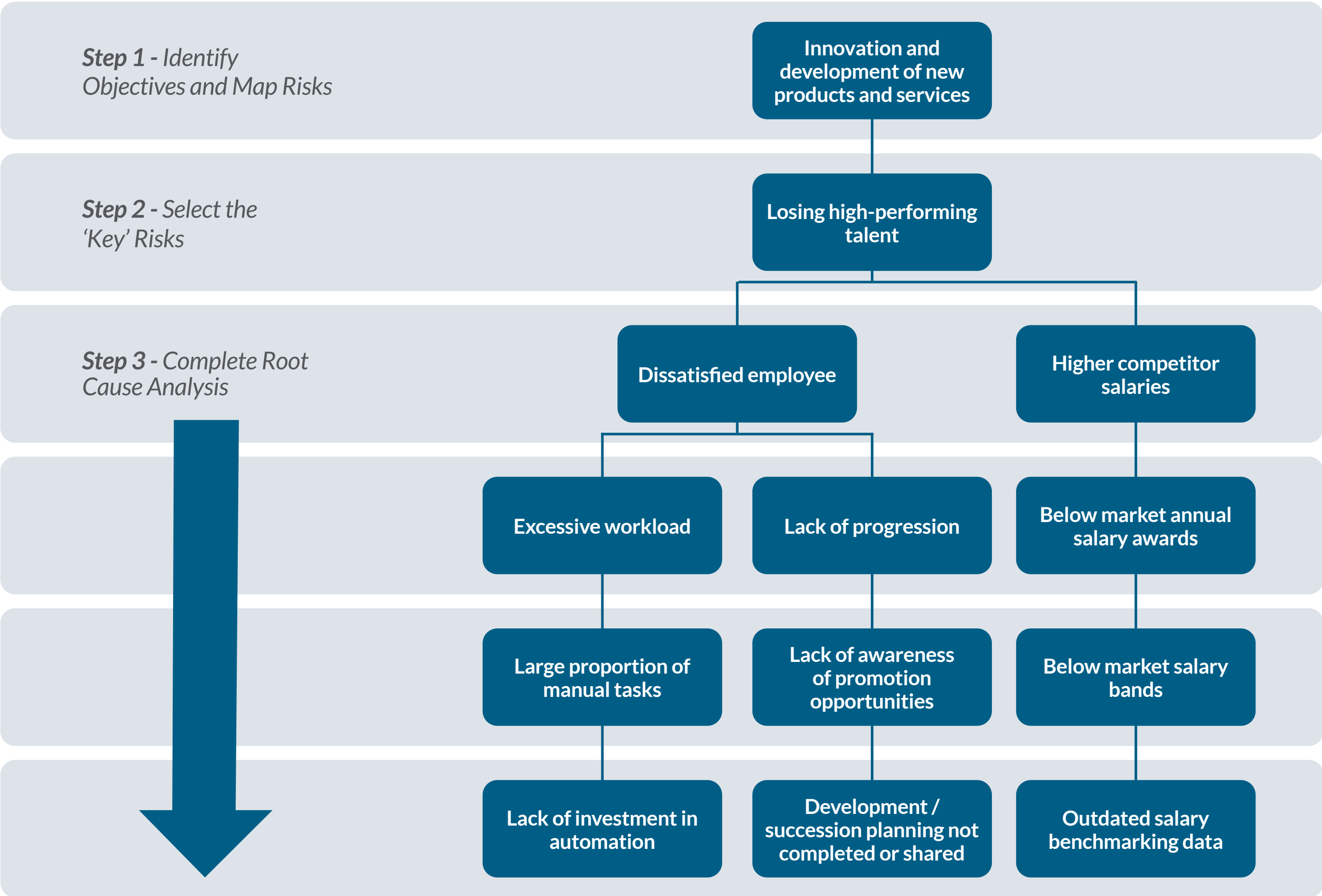
For the purposes of this example, the objective selected is 'Innovation and development of new products and services'. There are likely to be lots of risks that could prevent a business from achieving this objective; however, we will explore the risk of 'Losing high-performing talent'. This is likely to be a fairly common risk that may appear in the enterprise risk registers of most businesses.

It is common that KRIs for 'People' or 'Talent' related risks tend to focus on levels of dissatisfaction recorded in employee surveys or metrics for employees leaving the company. Placing reliance on these metrics as KRIs will focus attention on the 'symptoms' of a risk materialising, rather than the real root cause of the risk.

If a high-performing employee is already dissatisfied, or has left the business, it is already too late for management to act to prevent the risk from materialising.

Therefore, we need to conduct a deeper analysis and explore this further down the chain of root causes. This will enable suitable metrics to be identified to give management the early warning they need.

Figure 16:



Step 4 – Identify suitable metrics, both existing and potential

It is likely that the business already gathers, reports and monitors hundreds of metrics and data points that could be used to support the KRI development. It will be important to engage the risk owners and subject matter experts to assess what is already available and what may need to be developed.

Metrics could be applied at any of the levels of the root cause analysis. It will be down to the judgement of management to assess the most appropriate level. Some examples of metrics are suggested below in Figure 17.

Figure 17:

Risk Root Cause	*Example KRI metric*
Higher competitor salaries	*% High-performing talent salaries > mid-point of salary band*
Below market annual salary award	*% Deviation of salary awards compared to upper, mid-point and lower-end market salary awards.*
Below market salary bands	*% Deviation of mid-point, lower level, upper level of salary bands from market average levels*
Outdated salary benchmarking data	*Salary benchmarking data updated within the prior 3 months of the annual salary review cycle*

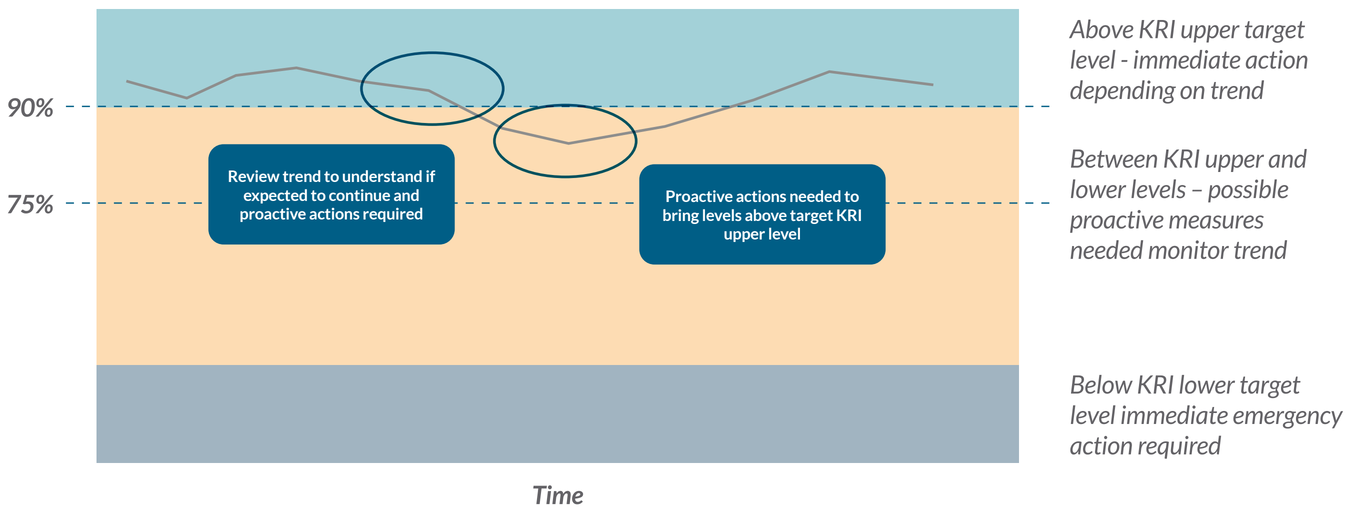
Step 5 – Assign tolerance levels aligned to risk appetite of the risk

According to, and in alignment with the risk appetite, assign tolerance levels to each metric (consider upper, lower and target depending on metric type).

Figure 18:

Higher competitor salaries	*% High-performing talent salaries > mid-point of salary band*

Figure 19:



Step 6 – Define frequency and audience of KRI monitoring

Align with the management team the frequency and audience for the review and monitoring of the KRIs.

This will depend on the types of risk and the KRIs being monitored. Some would benefit from a more regular monthly review and others may not need reviewing any more often than every six months. This needs and benefits from engagement and discussion with senior management and the relevant risk owners.

Ideally, a clear dashboard and reporting pack should be developed that can be circulated in advance of any review meetings to ensure that the team have an opportunity to review and ask questions before the review meeting. Having these KRIs in one place, so that management are receiving a consolidated view that enables them to look across all risks and KRIs enables potential connections and dependencies to be visible.

It is also worth considering if the general management KPI pack could be expanded to include the KRIs as well. As referenced earlier, KRIs are providing management with an early warning that their objectives and goals, as measured by the KPIs, are at risk of being missed.

A regular review of the KRIs and their tolerances is also of importance. This enables the KRIs to remain relevant to the market, the business objectives, the business risks and the business appetite.

Further Reading

- www.airmic.com – Airmic Explained – Risk and managing risk
- www.airmic.com – The Chairman's Forum – Ensuring corporate viability in an uncertain world
- www.bsigroup.com – ISO 31000: 2018 - Risk Managenment Principles and guidelines
- www.coso.org COSO – Understanding and Communicating Risk Appetite
- www.coso.org COSO ERM – Enterprise Risk Management Framework: Integrating with Strategy and Performance
- www.gov.uk – Government Publications – Orange Book
- www.theirm.org IRM – Risk Culture – Resources for Practitioners
- www.rims.org RIMS – Exploring Risk Appetite and Risk Tolerance
- www.soa.org Society of Actuaries – Risk Appetite: Linkage with Strategic Planning
- www.iod.com Institute of Directors – Business Risk – A practical guide for Board members
- www.frc.org.uk – Guidance on Risk Management, Internal Control and Related Financial and Business Reporting
- www.fca.org – Enhancing frameworks in the standardised approach to operational risk

9. GLOSSARY

- **Risk attitude –** The opinion or chosen qualitative or quantitative value in comparison to the related loss or losses taken by individuals. This is linked closely with risk perception and underpins the risk culture of an organisation.
- **Risk culture –** The shared values, beliefs, knowledge, attitudes and understanding about risk, shared by a group of people with a common intended purpose, in particular the leadership and employees of an organisation. Every organisation has a risk culture that should support the achievement of objectives.
- **Risk maturity –** The measure of how well the enterprise risk management (ERM) is working across the whole organisation.
- **Risk perception –** The judgement made by individuals with respect to risk both in terms of the potential impact of downside and the opportunities presented by the risk scenario.
- **Risk tolerance –** The amount of risk or degree of uncertainty that an organisation is willing to pursue or retain.
- **Risk monitoring –** The process by which risks facing the organisation are tracked, and the trends reported to management to inform decision-making.
- **Key Risk Indicators –** The metrics implemented across the organisation to proactively monitor the level of risk-taking in an activity or organisation that may impact the strategic objectives.
- **Risk data –** The data from across the business that is used to monitor the levels of risk facing the organisation. This may be in various formats and derived from a number of systems/sources.
- **Risk technology –** The various systems and data that support effective risk management. Often referred to as Governance, Risk Management & Compliance (GRC) technology.

Airmic
Marlow House
1a Lloyd's Avenue
London
EC3N 3AA

Tel: +44 207 680 3088
Fax: +44 207 702 3752
Email: enquiries@airmic.com
Web: www.airmic.com