airmic

Risk and managing risk EXPLAINED Guide

In association with:

Marsh

RISK AND MANAGING RISK EXPLAINED GUIDE

CONTENTS

1. INTRODUCTION

Risk-taking is fundamental to the success of any organisation. The leaders of an organisation must decide the extent to which risk needs to be sought, accepted, addressed or avoided, and their approach to this will determine how risks are managed across their organisation.

The concept of risk management has been of increasing relevance and importance in recent years, triggered in part by the greater maturity of corporate governance frameworks and recognition of risk management as an enabler and protector of value and achievement of strategic objectives.

Societal trends such as business accountability, disclosure of information, the velocity of change, the connectivity of risks, the impact of emerging technologies and high impact, low probability risk have all added emphasis and importance to the need for effective risk management.

According to the 2024 World Economic Forum Global Risk Report, the disruptive capabilities of manipulated information are rapidly accelerating, as open access to increasingly sophisticated technologies including artificial intelligence (AI) proliferates and trust in information and institutions deteriorates. It is anticipated that the boom in synthetic content will amplify societal divisions, with rises in ideological violence and political repression.

The rapid proliferation of AI brings with it a potential shift in how society and business interact with the digital world. New opportunities and challenges are emerging at an unprecedented speed, but we need to identify risks and opportunities, how we embrace and manage these, and how we protect ourselves from the unforeseen consequences that could flow from unregulated AI development and adoption.

The 2024 Edelman Trust Barometer highlighted the risks which are exacerbating trust issues, bringing with it the threat of further societal instability and political polarisation.

Coupled with the rise in global regulations and laws, risk management has never been higher on the board agenda nor required more of today's risk manager.

A wealth of knowledge, guides, standards and publications exists to help with the detailed development of risk management strategies and implementation of risk management programmes.

However, the focus now is to address increased complexity and connectivity, and ensure that risk management enhances business models by operating as an integral part of established and future processes. This approach requires a shared view of the impact of risk on business objectives and effective communication between business leaders, functional teams and business operations.

This guide summarises current approaches to risk management to promote a shared understanding. It will be particularly useful for those new to risk management.

It looks initially at the definition of risk and how risk management helps organisations address uncertainty.

It then summarises the key principles underpinning the design and operation of a risk management programme with reference to the international risk management standard ISO 31000:2018. It moves on to consider how risk governance fits within the developing corporate governance codes and framework and associated guidance s.

Human and cultural factors have a fundamental impact on the success of the risk management programme. These factors and the importance of leadership are considered in section 5.

Section 6 focuses on articulating risk within the organisation and will help the reader understand how risks are identified and assessed in the internal and external context of the business. The approach to accepting and managing risks in order to create and protect value varies substantially across businesses and this section highlights the way risks are

evaluated in conjunction with the risk criteria developed by the business.

The guide incorporates practical examples where appropriate. It also introduces the subject of organisational resilience and outlines the importance of appropriate resilience within the wider risk management approach. The International standard ISO 22301:2019, which specifies the requirements for a management system to protect against, reduce the likelihood of and ensure a business recovers from disruptive incidents, and British standard BS 65000:2014, which provides guidance on organisational resilience, are both referenced alongside cases from the Airmic Roads to Ruin and Roads to Resilience publications.

The guide outlines why internal and external communication and monitoring are a key part of any successful risk management programme. The impact of the Financial Reporting Council (FRC) guidance is considered as part of the external communication strategy of a listed company.

This guide is intended to be used by Airmic members starting out in their career in the profession, and by those who may be new to this subject, or to be shared with their business colleagues in areas such as procurement, finance, human resources, IT and internal audit.

2. WHAT IS RISK?

Risk is a natural part of life, both in business and leisure. In *Against the Gods*, Peter Bernstein, the American financial historian, portrays the mastery of risk as the key revolutionary idea defining the boundary between the past and modern times. He demonstrates how the understanding and management of risk has been and continues to be the driver for economic prosperity.

Risk is linked to uncertainty as many ventures face challenges and obstacles on the path to success.

2.1 Understanding the definition of risk

Whilst there are many definitions of risk, this guide adopts the definition contained in the international standard ISO 31000:2018 which states:

"Risk is the effect of uncertainty on objectives."

The following are of particular importance in considering this:

- This definition allows for either a positive or negative deviation from the planned outcome. This is an important distinction and helps view risk as something to be embraced and not just controlled or avoided.
- Risk is often characterised by reference to potential events and consequences. For example, low-lying premises near a river might be at risk of flooding, which could cause damage to property and disruption to a business, a community or people.
- Risk can be expressed in terms of a combination of the consequences of an event and the associated likelihood of an occurrence. This can be helpful to allow comparison of disparate risks with very different impacts on an organisation or its people and other stakeholders including investors, suppliers and customers..
- Uncertainty is inherent in risk. Uncertainty can arise from a number of different sources, including a deficiency of information, understanding or knowledge of an event, or a lack of awareness of its possible impact and likelihood.
- Objectives can have many different dimensions, including finance, safety, quality, regulatory or reputation, and can apply at different levels of an organisation.
- An appreciation of these metrics helps determine risk characteristics such as causes and consequences, as well as helping design risk indictors to monitor risk status.

2.2 What is risk management?

Risk management is the identification, assessment and prioritisation of risks followed by coordinated and economic

application of resources to maximise the realisation of opportunity or address the impact and/or likelihood of adverse events.

Risk management should have an objective to ensure that managing risk creates and protects value. Risk management must be an integral part of the management system and be embedded within the culture of the organisation, encompassing the entire workforce.

2.3 Recognising sources of risk

No organisation or individual can exist in isolation and consideration of risk must take account of factors that are both internal and external to an organisation. The internal and external environment in which the organisation seeks to achieve its objectives is referred to as 'context' in the ISO guide.

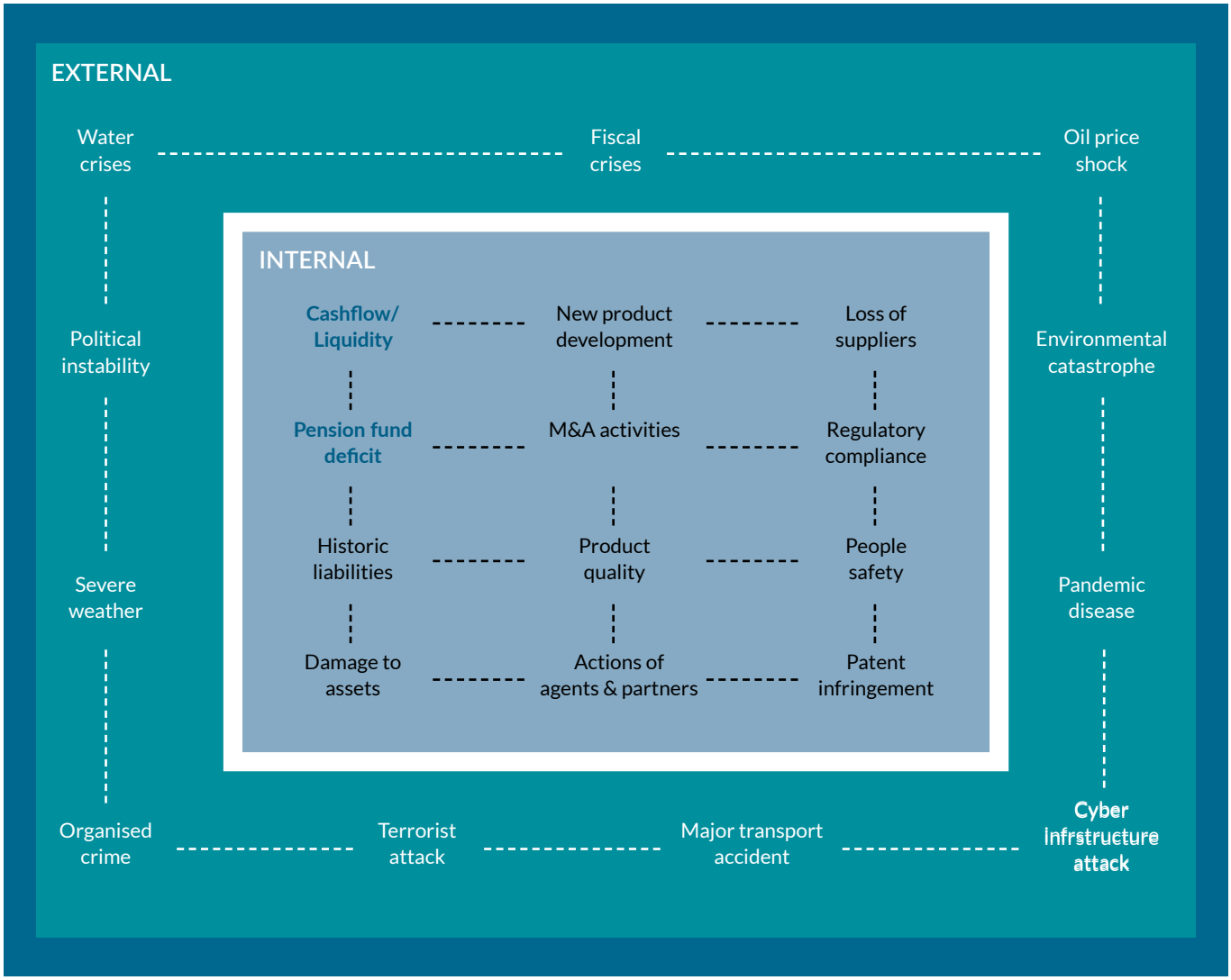
There should be an understanding of the interconnectivity between internal and external risk events and coordination of risk management activities through supply chain partnerships, where possible. Figure 1 illustrates internal and external sources of risk.

2.4 Analysing and evaluating risks

There are many ways in which an organisation might choose to evaluate risks arising from the internal and external contexts, and there are many different response strategies depending upon the objectives of the organisation

FIGURE 1

Some examples of internal and external sources of risk



However, it is important to recognise that a successful risk management approach will add value by integrating with and supporting existing business systems to enable improved decision-making and to enhance controls and realise opportunities.

Once the organisation has understood and evaluated the risk in the context of the business, attention turns to risk treatment to address the risk.

2.5 Treating risks

Options for risk treatment include removing the source of the risk, changing the nature of the risk, sharing the risk with another party, seeking an opportunity to create or enhance the risk, or avoiding the activity. Risk management tools are used to determine the possible impact of the risk and its likelihood. These help organisations to understand their risk exposure and the relative importance of the risks to assist them in establishing priorities for action. For example, an organisation has a number of options to address the risk of disruption relating to a single-source supplier, including appointing a dual supplier, creating capacity inhouse or accepting the risk, periodically monitoring it to ensure acceptability, and potentially transferring the financial implications of supplier failure to an insurance solution.

In practice, it is necessary to have regard to organisational objectives, and management and operational processes, and to consider these in the internal and external context in order for risk decision-making to be effective.

Risk management assists the organisation by specifically addressing uncertainty. It establishes a structured process, operating within existing systems and procedures, to clarify the nature of the uncertainty and how the uncertainty might be addressed.

When a risk treatment concerns an opportunity this might include exploit (increasing the likelihood), experiment (testing new solutions or gathering and analysing additional data), enhance (taking more of the risk or relaxing controls) or accept (adding no additional controls).

2.6 Introducing Enterprise Risk Management

Enterprise risk management (ERM) is the term used to describe risk management applied across the entire organisation. ERM should be integral to the planning and performance across the entire enterprise.

Risk maturity is about having a sustainable, repeatable and mature ERM programme. Risk maturity models measure maturity from the equivalent of 'ad hoc' to 'fully embedded' levels. Risk maturity models or tools can be used to assess maturity using maturity metrics.That facilitate benchmarking of a programme against a number of criteria, which typically include the planning and governance of the programme, the execution of risk assessments, and the aggregation, analysis and communication of risk information. These criteria form a matrix with competency drivers which are scored.

Research indicates from the analysis of organisations using risk maturity models that mature risk management can be correlated with enhanced business performance. However, the highest score from a maturity model is not always necessary or desirable – key is the systematic assessment against the risk management objectives of an organisations and this should drive maturity model targets. The cost of risk controls should be proportionate the improvement in managing risk.

The term 'risk progress' is also used as an alternative to 'risk maturity', which for some risk professionals better expresses the risk journey being travelled towards a target or risk maturity goal.

2.7 The COSO risk management framework

Whilst this guide focuses on the risk management standard ISO 31000:2018, it is important to be aware of other risk management standards and frameworks. The most commonly used in addition to ISO 31000:2018 is the COSO Enterprise Risk Management (ERM) framework. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued the Enterprise Risk Management – Integrated.

Framework to help businesses and other entities incorporate into policy, rule and regulation, and it has been used by thousands of enterprises to better control their activities in moving toward achievement of their established objectives. COSO initiated a project to develop a framework that would be usable by organisations to evaluate and improve their enterprise risk management. COSO ERM required considering risks from a portfolio or 'enterprise' perspective, which was not contemplated in COSO's Internal Control – Integrated Framework, which is a complementary but distinct publication first released by COSO in 1992.

FIGURE 2

The COSO Framework is a set of principles organised into five interrelated components

The COSO ERM framework was revised and reissued in 2017 under the title Enterprise Risk Management – Integrating with Strategy and Performance. As with ISO 31000, it emphasises the connectivity between performance, strategy and ERM. The COSO ERM framework contains 23 principles that can be used to inform the design and continuous improvement of a risk management framework.

The principles are grouped under the following headings:

- Risk governance and culture
- Risk strategy and objective setting
- Risk in execution
- Risk information, communication and reporting
- Monitoring enterprise risk management performance

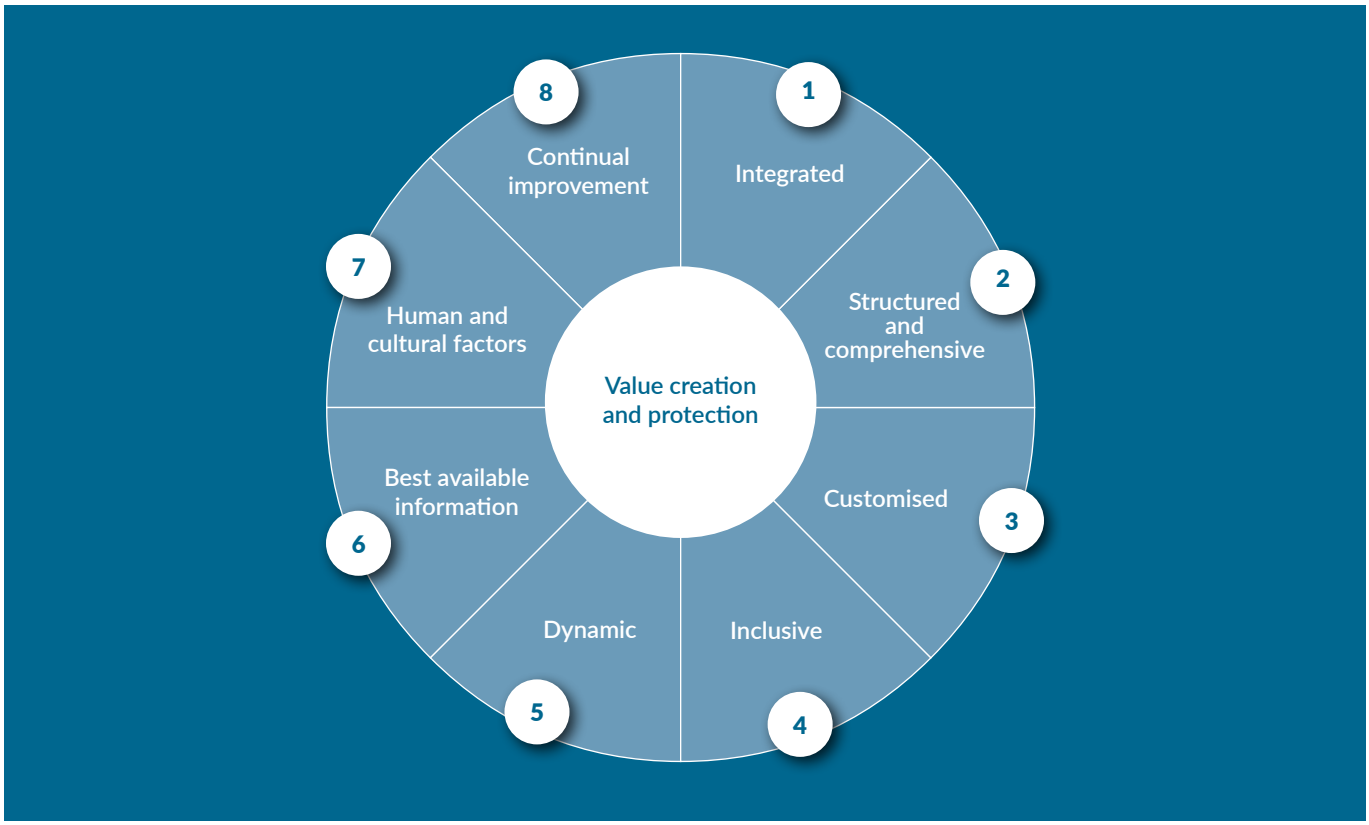
The COSO approach is scalable and suited to all organisations.

The structure of the COSO ERM is illustrated in Figure 2 above.

3. UNDERSTANDING RISK MANAGEMENT PRINCIPLES

FIGURE 3

The risk management Principles – ISO 31000:2018



Effective risk management enables better decision-making, leading to enhanced stakeholder value creation and protection.

ISO 31000: 2018 contains eight principles which help guide organisations in the design, implementation and evaluation of their risk management framework to ensure it contributes to the demonstrable achievement of objectives and improvement of performance.

These principles (See Figure 3.) A more detailed description/ explanation of these principles follows:

1. **Integrated: To be truly effective, risk management must be an integral part of the management system and be embedded within the culture of the organisation, encompassing the entire workforce.**

   Risk management should not exist as a stand-alone activity.

   It must be structured within and form part of all organisational processes, including strategic planning, operational, financial, legal, IT as well as project and change management processes. The approach will

enable the organisation to grasp new opportunities whilst reducing the risk of business threats to it in a controlled manner. Board risk blindness can be avoided by encouraging the sharing of information and bringing uncomfortable truths to senior management, so that board decisions are well informed. The risk framework must be designed to reflect the reality of internal and external influences.

However, risk should not be a bureaucratic process but one which is intuitive, connected and dynamic. Management systems are important to enable integration, but arguably more critical are employee participation and shared ownership, regardless of functional or business unit reporting lines.

Risk management is an integral part of decision-making. Risk management should assist the organisation in making decisions about activities that may represent either upside or downside risks. Risk-taking must be recognised as an important part of decision-making. Such decisions will be informed by the organisation's appetite for risk (see section 6 of this guide). For example, an organisation will generally have a higher risk appetite for commercial risk than for regulatory risk. Effective risk management, properly embedded within the decision- making process, will help an organisation survive and thrive.

2. **Structured and comprehensive: Risk management is systematic, structured and timely.**

Risk should be dealt with in a consistent way across different disciplines, allowing for decisions to be taken with confidence and avoiding duplication of effort, through efficient use of resources and management tools.

The risk management framework should comprehensively cover all areas of risk, both internal and external, that are of relevance to the organisation.

Whilst the framework would be expected to incorporate a risk procedure providing clear guidance to members of staff with risk roles and responsibilities, it should not be overly bureaucratic as this will hinder implementation.

3. **Customised: The risk management framework is tailored to the organisational need and context. The approach to risk management should be proportionate and scaled to the needs of the organisation and the business environment in which it operates.**

Organisations operate in different contexts so that risk management needs to be tailored to the specific organisation's requirements. For example, organisations working in highly technical environments such as the nuclear industry will have a much more complex risk management approach compared with a small retailer.

Business ownership and growth trajectory are also important considerations, for example, a privately held business seeking an Initial Public Offering (IPO) will have a considerably different framework to a partner owned organisation.

4. **Inclusive: Risk management is transparent and inclusive.**

Key stakeholders within the organisation have formalised accountabilities and responsibilities for risk management. However, all members of staff have a part to play, for example, in communicating risks and incidents and embedding the control framework. Senior management should ensure that all internal and external stakeholders are identified, and that effective two-way communication is maintained. This will help in the identification and assessment of risk, and inform and drive the organisational response.

5. **Dynamic - Risk management is agile, iterative and responsive to change.**

Organisations need to be able to respond effectively to internal and external change in a timely manner. The risk management framework should be able to continually identify and respond to significant change, recognising that some factors are subject to frequent change whereas others can remain constant over long periods.

Risk management assists the organisation in clarifying the nature of the uncertainty and how the uncertainty might be addressed.

6. **Best available information: Risk management decisions**

should be based on the reliable sources of data.

Sources of risk data will include subjective opinion, empirical data and forecast information. Data should be accurate, timely and verifiable, with quality assurance in place.

Risk perception and attitudes will vary widely across the organisation and the risk manager should be aware of biases which may distort risk information and lead to the wrong decisions being made.

Risk owners should be prepared to question assumptions and opinions, and be aware of how risk can change over time.

7. **Human and cultural factors: Risk management takes human and cultural factors into account.**

Risk culture is a term that describes the values, beliefs, knowledge and understanding about risk shared by a group of people with a common objective. An effective risk culture enables and rewards individuals and groups for taking the right risks in an informed manner. Risk culture is considered in more detail in section 5 of this guide.

8. **Continual improvement: Risk management facilitates organisational learning.**

Over time, the organisational objectives will change to reflect the new environment. There should be a regular review of the way in which these risk management principles are applied, taking account of learning from relevant events, technological change and stakeholder expectations, to ensure that the risk management approach continues to support and drive these new objectives.

"Directors face discharging their responsibilities for risk management in an increasingly complex and fast moving world.

"Before they should not however be expected to know all the answers about every risk, or combination of risks, but they should be expected to ask Informed questions posed to relevant experts employed or contracted by the company. The Airmic series of guidance published with Airmic Partners McGill and partners, "Perfecting Governance", is designed to provide a context with twelve questions each designed to help directors explore a series of important risk subjects at the boardroom level".

Julia Graham, CEO, Airmic

4. GOVERNANCE

4.1 Governance explained

Governance, Corporate Governance and Risk Governance
Governance is a system that provides a framework for managing organisations. It identifies who can make decisions, who has the authority to act on behalf of the organisation and who is accountable for how an organisation and its people behave and perform. Governance enables the management team and the board to run organisations legally, ethically, sustainably, and successfully, for the benefit of stakeholders, including shareholders, employees, customers, and for the good of wider society". (Chartered Governance Institute UK and Ireland 2024: www.cgi.org.uk)

Corporate Governance is a code of behaviour expressing how management teams in organisations should act and be governed, to create and protect value on behalf of their stakeholders.

The purpose of Corporate Governance is to create and maintain a flexible, efficient, and effective framework for good management that delivers on the stated objectives of an organisation over the longer term. Risk governance applies the values of Corporate Governance to the ways in which an organisation manages its risks. Good risk governance is associated with having clearly defined roles and responsibilities across the organisation, where management collectively recognises its ongoing responsibility to manage risks.

Successful Risk Governance starts with an understanding of the objectives. The risk management framework will be developed to reflect the corporate objectives and the risk objectives. Different organisations will have different objectives and very different views of the risks they are prepared to take and the opportunities they are prepared to take to achieve these. The governance and framework will reflect this. Risk governance relies on assurance over identified risks, as well as confidence in the assessment of the impact and likelihood of the risks. There should be assurance around the organisation's risk control environment and effective allocation of resources in response to risk.

Successful risk governance starts with an understanding of the objectives. The risk management framework will be developed to reflect the corporate objectives and the risk objectives. Different organisations will have very different objectives and therefore very different views of the risks they are prepared to take and the opportunities they are prepared to take to achieve these. The governance and framework will reflect this.

Successful risk governance relies on assurance over risk exposures, as well as confidence in the assessment of the impact and likelihood of the identified exposures. There should be assurance around the organisation's risk control environment and effective allocation of resources in response to risk.

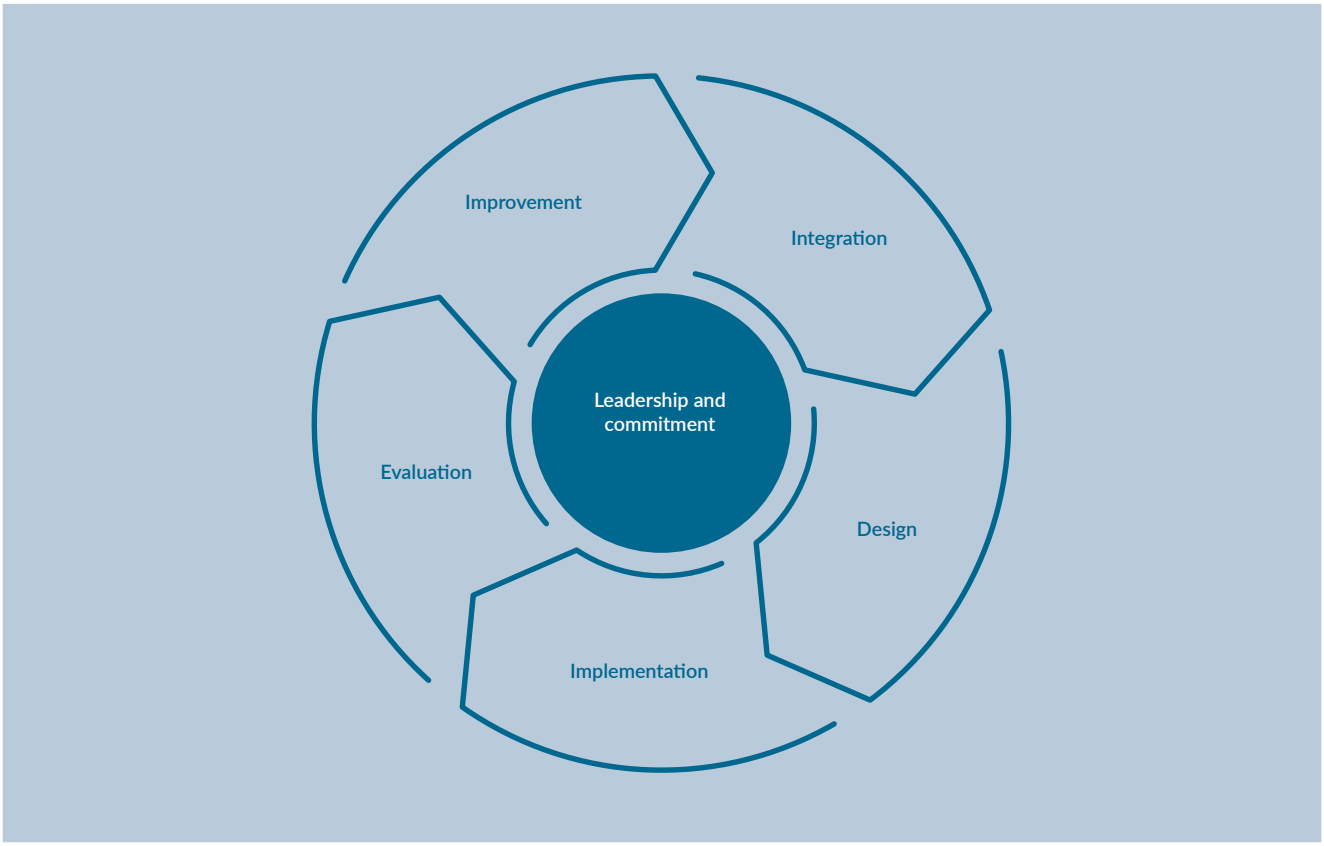
Successful risk governance starts with an understanding of the objectives. The risk framework will be developed to reflect the corporate objectives and the risk objectives. Different organisations will have very different objectives and therefore very different views of the risks they are prepared to take to achieve these. The governance and framework will reflect this.

> *"Organisations must build a more inclusive pipeline of talent for senior management roles. There are proportionately still more men than women holding positions as head of risk management and/or heads of insurance, and this impacts the gender pay gap".*

Investing in the right future: Artificial intelligence and the Future of the Profession - Airmic annual survey 2023

FIGURE 4

Risk management Framework ISO 31000: 2018



4.2 Introducing the risk framework

The framework encompasses the organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management. It provides a structure for using the risk management process as a basis for decision-making and accountability at all levels of the organisation. The relationship between the components of the framework is shown in Figure 4.

Leadership and commitment lie at the heart of the framework and drive the process.

This can be further illustrated by considering how in practice the framework will operate in an organisation. In a typical large company, the board will set the company policy and this will flow down for action to operational executives at a divisional level and then to local site management for implementation. Risk oversight will often be the responsibility of the Risk or Audit Committee, reporting to the board, with decisions flowing down through the Risk function, through Risk Champions at a divisional level and then to local specialists. Alongside this, there will be documentation and toolkits to inform people at every level of the organisation.

The risk framework should be developed as an integral element of the other organisational procedures and processes to bring maximum efficiency and effectiveness.

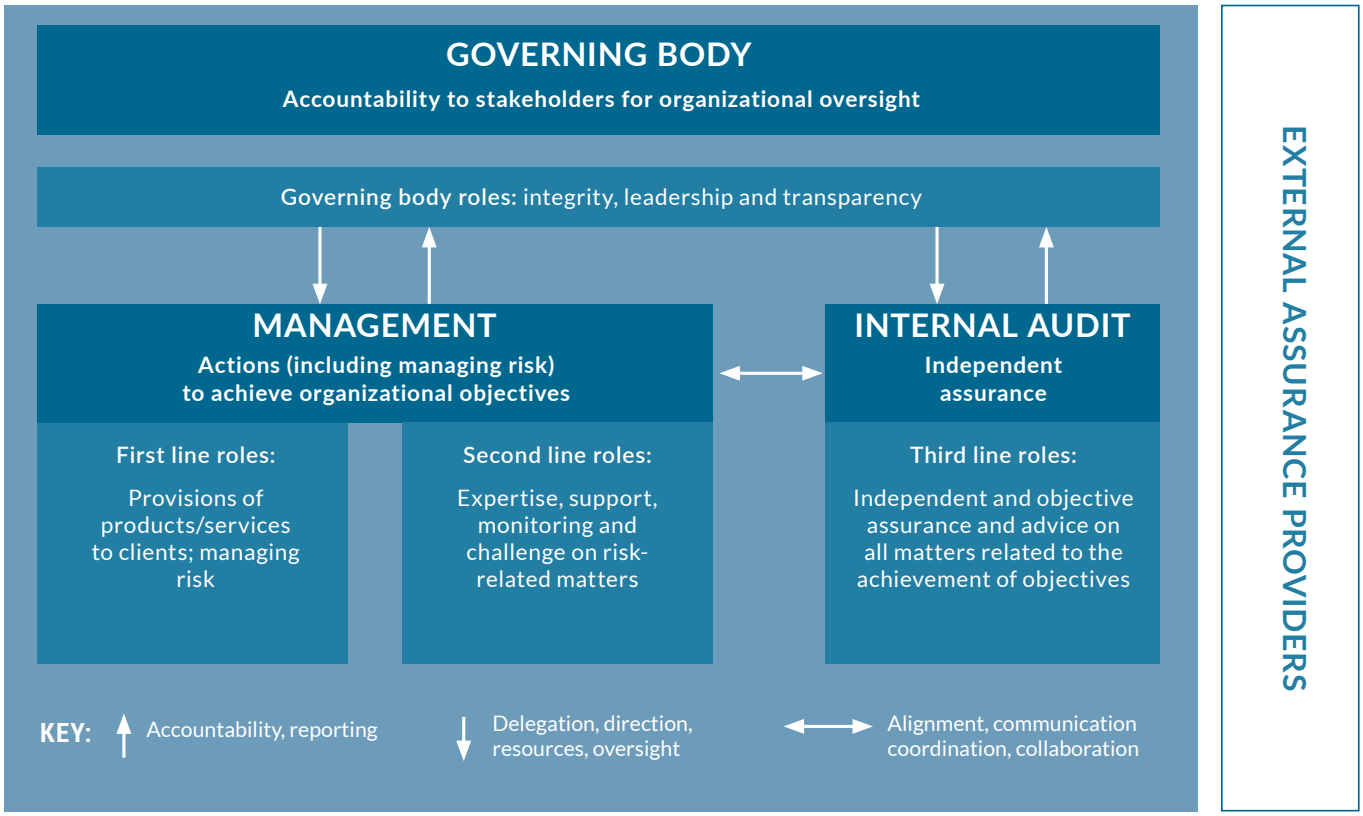
4.3 The three lines (of defence) model

Organisations differ in their distribution of responsibilities.

In a version of the model published by the Institute of Internal Audit (IIA) (see Figure 5), the following six Principles were introduced:

FIGURE 5

The IIA version of the three lines (of defence) model - IIA 2020



www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-model/

Principle 1: Governance
Principle 2: Governing body roles
Principle 3: Management and first and second line roles
Principle 4: Third line roles
Principle 5: Third line independence
Principle 6: Creating and protecting value

The following high-level roles serve to amplify the Principles:

The governing body accepts accountability to stakeholders for oversight of the organisation. It engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives. The body should ensure a culture promoting ethical behaviour and accountability. It should establish structures and processes for governance, including subcommittees, where considered appropriate for Risk and Audit committees. The body delegates responsibility and provides resources to management for achieving the objectives of the organisation. It should determine the appetite for risk, and establish and oversee independent risk management and internal control functions, whilst overseeing compliance with legal, regulatory and ethical expectations.

1. **The first line** leads and directs actions, including managing risk and application of resources to achieve the objectives of the organisation. It maintains a continuous dialogue with the governing body, and reports on planned, actual and expected outcomes linked to the objectives of the organisation. This line establishes and maintains appropriate structures and processes for the management of risk and internal control, and ensures compliance with legal, regulatory and ethical expectations.

2. **The second line** provides expertise, support, monitoring and challenge related to the management of risk, including the development, implementation and continuous improvement of the risk management framework and processes, reporting on the achievement of risk management objectives, such as compliance with laws, regulations and acceptable ethical behaviour, internal control, information and technology security, sustainability and quality assurance. It provides information, analysis and reports on the adequacy and effectiveness of risk management and internal control.

3. **The third line** communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management, including internal control, to support the achievement of organisational objectives and to promote and facilitate continuous improvement. It reports impairments to independence and objectivity to the governing body and implements safeguards as required.

External assurance providers provide assurance of legislative and regulatory compliance, satisfy requests by management and the governing body to complement internal sources of assurance, and provide specialist support to the Second line and Governing Body through an independent assessment of the framework, assistance in designing and implementing the framework, or specialist analysis.

4.4 What the Financial Reporting Council requires

The Financial Reporting Council (FRC) regulates auditors, accountants, and actuaries, and sets the UK's Corporate Governance Code. Their work is aimed at investors and others who rely on company reports and quality risk management. The FRC requires a board to establish an audit committee of independent directors. The committee should have recent financial experience and competence relevant to the sector in which it operates. In addition to finance-related roles and responsibilities, the board is charged with reviewing company internal financial controls and internal control and risk management systems, unless as regards risk, this is expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself.

The FRC's 2024 revision of the Code is intended to provide a stronger basis for companies to evidence the effectiveness of their internal controls, thereby enhancing transparency and investor confidence. The board is required to take a stronger role in overseeing risk management and internal controls and to review the effectiveness of both at least annually. The 2024 Code will apply to financial years beginning on or after 1 January 2025. The 2018 Code remains in place until this time. The Code is supported by Guidance which provides further useful information but this does not form part of the Code.

Underpinning the 2024 Code is the responsibility of boards to establish a company culture based on integrity, openness, and diversity, and which is responsive to the views of investors and wider stakeholders.

5. LEADERSHIP COMMITMENT AND CULTURE, ROLES AND RESPONSIBILITIES

It is widely accepted that the commitment demonstrated by those in control of an organisation can make a significant difference in the level of organisational achievement.

This applies equally to risk management: strong leadership and a positive culture are vital to the successful achievement of risk management objectives. To be successful, risk management must be embedded within the culture of an organisation and this requires that all those working within and on behalf of an organisation understand how their own roles and responsibilities help the organisation survive and thrive.

5.1 Risk culture explained

Risk culture is a term describing the values, beliefs, knowledge and understanding about risk shared by a group of people with a common purpose. This applies whether the organisations are private companies, public bodies or not-for-profits, and wherever they are in the world.

An effective risk culture is one that enables and rewards individuals and groups for taking the right risks in an informed manner. To achieve success, the risk culture would include:

1. A distinct and consistent tone from the top from the board and senior management in respect of risk-taking and risk avoidance
2. A commitment to ethical principles and the consideration of wider stakeholder positions in decision-making. Examples of poor behaviour include bullying or inappropriate sales incentives
3. A common acceptance across the organisation of risk management, including clear accountability for and ownership of specific risks and risk areas
4. Transparent and timely risk information flowing up and down the organisation, with adverse news rapidly communicated without fear of blame
5. Actively seeking to learn from mistakes and near misses by encouragement of risk event reporting and whistle-blowing
6. Ensuring that no process or activity is too large, complex or obscure for the risk not to be readily understood
7. Appropriate risk-taking behaviours rewarded and encouraged, and inappropriate risk-taking behaviours challenged and sanctioned
8. Risk management skills and knowledge valued, encouraged and developed
9. Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged
10. Appropriate employee engagement to ensure focus on both business and personal needs.

5.2 Illustrating the impact of poor culture

Risk culture is organisational culture viewed through a risk lens, and acts as a vital bridge between the risk appetite of the organisation and the overall culture and management systems. The prevailing risk culture will orient employees towards organisational risk and their own risk responsibilities, and in particular their decisions on risk-taking. Risk managers therefore must integrate cultural

management into the overall risk management framework. Problems with business and risk culture are frequently at the heart of organisational scandals and collapses. The following demonstrate real-life examples of poor business culture leading to corporate disaster:

VW and car emissions 2015: VW has admitted lying to markets and government officials about vehicle mileage and emissions. Investors in Both investors and customers have suffered. Reports indicate that the leadership of VW had such aggressive goals that technical teams could not achieve them. Rather than have the courage to speak up, employees chose the 'easier' route of dishonesty.

5.3 Communicating roles and responsibilities

Top management in an organisation it accountable for achievement of the strategic objectives and business performance. Their obligation to shareholders and other stakeholders requires it also to be responsible for the risk management policy in the organisation. Therefore, the board (or equivalent) should demonstrate its commitment to risk management by:

- Recognising that it is ultimately accountable
- Defining roles, responsibilities and accountability for managing and reporting on risk throughout the organisation
- Setting risk management objectives to support and achieve the organisation's risk appetite
- Setting risk management objectives to recognise risk in decision-making
- Providing achievable risk management goals
- Communicating the commitment across the organisation
- Providing the infrastructure to support the successful risk culture elements identified above.

Everyone across the organisation has an active role to play in risk management. Senior management, line managers, supervisors and individuals need to understand their role and how important it is to the success of the organisation.

The following should be regarded as minimum responsibilities for everyone in the organisation:

- Be aware of the risks that relate to their roles and activities
- Continuously improve their management of risk
- Provide information to inform the risk management process, such as information that helps identify ... risks, and [supports] the effectiveness of controls
- Implement controls as part of day-to-day duties
- Report ineffective and/or inefficient controls.

Everyone in the organisation should be aware of their role in the risk management strategy of the organisation, and personal objectives should be included within their own job roles to reflect this.

6. ARTICULATING RISK IN THE ORGANISATION

As outlined in section 4 of this guide, there is an increased emphasis on the role of the board in determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives.

6.1 Defining risk criteria for consequence

In order to consider different types of risks, an organisation should first define the risk criteria used when evaluating the risks. Risk criteria are the reference points which allow different risks to be evaluated in a manner that enables them to be compared and prioritised.

The matrix overleaf shows an example of risk criteria for consequence for a large business. The matrix illustrates five different types of consequence (organisational objectives, people, financial loss, reputation and environmental damage) and five risk categories (insignificant, minor, significant, major and catastrophic). The five risk categories are also ranked in increasing severity from 1 (lowest) to 5 (highest). In this way, it is possible for the organisation to undertake an assessment across diverse risks and be able to express them in a manner that allows comparison. Financial loss is often best considered as a percentage of turnover or profit as this is then easier to apply to a range of organisations of different sizes.

The key is to define the risk criteria in a way that is appropriate to the business.

TABLE 1

Examples of risk assessment criteria for consequence

Score Consequence Type	1 Insignificant	2 Minor	3 Significant	4 Major	5 Catastrophic
Organisational Objectives	Internal information failure	Project failures in one division	Divisional objectives not met	Failure to meet one key group objective	Failure to meet key group objectives
People	Minimal harm	Short-term disability	Permanent disability	Single fatality	Multiple fatalities
Financial Loss	Less than £10k loss	£10k - £100k loss	£100k - £1m loss	£1m - £10m loss	> £10m loss
Reputation Damage	Adverse mention in local press	Significant attention from government agencies/regulators	Headlines in national press and television	Headlines in international media, prosecution	Regulator action, prosecution, punitive fines
Environment Damage	Will recover fully in the short term	Will recover fully within 2 years	Short-term change to eco system; good recovery potential	Change in eco system for up to 2 years; reasonable potential for recovery	Long-term damage to eco system; poor potential for recovery

6.2 Defining risk criteria for likelihood

Similarly, it is usual to develop risk assessment criteria for likelihood. This can often present more of a challenge as it is often difficult to obtain accurate information on probability of occurrence.

Table 2 is an example of a matrix for likelihood with criteria expressed as a percentage probability and also in more commonplace language. As in Table 1, the criteria is also expressed as a risk score to facilitate ranking and comparison across different risks.

> *Risk criteria are the terms of reference against which the significance of a risk is evaluated.*
>
> Definition from ISO Guide 73

TABLE 2

Examples of risk assessment criteria for likelihood

Score	Probability of occurrence in next 24 months %	Likelihood expressed in day-to-day language
1	0-10	**Very unlikely:** Only in exceptional circumstances "Never heard of it"
2	10-40	**Low:** Once in 10 years "Heard it has happened"
3	40-60	**Possible:** Once in 5 years "Know it's happened"
4	60-90	**Likely:** Once in a year "Seen it happen"
5	90-100	**Almost Certain:** More than once a year "Happens all the time"

6.3 Using heat maps to display different risks

Comparing the risk criteria makes it possible to assess and compare different risks across the business and provides a common format for articulating risk across the business. In many organisations, it is common to use risk maps to display risks on a grid which combines the risk scores for consequences and likelihood onto one chart. A typical format is shown in Figure 6.

This form of display is often referred to as a heat map or Probability Impact Diagram (PID). In such a map the colours represent the following:

- The green zone includes risks with low consequence and/or likelihood
- The red zone contains high risks which may be catastrophic to the organisation
- The amber zone shows risks falling between the two extremes.

The heat map is perhaps the most common visual tool employed to demonstrate different risks across a business. Different organisations will use a range of different criteria and detail; however, the underlying basis of presentation is often similar.

6.4 Risk appetite

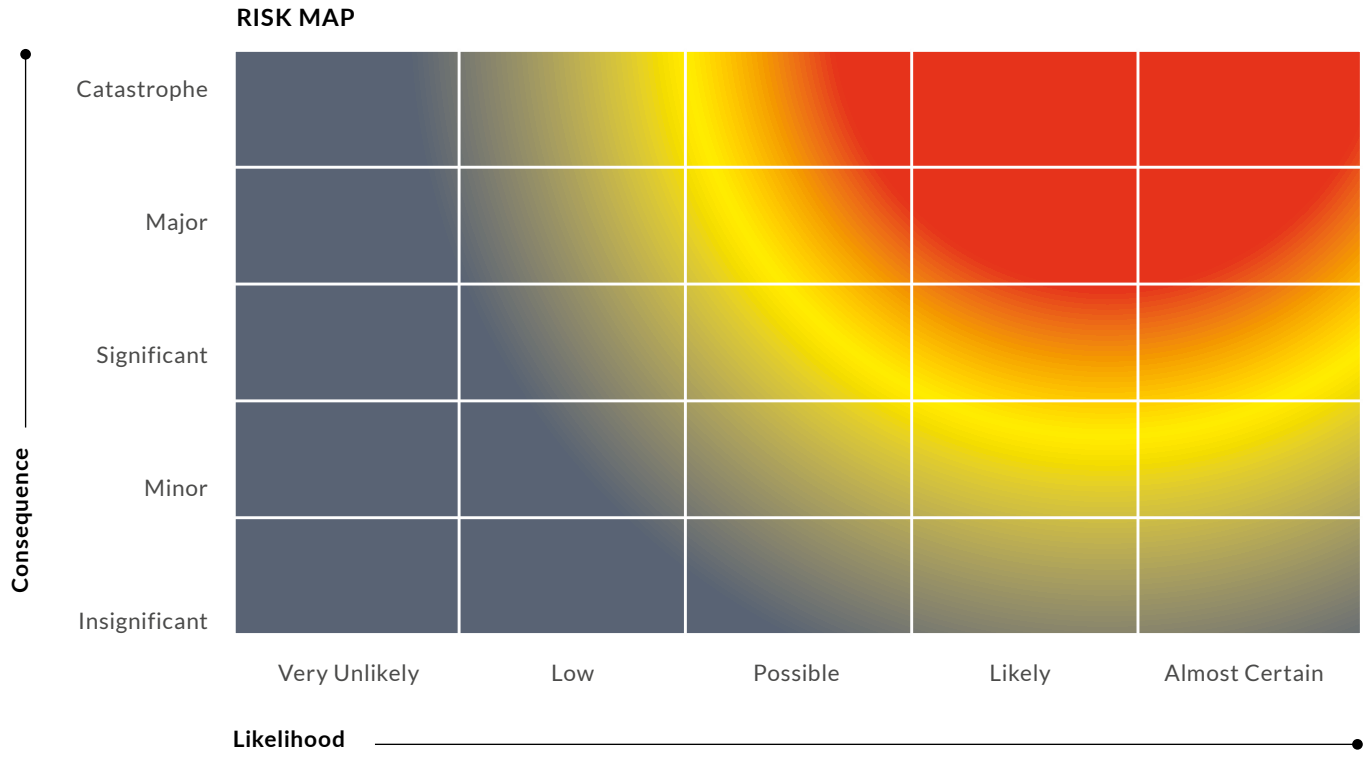
Understanding the comparative effect of different risks and formalising risk appetite is an important exercise for any organisation. Although there are a number of definitions of risk appetite in existence, most view risk appetite as the amount and type of risk exposure, or potential consequence from an event, that an organisation is willing to pursue or retain.

Risk appetite is about understanding the risks associated with the organisation and relating these to possible outcomes. Some organisations actively seek to take risks that others might regard as completely unacceptable. Some organisations might view the primary objective as vital and will accept other risks with adverse outcomes.

The expression 'risk tolerance' is also sometimes used.

FIGURE 6

A typical risk map or heat map



The amount of risk an organisation is willing to accept in pursuit of its strategic, operational, and financial objectives. It reflects the risk management philosophy that a board or equivalent governance body wants the organisation to adopt and, in turn, influences its risk culture, operating style and decision-making".

The risk the organisation is not prepared to take, or the range of variation from Risk Appetite which it is prepared to take".

TABLE 3

Risk appetite for outcome

Outcome	Appetite for Outcome	
	Win at all costs	Ethical play
Cause personal injury to opposition players	Accept	Avoid
Break rules if necessary	Accept	Avoid
Incite supporters to intimidate opposition	Accept	Avoid
Intimidate referee	Accept	Avoid
Play to win	Accept	Accept

As an example, consider a typical football match where both sides are striving to win. Whilst they have the same ultimate objective, some teams might be prepared to go to any lengths to achieve victory, whereas others might only wish to play to win within the spirit and the rules of the game. Table 3 outlines how the appetite for the outcome will be different for each team.

Whilst both teams have the same overall objective, their team philosophy and culture will influence the extent to which their actions are acceptable or not.

6.5 Illustrating risk appetite in business

This simple approach to risk appetite can be developed and applied in complex situations to enable the board or top management of an organisation to establish the guiding principles that allow the organisation to assess and take risk in the appropriate way. Organisations can establish both qualitative and quantitative measures for their risk appetite statements.

Qualitative statements might include the following:

- We have a low appetite for risk
- We have a high appetite for development in emerging markets
- We have no appetite for fraud/ financial crime risk
- We have a zero tolerance for regulatory breaches
- We wish always to avoid negative press coverage
- We will seek to introduce new innovate products in growth markets
- We are committed to protecting the environment.

Such statements demonstrate an organisation's attitude or philosophy towards upside and downside risks, which are difficult to quantify numerically.

Quantitative statements might include the following:

- We will maintain a credit rating of AA
- We will maintain our market share of 40% irrespective of profit margin
- We will maintain a dividend cover of 4x earnings
- We will reduce energy consumption per unit produced by x% in 10 years.

Organisations can utilise other financial performance indicators such as Operating Income, Earnings Per Share, Profit Before Tax and Cashflow within their risk appetite statements.

TABLE 4

Risk appetite for team 'Win at all costs'

Outcome	Low	Medium	High
Cause personal injury			
Break rules if necessary			
Incite supporters to intimidate			
Intimidate referee			
Play to win			

TABLE 5

Risk appetite for team 'Ethical Play'

Outcome	Low	Medium	High
Cause personal injury			
Break rules if necessary			
Incite supporters to intimidate			
Intimidate referee			
Play to win			

7. RISK COMMUNICATION, REPORTING AND MONITORING

7.1 Communicating your risk management programme

Effective communications are an essential element of a successful risk management programme. There is a wide range of internal and external stakeholders, each with different needs and expectations. The communication plan will reflect the nature of the organisation and is likely to include the following elements:

- A succinct policy statement outlining the tone from the board and establishing the risk appetite and supporting the ERM risk processes, in the language of the organisation
- Provision of practical skills, training and knowledge transfer to facilitate successful implementation of the ERM processes across the whole organisation
- Risk owners, appointed to be responsible for identified key risks, should provide regular updates on the actions required and implemented to address those risks
- Provision of regular reports and case studies detailing risk and related issues to enable everyone to understand and learn from internal and external events, including near misses
- New and emerging risks to be subject to monitoring and review.

The Corruption Perceptions Index published by Transparency International ranks countries by their perceived level of corruption.

7.2 Formalising monitoring

The monitoring of risk actions and updating of all elements of the risk process should be undertaken in accordance with the relevant requirements. It should be noted that the ISO standard requires that risk management activities should be traceable, so it is important that this is reflected in the ERM processes and is capable of being audited and validated, if appropriate.

The Dow Jones Sustainability World Index tracks the stock performance of the world's leading companies in terms of economic, environmental and social criteria.

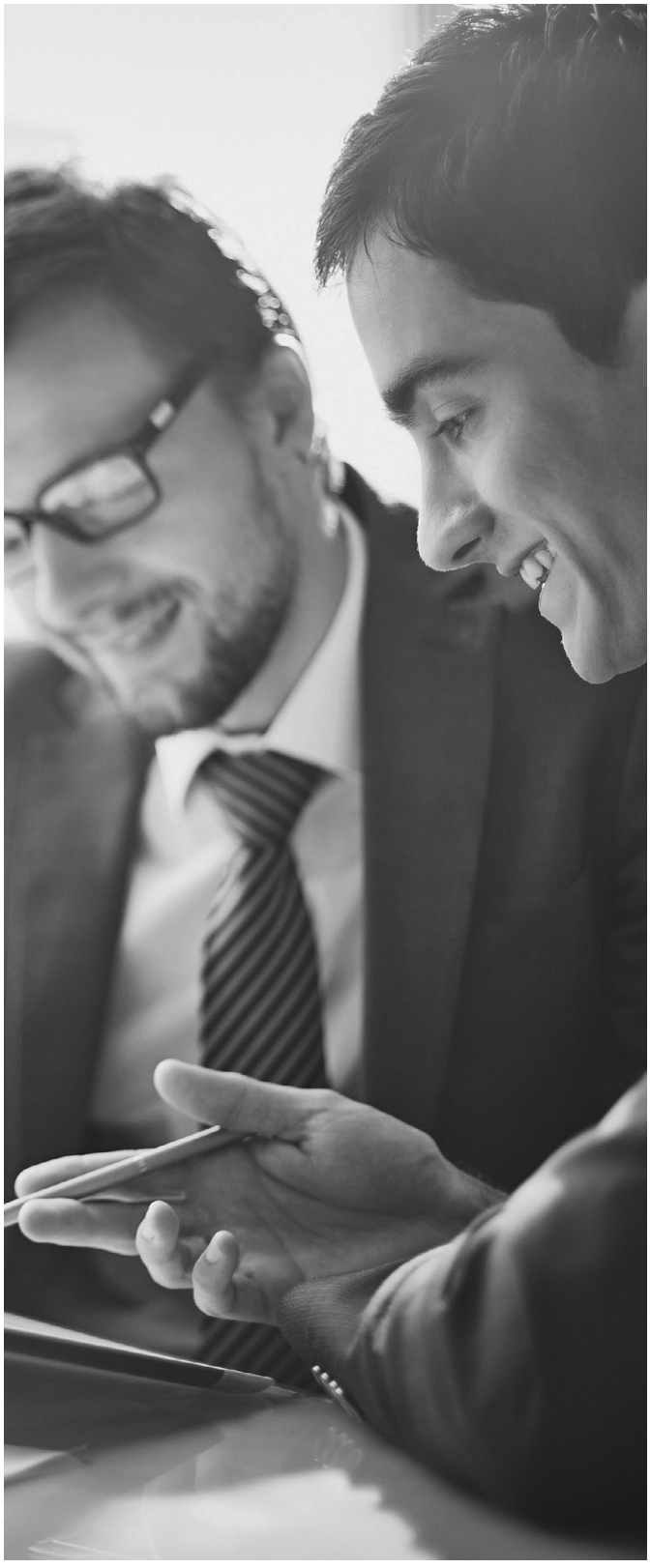
7.3 External reporting

External communication is important for commercial, regulatory and learning purposes. In addition to the FRC reporting requirements referenced earlier in this guide, investors increasingly are seeking reassurance that organisations adhering to risk practices that reflect their investment criteria. Relevant areas for attention include climate change, sustainability, corruption and safety. The indexes issued by Dow Jones on sustainability and by Transparency International on corruption illustrate the importance attached to these issues.

An introduction to the risk management strategy and expectations should be included in staff inductions and

articulated to third-party partners as appropriate. Also learning should be driven not just through the organisation and the supply chain, but more broadly across different organisations so that the experience gained from events can be transferred as far as possible. Some of the most tragic events have occurred through failure to communicate such information both internally and externally.

At the highest level, risks and their management will be reported to shareholders within the organisation's annual report.



"Companies have faced several years of economic and geopolitical turbulence following the pandemic and Russia's invasion of Ukraine. Interest rate rises in response to persistent inflation, the related impact on consumer behaviour, and limited growth remain immediate concerns in many economies. There are also considerable uncertainties surrounding companies" exposures to climate change and their plans for the transition to a low carbon economy.

"This presents a challenging environment for financial reporting as companies need to consider, and communicate to investors, how these issues affect their business, as well as the assumptions underpinning the values of assets and liabilities in their financial statements".

"The development and consolidation of the sustainability reporting ecosystem continues at pace, with the phased introduction of climaterelated disclosures in the UK and a major milestone, the publication of the first International Sustainability Standards Board (ISSB) standards,1 this year, reflecting the demand for investor-focused information in this area".

FRC, Annual Review of Corporate Reporting 2022/23

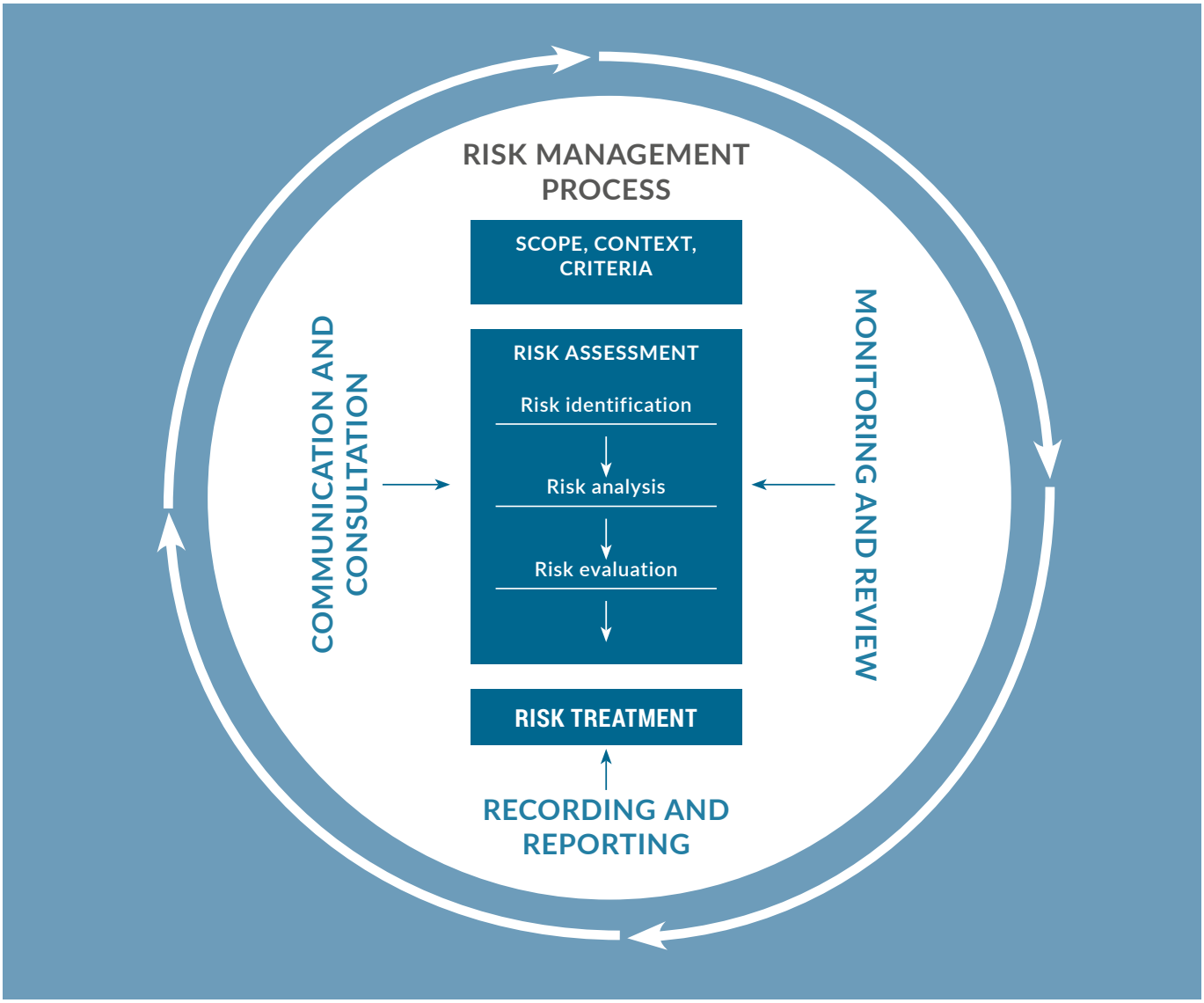
8. RISK PROCESS OVERVIEW

The overall risk process takes account of all the different aspects referred to in this guide and is summarised below.

This process, as illustrated in Figure 7, supports business leaders by using a structured methodology to identify, define and assess risks to their business strategy, financial performance and operational effectiveness. In enabling clear understanding of the most critical risks, it provides a basis for the most cost and time effective allocation of resources to the protection and creation of business value.

FIGURE 7

The risk management Process – ISO 31000:2018



9. BUSINESS CONTINUITY, RESILIENCE AND INSURANCE

A wide range of specialists can be utilised to control risks across different parts of an organisation. These include Legal, Financial, Audit, Security, IT, Quality and Safety to name just a few.

However, now there is increasing focus on bringing these different specialists together within a unified risk strategy for the organisation. This section outlines how business continuity management, organisational resilience and insurance operate as an integral part of an enterprise risk management strategy.

9.1 Business continuity management explained

Business continuity management (BCM) is about identifying those parts of your organisation that you cannot afford to lose and planning how to maintain these should an adverse event occur. International standard ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organisations, regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity.

An effective BCM plan should address the following core elements:

- Emergency response
- Crisis management
- Technology disaster recovery
- Business recovery.

Emergency response – Describes a process at a specific location to safeguard life and to allow initial control of an emergency situation.

Crisis management – Considers the strategic response to issues, including crisis communications (both internal and external), and initial coordination of the business recovery efforts.

IT disaster recovery – Addresses how to recover IT and infrastructure services.

Business recovery – Addresses the phased recovery of business-critical processes.

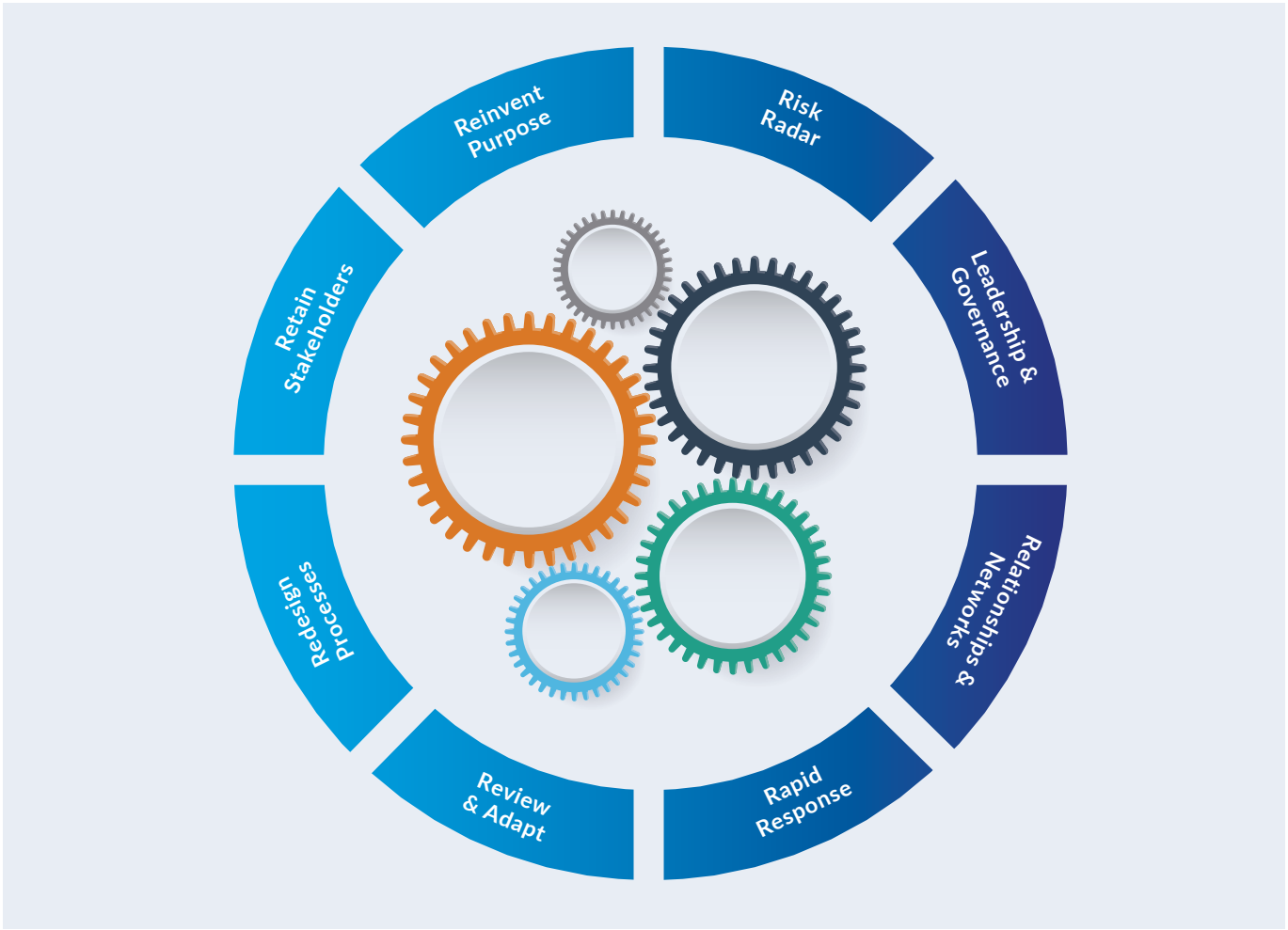
The BCM plan should be developed in conjunction with appropriate internal and external stakeholders to ensure that roles, responsibilities and communication lines are understood and agreed.

9.2 Introducing organisational resilience

International standard ISO 22316: security and resilience - Organizational resilience - Principles and attributes helps to shape what resilience is and what it means to businesses. James Crask, Global Head of Resilience Advisory, Marsh, and Convenor of the ISO working group of experts that developed the standard, says "the standard takes a wide view of the things that can drive resilience in an organisation. The standard emphasises that many of these are behavioural and have historically been overlooked. This is why one of the key principles of the standard is to help them develop a culture that supports resilience."

FIGURE 8

The resilience and transformation model – *Roads to Revolution*, Airmic, 2018



Organisational resilience addresses the effective management of a negative outcome resulting from any risk or potential risk. Resilience encompasses the entire organisation, enabling it to respond quickly and effectively to adverse events. Resilience also encompasses the long-term viability of the business in the context of organisational change.

The intangible nature of resilience means that there is no single correct approach; rather, it depends on the intricacies of each organisation.

There are, however, characteristics of a resilient organisation and, by understanding these, it is possible to determine where organisations are in terms of resilience maturity.

The following capabilities are critical when considering an organisation's level of resilience.

Figure 8 is reproduced from *Roads to Revolution* and illustrates the link between the principles of resilience, business enablers and resilience outcomes.

1. **Risk radars** focused on emerging risks and developments in technology
2. **Resources and assets** flexible and diverse to take full advantage of developments in technology
3. **Relationships and networks** constantly developed and extended

4. **Rapid response capability** supported by excellent communications

5. **Review and adapt mechanisms** an ability to change events to protect and enhance reputation

6. **Redesigned processes** to embrace new technologies and encourage and exploit innovation

7. **Retention of stakeholders** to discuss and share opinions with all interested parties and develop options for digital delivery of benefits identified

8. **Continuous reinvention of purpose** achieved through commitment, capabilities, awareness and the willingness and courage to convert opportunities

9.3 Transferring risk by insurance

All businesses buy insurance. The type and amount of insurance cover purchased will vary according to the risk profile and the risk appetite of the business. In the insurance contract, an insurer promises to pay the insured if one of a series of specified events occurs in the future. Businesses buy insurance to protect their assets and income streams; to protect the assets of directors and officers of the company; to pay compensation to third parties in the event of a claim against the company; and, in certain circumstances, because it is a legal obligation.

Many insurance companies also offer additional services to help reduce the risk of loss and to assist in the response to an adverse event should it occur.

Insurance is an important risk treatment option for an organisation as it allows specified risks to be transferred to another party, the insurance company. The decisions on insurance purchase and the design of the insurance programme, therefore, should be directly linked to the risk management framework and specifically take account of the organisation's risk profile and risk appetite. Moreover, the process for dealing with insurance claims should be directly linked with the BCM and resilience strategies for the organisation to ensure the wider objectives are achieved.

Further to the risk communication, monitoring and reporting principles discussed in section 7, the Insurance Act 2015 places a duty on the insured to make a "fair presentation of the risk" to the insurer. This therefore requires the disclosure of all material circumstances and information to the insurer in a timely manner, based upon the risk management framework.

10. MANAGING INTANGIBLE RISKS

10.1 The increasing value of intangible assets

Managing the risks to intangible assets is a common theme for risk and insurance professionals. Increasingly, risk registers are dominated by external threats to the organisation and focused on protecting assets that are difficult to define and harder to value.

The importance of intangible assets has grown over the last three decades from around 17% of S&P asset value in 1975, to 32% in 1985, to 68% another decade later in 1985, to ultimately today exceeding 85%. This has been closely linked to the changes in the economic landscape, with technology-driven service companies becoming increasingly prominent, while industries famous for their holdings of property, machinery and other tangible assets have slowly lost position. American tech companies flew high before the coronavirus pandemic. The upheaval of the pandemic has lifted them to new heights, putting the industry in a position to dominate business in a way unseen since the days of railroads. The stocks of Apple, Amazon, Alphabet, Microsoft and Facebook, the five largest publicly traded companies in US, now constitute 20% of the stock market's total worth, a level not seen from a single industry in at least 70 years.

The focus of risk professionals has consequently shifted towards protecting intangible assets, reflecting the transformation within their organisations.

As the post coronavirus world drives anxiety levels to new highs, businesses are also more prone to making reputational mistakes that can leave lasting impact in the way their customers, employees, distribution partners and other stakeholders perceive the character of their business. This is particularly important as various activist events keep pushing the corporate environment from traditional shareholder capitalism to stakeholder capitalism. The recent 'Black Lives Matter' protests have demonstrated the power of social activism and the need for businesses to embrace the changing social norms.

"We could well see activist movements growing in the next few years to address some of the well-known global challenges, ranging from climate change to income inequality. Risk owners in businesses across all industries will have to be alive to these changes to make sure they have the right tools to keep enhancing their corporate value. They will have to rethink the optimal ways of using risk management practices to build internal resilience and become proficient at safeguarding their existing and new intangible assets."

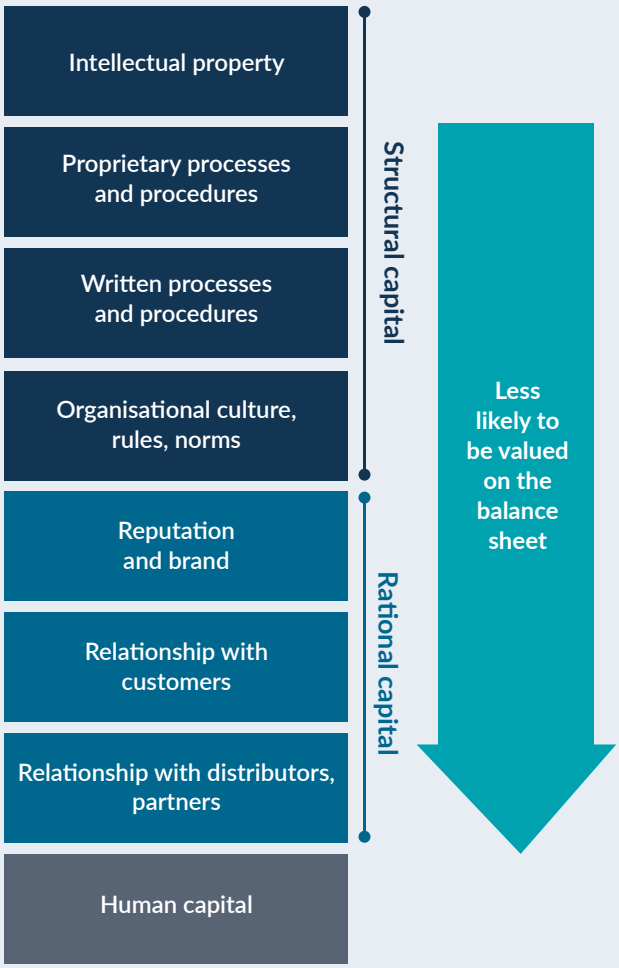
Protecting Intangible assets: preparing for a new reality – Lloyd's and KPMG 2020

10.2 A framework for intangible risks

Just as we manage the impact of physical risks (e.g. fire and flood) of tangible assets (e.g. buildings and machinery),

FIGURE 9

Protecting Intangible assets: preparing for a new reality – Lloyd's and KPMG 2020



"In order to remain resilient and competitive, organisations across all industries must be proactive in finding new ways to enhance their business practices to protect these assets, and this will require a new way of thinking and acting."

Paul Merrey
Partners KPMG

organisations also need to develop similar risk frameworks to manage the risks associated with intangible assets.

Steps to take:

- Assess the total intangible value of the organisation, including 'hidden' intangible assets that are valuable but not visible on the balance sheet (see FIGURE 9)
- Collaborate with finance and corporate communications teams to assess whether other assets should be included and to help validate the assessment
- Form interdepartmental working groups to assess the relative value of different types of intangible assets in the organisation
- With the same working groups, decide which types of intangible assets are most important to the organisation and critical to the achievement of organisational strategy and objectives
- Perform 'war-gaming' exercises and 'horizon scanning' with the working groups and top management to test organisational resilience to risks that may impact intangible assets
- Assess which risks are potential areas of material weakness and opportunity
- Design triggers to create a dashboard to provide warnings when threats start to emerge and monitor these through clearly assigned risk owners
- Determine if there are risks the organisation cannot manage within the organisation and evaluate what financial or other solutions may be available.

TAKEAWAYS

1. **The type of intangible assets organisations have to protect and the risks impacting these assets are very diverse – each risk will require unique preventative and responsive measures.**
2. **Consider the connection between physical and intangible risks – the cumulative and cascading financial vulnerabilities caused by an inherent weakness in the inter-connected architecture of today's business-to-business relationships can allow a single negative event to exponentially spread disruption and paralysis, and economic damage within and between organisations.**
3. **Include near misses in risk databases – organisations suffer far more near misses than actual risk events – these can provide a wealth of information to inform the risk management.**
4. **Organisations must think beyond financial implications of risks to achieve long-term success – many intangible risks can be hidden from financial view.**
5. **Intangible risk frameworks can be supported by external sources of information often accessible without charge – check what sources of information are used by the insurance companies, insurance brokers and other external advisors that the organisation deals with, and other functions in the organisation.**
6. **Intangible risks can be less predictable than physical risks so consider how often intangible risk assessments should be conducted – this will vary by risk and connected risks according to the internal and external context of the organisation.**
7. **Traditional risk management tools and techniques may be less effective when dealing with intangible risks – tools and techniques are addressed at section 12.**
8. **Record which assets and risks are currently financially transferable or insurable – this can help focus the attention of top management on risks that need greater attention in terms of non-financial risk controls.**
9. **Remain agile and adaptive to change – intangible risks can typically change profile and direction at high velocity.**

11. MANAGING EMERGING RISKS

11.1 Emerging risks – the context

Boards confirm that one of their biggest needs for managing their risk responsibilities is timely and accurate information. Risk professionals cannot and should not try to predict the future, but the tools and techniques used for managing traditional risks may not be effective for managing risks that are emerging and evolving. These risks typically emit low signals on the risk radar, data about them can be sparse and unreliable; therefore, these risks are often therefore, these risks are often hard to detect and their trajectories hard to assess. New tools and techniques must be developed if risk professionals are to rise to the emerging risks challenge.

> *"Intelligence is the ability to adapt to change."*
>
> Stephen Hawking

11.2 Emerging risks defined

In simple terms, emerging risks are risks that are new or changing in significance. Their possible trajectories exhibit high levels of uncertainty. Similarly, they often lead to multiple knock-on consequences. New means that the risk did not previously exist. New risks often arise from scientific developments and transformational technologies, societal and attitudinal shifts, or the introduction of unfamiliar or revised processes. Changing means that the profile or shape of a 'known' risk is being aggravated by changing external conditions (such as higher taxes on sugar in food and drink products, tightening environmental regulation or a trade war) or has become more consequential due to internal factors (more aggressive strategic ambitions, lower institutional resilience due to cost-cutting measures or challenges in embedding new values and behaviours to reflect repurposing initiatives).

However, there is no single definition of an emerging risk, but organisations need to clearly define what they mean, ensure this is understood as part of their risk language, and communicate this internally and externally.

11.3 Assessing emerging risk

In practice, although a robust discussion of principal risks would also likely capture emerging risks, few organisations currently have a formal process for identifying emerging risks or can specify how they apply this in practice. While the approach for emerging risks should be analytical, it should also be creative and pragmatic, reflecting the complexity of uncertainties to secure buy-in and actionable results. Often there are no 'right' answers.

Emerging risk assessment should focus on plausibility and impact. Probability is notoriously challenging to assess for emerging risks and creating angst over this can act as a distraction. Formal assessments and heat maps should be exchanged for structured, creative discussions across business units and functions that bring different perspectives to bear on the topic and seek to strip away unhelpful biases. This will help organisations to better appreciate potential risk trajectories, where the organisation might be touched and the knock-on consequences.

The key is to ensure that high impact, low probability risks are not overlooked when profiling top risks and issues.

Covid-19

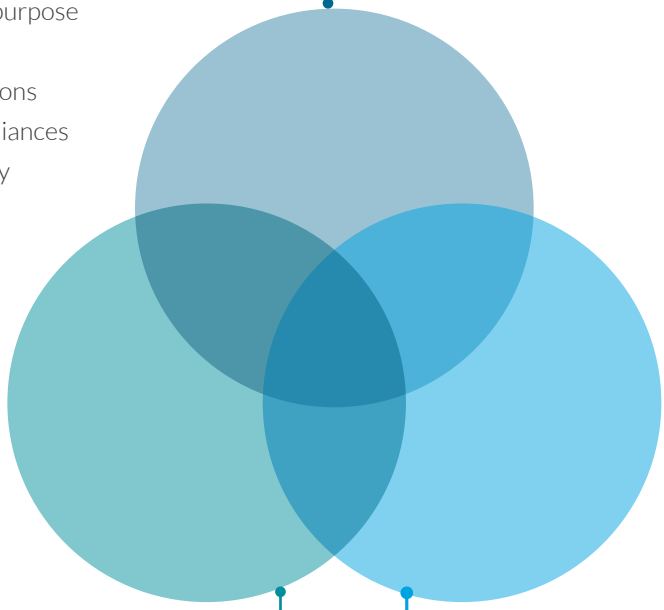
For over fifteen years before the Covid-19 pandemic, the World Economic Forum's Global Risks Report had been warning the world about the dangers of pandemics. In 2020, we saw the effects of ignoring preparation and ignoring High Impact, Low Probability risks.

FIGURE 10

Response options for emerging risks – Emerging Risks Airmic 2019

STRATEGY

- Rethink strategic purpose
- Align products and processes with purpose
- Align culture and talent with purpose
- Change investment allocation
- Make divestitures or acquisitions
- Develop joint ventures and alliances
- Build know-how and capability
- Embed flexibility and agility
- Adopt the Airmic Resilience and Transformation Model



OPERATIONS

- Tighten business controls and limits
- Undertake public affairs and public relations campaigns
- Respond to a shift in the supply chain curve
- Strengthen Environmental, Social and Governance capabilities
- Adopt new technologies to achieve digital transformation

FINANCE

- Flex risk appetite
- Reinforce financial buffers
- Increase risk transfer
- Boost hedging
- Reduce cost

11.4 The value of scenarios

Airmic members report that risk conversations often take place in silos and that the integration of output and actions could be improved. Scenarios are a good way of making emerging risks tangible, with a view to delineating or calculating the immediate and longer-term impacts on strategic, tactical and operational targets. They can, moreover, capture attention, initiating discussion about mitigation measures. Facilitators should be unafraid to have the assumptions of the business challenged, creating space to 'think the unthinkable' and 'speak the unspeakable'. This can help surface and resolve conflicts between commercial ambitions and corporate risk appetite.

11.5 The importance of connected risks

It is crucial to understand the interconnections between risks that can be influenced by the same external and internal factors, and that can also influence one another. Based on discussions with Airmic members, there is a tendency for organisations to manage risk in business silos and for senior leaders to play down emerging risks until they are on the risk register. Most resource assigned to managing risk continues to be focused on near-time, downside risks, rather than risks further out on the horizon, which may present opportunities for future value creation. Coupled with the absence of useful data sets from which to draw conclusions, this often means that the consideration of emerging risks is relegated to the back seat.

As the complexity of the world increases and the pace of change heats up, managing emerging risk cannot be a strategic afterthought. A time lag can open up when the external and internal context of an organisation moves faster than the organisation, creating a gap between the reality and the perception of risk. An assessment of these risks should be part of the strategic planning process and contribute to the strategy context-setting process. The frequency of risk assessment and analysis should be a function of how fast risks are emerging and the level of their materiality, rather than being determined by traditional institutional administrative cycles.

TAKEAWAYS

1. Is there a clear definition of emerging risks in your organisation and is this well understood and communicated?
2. Is the assessment of emerging risks part of the overall risk management system for your organisation?
3. Is consideration of emerging risks built into strategic planning and major investment decisions sufficiently early and sufficiently well?
4. Are you comfortable with the oversight arrangements for emerging risks?
5. Is there a consistent risk reporting methodology across your organisation using key metrics that can be aggregated?
6. Is there an arrangement for risk communication and reporting to ensure that your board is sufficiently engaged on emerging risk issues?
7. Is your organisation's decision-making capacity adequate should there be a significant change in the risk context, internally or externally?
8. Is challenge and debate encouraged with respect to risk-weighted decision-making for strategy, tactics and operations?
9. Is there a process for recording, analysing and discussing incidents and near-miss events to encourage a culture of continuous learning?
10. Is there a preparedness by senior post-holders and business partners to admit mistakes, biases and gaps in their knowledge?
11. Is the use of risk-based objectives part of the personal evaluation, development and structured learning of all the workforce?
12. Has the crisis management programme been calibrated to reflect the emerging risk universe and the different characteristics of emerging risks response?

12. RISK MANAGEMENT ASSESSMENT AND ANALYSIS, TECHNIQUES, METHODS AND TOOLS

This section provides an overview of the subject and signposts for further learning – it is not intended to provide a comprehensive study of all techniques, methods and tools.

12.1 Techniques and methods

Some distinguish between techniques and methods, but for the purpose of this guide they are interchangeable expressions.

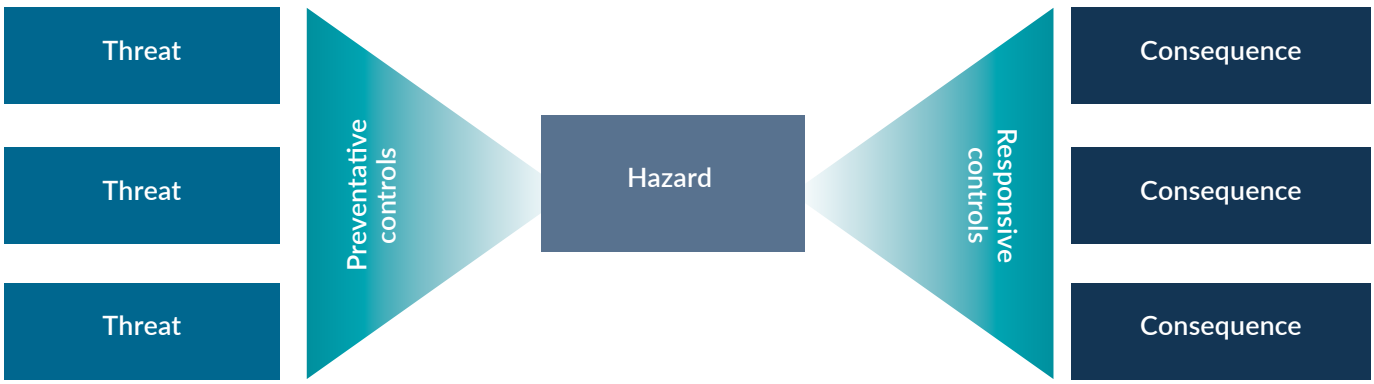
Business studies, surveys and benchmarking reports: There is a significant choice of reports available, generally at no charge. Define the criteria required, for example, by geography, sector or subject and then search online. The Airmic Library is a great place to start. Search other functions within the organisation, including internal audit, corporate communications and human resources, as well as 'affiliated' risk functions such as insurance, health and safety, security, information security and business continuity.

Staff surveys: Surveys of an organisation's own people can be a simple and useful way of gathering information from across an organisation. These surveys can also concurrently be used to embed risk management communications.

Brainstorming: Brainstorming is a group creativity technique. It involves a group of people meeting to generate new ideas and solutions about a specific issue or challenge. People are able to think more freely in an informal gathering and they are more likely to suggest ideas spontaneously. All the ideas are noted down without criticism and after the brainstorming session, the ideas are evaluated.

Bow ties: The bow tie is a risk assessment method that can be used to demonstrate causal relationships and provide a visual summary of risk scenarios. The bow tie can be overlaid with control measures and integrated with semi-quantitative analysis techniques such as Layers of Protection Analysis, which is typically used in process industries where risk controls are developed as layers of defence that are related to, but operate independently from, one another. First developed five decades ago in the oil industry, bow ties are now used in many other sectors, including aviation, mining, maritime, chemical and health care.

Root cause analysis: Often root cause analysis is used after a problem has already come up. It seeks to address causes rather than symptoms. But it can be applied to assessing risk



by going through the goals of any analysis, that asks: What happened? How did it happen? Why did it happen? Once those questions are addressed, develop a plan of action to prevent it from happening again.

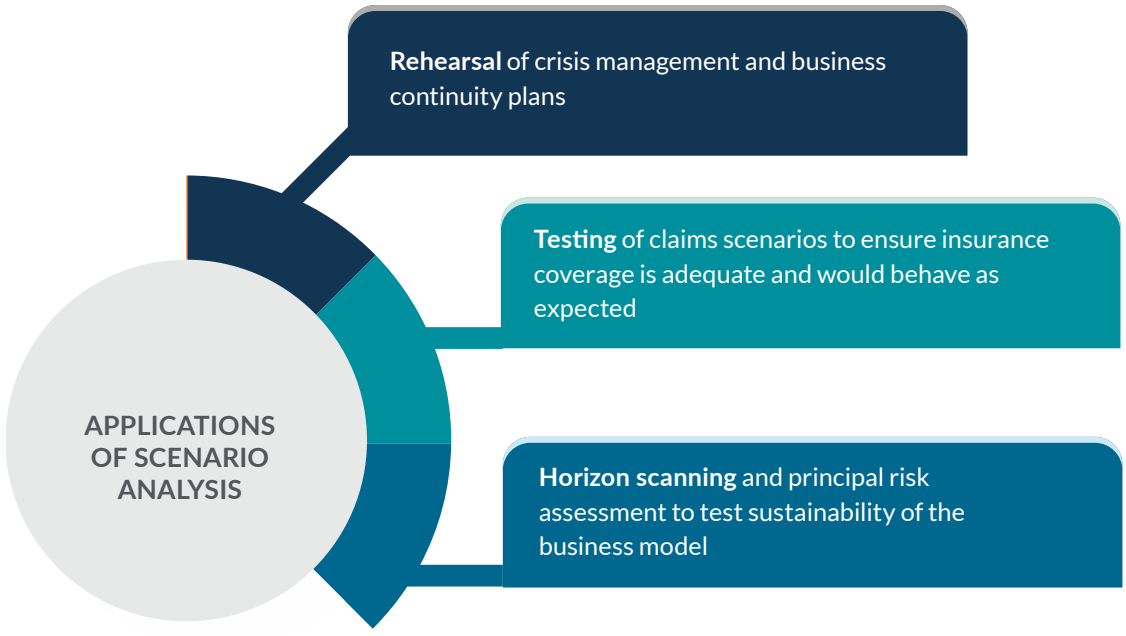
SWOT: SWOT, or strengths, weaknesses, opportunities, threats, is another tool to help with identifying risks. To apply this tool, go through the acronym. Begin with strengths and determine what those are in relation to the project (though this can work on an organisation level, too). Next, list the weaknesses or things that could be improved or are missing from the project. This is where the likelihood of negative risk will raise its head, while positive risk comes from the identification of strengths. Opportunities are another way of referring to positive risks and threats are negative risks. When collecting SWOT, illustrate your findings in a four-square grid. The top of the square has strengths to the left and weaknesses to the right. The bottom of the square has opportunities to the left and threats to the right. The contents of left-hand side is helpful to achieving the objective of the project and those on the right-hand side are harmful to achieving the objective of the project. This allows for analysis and cross-reference.

Futures, Foresight and Horizon Scanning: Futures is a structured approach to exploring what is possible in the future and what is preferable. It typically involves identifying areas of uncertainty, underlying drivers, opportunities and challenges. Foresight refers to the process of conducting Futures work and what you get from it. Horizon Scanning is a specific systematic technique for looking ahead. Its focus is the future rather than the present and its purpose is to identify the strategic issues that will be important. Mostly, these will be different from the issues that are important today.

The 'Three Horizon Model' is a mature and respected technique. Horizon 1 issues are strategically important now. They are visible and well understood, and are generally the issues organisations are already responding

FIGURE 11

Applications of scenario analysis



to. Horizon 2 issues may not be apparent yet, but many of the key trends and factors, the change drivers, that will define it are already in play. Horizon 3 challenges will emerge, but the change drivers are difficult to see in the present. It is not clear how these factors will develop, how they will interact or whether they will create opportunities or threats in the future. The objective is to identify and track the drivers that will shape the future as doing so allows organisations to develop foresight about the strategic challenges and choices they might face in the long term and what kind of interventions might be required to sustain success. The main focus of this process is therefore the mid to long term. The UK Government Futures Toolkit provides further information is a widely respected: The Futures Toolkit*.

Scenario analysis: Scenarios are not risks. Scenario analysis is the exercise of considering unexpected events (sometimes called 'alternative worlds'), occurrences and change by asking the questions 'what might happen?' and 'what could we do?' It is an important part of an organisation's risk management system, and involves understanding the extreme but plausible events, and tests the efficiency of the controls already in place by highlighting unexpected risks and opportunities. It can be used to test the operational, tactical and strategic plans and activities within the organisation and how they fit together. It does not try to show an exact picture of the future but, instead, presents several alternative future developments and helps in the creation of a scope of possible future outcomes and the development of paths leading to these outcomes.

Scenario analysis is not based on extrapolation of the past or the extension of past trends, it does not rely on historical data and does not expect past observations to remain valid in the future. To avoid confusion, organisations should create separate but linked scenario and risk registers.

Organisations will have their own definitions of scenarios, which can range from simple single-factor events, e.g. a retailer asking itself what would happen if there were a major fire at a warehouse, to more complex multi-factor future events involving an extensive chain of events, e.g. an oil company asking itself how technology will improve energy efficiency and subsequently change the oil demand. Single-factor scenarios are more useful for risk management where understanding impact and probability is key. The more complicated scenarios are more typically used to develop strategy by considering the business environment in the future and informing long-term decisions affecting research and development, marketing, etc.

Risk gamification: The idea behind gamification is to influence how people behave and what they do by tapping into their innate desire to play games. It's about making things fun – but more than that, it's about understanding what really motivates people and then using a variety of techniques to inspire them to perform desired behaviours. As a bonus, the desired behaviours that users perform are recordable and when there is data, that creates an opportunity to act on it.

Headline news and fake news scenario games: Headlines generated by newspapers, television or online, including social media posts, can change stock prices – even if the headline story is incorrect or misleading. It's interesting to note that risk connected to the headlines feared the most often don't feature in many risk registers. Thinking about headlines can create a simple exercise for top management to ensure its focus is on the issues and risks that really matter the most and to challenge the status quo and 'comfort' of risks listed neatly in a risk register which create a false impression of compliance and control.

War gaming, simulation and modelling: War gaming can help organisations to consider crisis scenarios, and experience and manage the reality of these. War gaming is a rigorous analytic process that enhances risk-informed decision-making through immersive experiential learning. Plausible, interactive scenarios bring diverse stakeholders together to challenge biases and assumptions, identify critical gaps and vulnerabilities, and provide insights into emerging threats and opportunities. Players are encouraged to ask 'so what?' or 'what if?' and allowed to experience failure in pursuit of these insights, all without facing real-world reputational, organisational and financial risk. Risk modelling and simulation leverage quantitative and

qualitative models to identify, assess and prioritize risks to populations, missions, programmes and operations. Modelling approaches include system dynamics modeling, agent-based modelling, discrete event process modelling, event-based scenario analysis, and machine learning for analysis of unstructured data.

Examples as the basis of war gaming exercises include:

Cyber-attack: where country, sector and organisation stakeholders need to understand the potential impacts of an attack, and the pre and post event practices to mitigate associated risks.

Physical infrastructure construction: using an immersive scenario that includes a dynamic and free-thinking adversary, with capabilities greater than prevailing biases and assumptions allow, organisations could be forced to confront undesirable and unintended consequences, yielding insights that can enable better preparation and anticipation of future crises and risks.

Pandemic: an effective tool for assessing immediate crisis response capabilities. As organisations have experienced throughout the current Covid-19 environment, it's a response with clear leadership and agility that has been a winning formula in maintaining focus in the face of deteriorating conditions and has demonstrated an organisation's resilience. It is imperative to test and stress an organisation's response and continuity plans during a war game.

12.2 Tools

Risk assessment templates: Templates can provide useful checklists to support the process of assessing risks. These can be especially useful when assessing risks that have legal or regulatory requirements such as health and safety in the workplace, information security and compliance with certified standards of performance. Some suppliers and customers may impose risk management requirements and these can be converted into a checklist to ensure compliance. Care must be taken to use risk assessment templates to support and not replace an effective and efficient enterprise-wide risk assessment process.

Risk registers: A risk register is a repository for risk information to meet organisational, legal, regulatory and stakeholder needs. A register will include risks identified with information about each entry, e.g. the nature of the risk, reference and owner, and mitigation measures. Some organisations also use risk registers to record near-miss risk events and examples of where risks are connected or aggregated. Risk information may be recorded before and after risk the effect of risk mitigation measures to provide gross and net gross and net reports of risk.

Risk management information systems (RMIS): A risk management information system (RMIS) or governance, risk management and compliance (GRC) system is an information system that assists in consolidating risk values, insured and non-insured losses, exposure information and details of insurance covers to provide tracking to support risk management reporting capabilities and the monitoring and control of the overall cost of risk. Top benefits reported by users of these systems include:

1. Spend less time consolidating data, more time analysing it
2. Facilitate sharing of information
3. Harmonise practices and reporting
4. Facilitate cross-departmental analysis and avoid silos
5. Optimise the sharing of risk management best practices
6. Visualise real-time data
7. Data reliability
8. Secure sensitive information
9. Be compliant with laws and regulations
10. Optimise transfer to insurance

The most common RMIS modules that are requested when selecting a software solution for risk management are:

1. Certificates of insurance
2. Claims administration
3. Claims management
4. Cost allocations
5. Exposure management
6. Incident management
7. Policy management
8. Root cause analysis

Source: Risk Panorama annual report 2019 - AMRAE, the French risk management association

Risk maturity models: In evaluating the effectiveness of the risk management frameworks, risk management maturity models rate the level of risk maturity across agreed risk areas such as risk context, risk culture, risk identification, risk assessment, risk treatment, communication and reporting, and through to five or seven based on benchmark information from the database created from user data. However, it is important that when using these tools that organisation as a first step, consider their desired level of risk maturity in line with their risk appetite, and then use the tool to assess their performance against this.

13. CONTINUOUS IMPROVEMENT

The enterprise risk management process must not become dormant and should be updated and improved to help the organisation achieve its changing objectives.

Having an agile risk management framework that can be relatively easily adapted is therefore beneficial. Change is inevitable and it is important that the risk framework reflects the structure of the organisation and is intuitive to use to ensure effectiveness across the organisation. The framework will be reviewed in conjunction with other critical business processes on a regular, perhaps annual, basis.

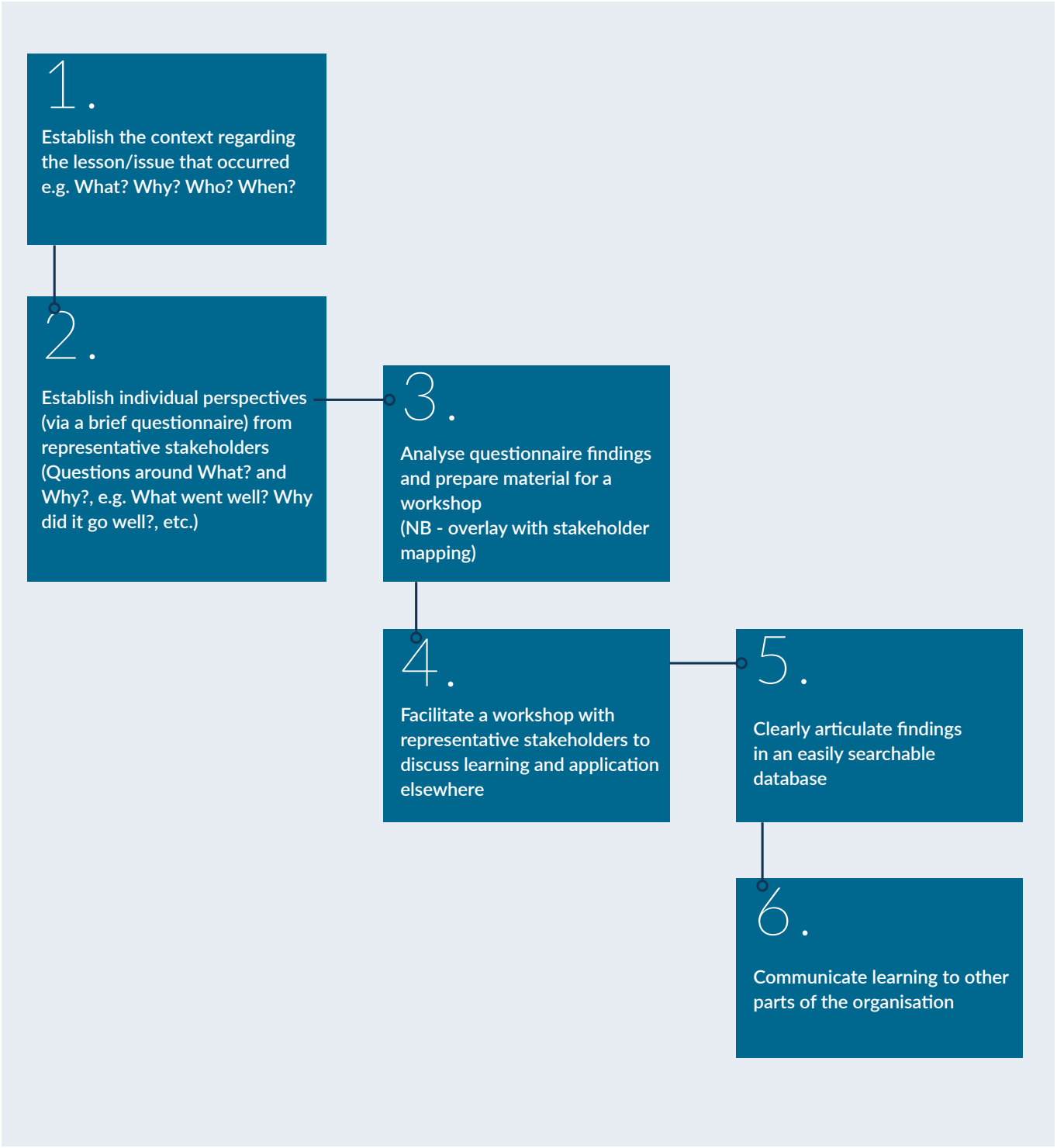
In order to receive accurate and timely information, it is important that members of staff feel free to make their opinions known without fear of blame or recrimination. Executives and managers are responsible for ensuring that an appropriate culture exists within the organisation.

The following are useful methods to help engender a culture of continuous improvement:

- Review of risk management information to determine the accuracy and effectiveness of data, for instance, did the estimation of risk impact accurately reflect the consequences of an event that occurred?
- Review of issues (events which that occurred) and insurance claims to ensure that the root causes are understood and actions are in place to control future events
- A process of lessons learned should be in place to systematically review good and bad practices, and identify measures to either disseminate good practices or mitigate bad ones. Figure 12 depicts a typical lessons learned process. Undertaking periodic lessons learned and implementing changes will help to ensure a culture of continuous improvement
- Compare your organisation against others within the same sector as well as best practice organisations from other industries. A list of relevant industry bodies and links to useful knowledge forums is provided in the appendix.

FIGURE 12

Lessons learned process



14. WHERE TO LOOK FOR FURTHER INFORMATION

- *Against the Gods – the remarkable story of risk*, by Peter L. Bernstein
- *Airmic: Roads to Ruin* – A study of major risk events: their origins, impact and implications. A report by Cass Business School on behalf of Airmic – 2011
  www.airmic.com
- *Airmic: Roads to Resilience* – Building dynamic approaches to risk to achieve future success.
  A report by Cranfield School of Management on behalf of Airmic – 2014
  www.airmic.com
- *Airmic: Roads to Revolution* – Reshaping risk and resilience for the future – 2018
  www.airmic.com
- *Airmic: The importance of managing corporate culture* – 2017
  www.airmic.com
- Airmic: Scenario Analysis: A Practical Guide: Helping to develop insight and manage uncertainty – 2023
  www.airmic.com
- *Airmic: Investing in the right future: AI and Future of the Profession 2023*
  www.airmic.com
- *Airmic: Competency Framework* – 2020
  www.airmic.com
- *Airmic: Reputational Risk Framework* – 2020
  www.airmic.com
- *Airmic: Navigating geopolitical risk: Building resilience demands collaboration in a challenging world – 2023*
- *Airmic: Complex supply chains in a complex world* – 2019
  www.airmic.com
- *Airmic: Emerging risks* – 2019
  www.airmic.com
- COSO: Committee of Sponsoring Organisations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework
  www.coso.org
- FRC: UK Corporate Governance Code 2024
  https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/
- FRC: Corporate Governance Code Guidance 2024
  https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance/
- FRC: Guidance on Board Effectiveness – 2018
  www.frc.org.uk
- FRC: The Financial Reporting LAB - where investors and companies can come together to develop pragmatic solutions to today's reporting needs
  www.frc.org.uk
- IIA: The IIA Three Lines Model – 2020
  www.global.theiia.org
- ISO: ISO 22316, Guidance for Organisational Resilience
  www.bsigroup.com
- ISO: ISO 22301 Societal security – Business continuity management systems – Requirements
  www.bsigroup.com
- ISO: ISO 31000:2018, Risk Management – Principles and guidelines
  www.bsigroup.com
- Marsh: The Global Risks Report – 2024 –
  www.marsh.com
- The Marsh McLennan Cyber Handbook – 2022
  www.marsh.com
- Risk Coalition: Raising the bar – Principles-based guidance for board risk committees – 2019
  www.riskcoalition.org.uk
- Riskonnect, Risk Management Information Systems (RMIS): The Buyer's Guide
  www.riskonnect.com

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.

airmic

www.airmic.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With more than 45,000 colleagues advising clients in over 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue of $23 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on LinkedIn and X.

Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511).

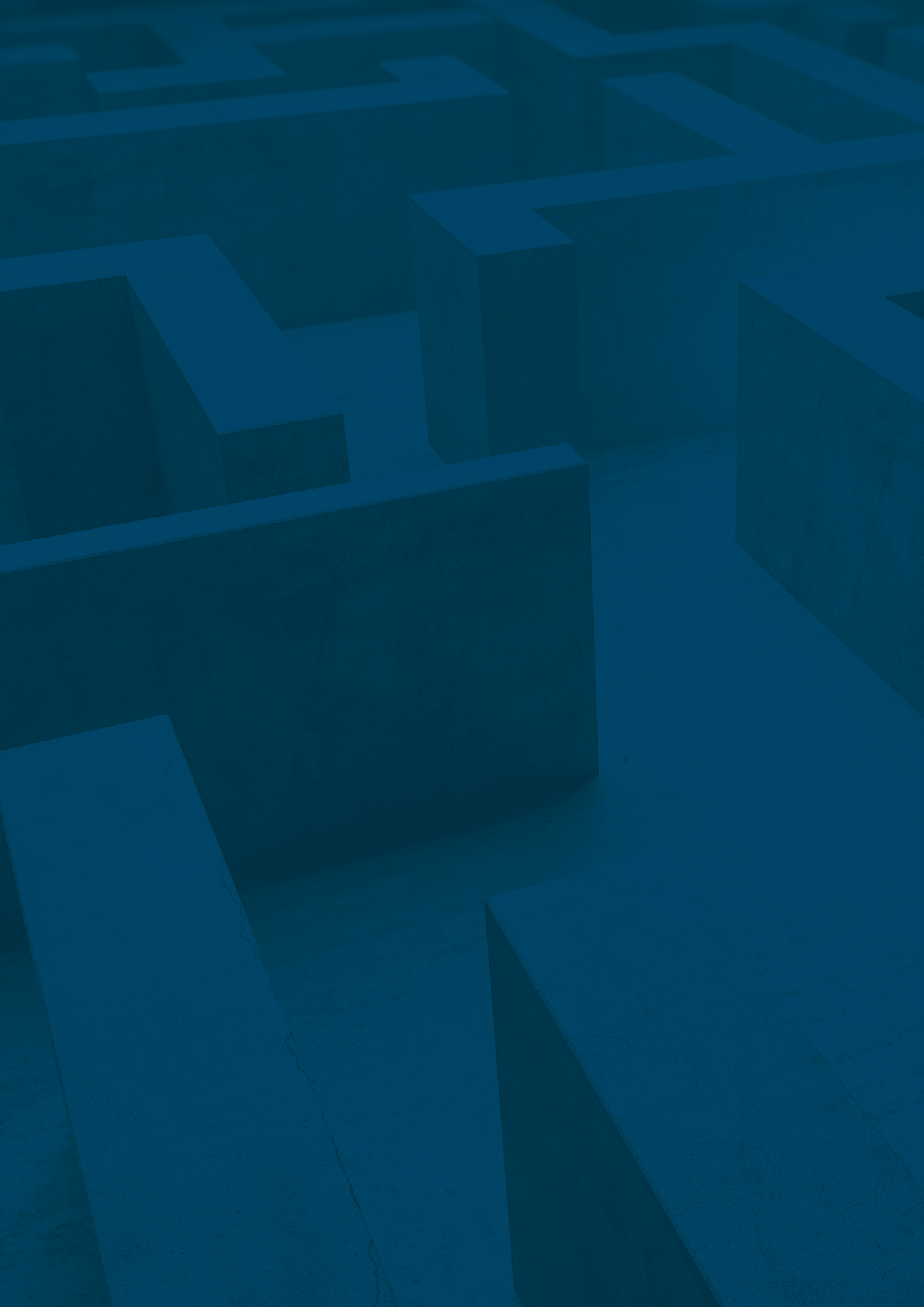
Tower Place, London,
EC3R 5BU
+44 20 7357 1000

Marsh

www.marsh.com

Fiona Davidge

Fiona Davidge, currently Head of Corporate Risk at the House of Commons, acted as Executive Editor for the original version of this guide.



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