

The background features a black and white photograph of a city skyline, including the Gherkin and The Shard. A thick red diagonal stripe runs from the bottom left to the top right, partially obscuring the buildings.

airmic

EXPLAINED

RISK AND MANAGING RISK

A short guide

2018

 MARSH

Acknowledgements

About Marsh

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US\$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter, @MarshGlobal; LinkedIn; Facebook; and YouTube.

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



Fiona Davidge

Fiona Davidge acted as Executive Editor for this guide and thanks for performing this role are extended to Fiona by Airmic.

Fiona Davidge is currently Enterprise Risk Manager with the Wellcome Trust, a global charitable foundation dedicated to achieving extraordinary improvements in human and animal health. Her role encompasses corporate risk management, insurance, health and safety, business continuity and fraud prevention. Previously she worked for Transport for London and Thames Water, in roles focused on risk management, incident response and security. She also held a commission in the Royal Air Force.

Fiona is a Fellow of the Institute of Risk Management and a Member of the Association of Insurance & Risk Managers in Industry & Commerce. She sits on the British Standards Risk Management Technical Committee and represents the UK as a Risk Expert to the International Standards Risk Management Technical Committee.

Contents

1	Introduction	4	5	Leadership commitment and culture; roles and responsibilities	22	7	Risk communication, reporting and monitoring	36
2	What is risk?	6				7.1	Communicating your risk management programme	36
2.1	Understanding the definition of risk	6	5.1	Risk culture explained	22	7.2	Formalising monitoring	36
2.2	What is risk management?	7	5.2	Illustrating the impact of poor culture	24	7.3	External reporting	37
2.3	Recognising sources of risk	8	5.3	Communicating roles and responsibilities	25	8	Risk process overview	38
2.4	Analysing and evaluating risk	8	6	Articulating risk in the organisation	26	9	Business continuity, resilience and insurance	40
2.5	Treating risks	8	6.1	Defining risk criteria for consequence	26	9.1	Business continuity management explained	40
2.6	Enterprise risk management	10	6.2	Defining risk criteria for likelihood	28	9.2	Introducing organisational resilience	41
2.7	The COSO risk management framework	11	6.3	Using heat maps to display different risks	29	9.3	Transferring risk by insurance	43
3	Understanding risk management principles	12	6.4	Risk appetite	30	10	Horizon scanning for new and developing issues	44
4	Understanding governance and framework	16	6.5	Illustrating risk appetite in business	33	11	Continuous improvement	46
4.1	Governance explained	16				12	Where to look for further information	50
4.2	Introducing the risk framework	17						
4.3	The three lines of defence model	19						
4.4	What the Financial Reporting Council requires	20						

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 2008 financial crisis, well publicised large company failures and the increasing maturity of corporate governance frameworks.

Societal trends such as business accountability, disclosure of information, the velocity of change, the connectivity of risks and the impact of emerging technologies have all added emphasis and importance to the need for effective risk management. 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, increasingly, the focus now is to avoid increased complexity and ensure that risk management enhances existing business structures by operating as an integral part of established 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 frameworks.

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 British Standard for business continuity, BS 22301, and

the British Standard for resilience, BS 65000, 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.

“Codes put forward principles for best practice that make poor behaviour less likely to occur; and public reporting can make it harder to conceal such behaviour. But, by itself, a code does not prevent inappropriate behaviour, strategies or decisions”.

*Stephen Haddrill
CEO, The Financial Reporting
Council,
The Airmic Lecture 2018*

2 What is Risk

Risk is a natural part of life, both in business and leisure. In “Against the Gods”, the writer 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 and ISO Guide 73 which state:

“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
- 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 the business, and even threaten lives.
- 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.
- Uncertainty is inherent in risk. Uncertainty can arise from a number of different sources, including deficiency of information, understanding or knowledge of an event, or a lack of awareness of its possible impact.
- Objectives can have many different aspects, including finance, safety, quality, regulatory or reputation, and can apply at different levels of an organisation.

2.2 What is risk management?

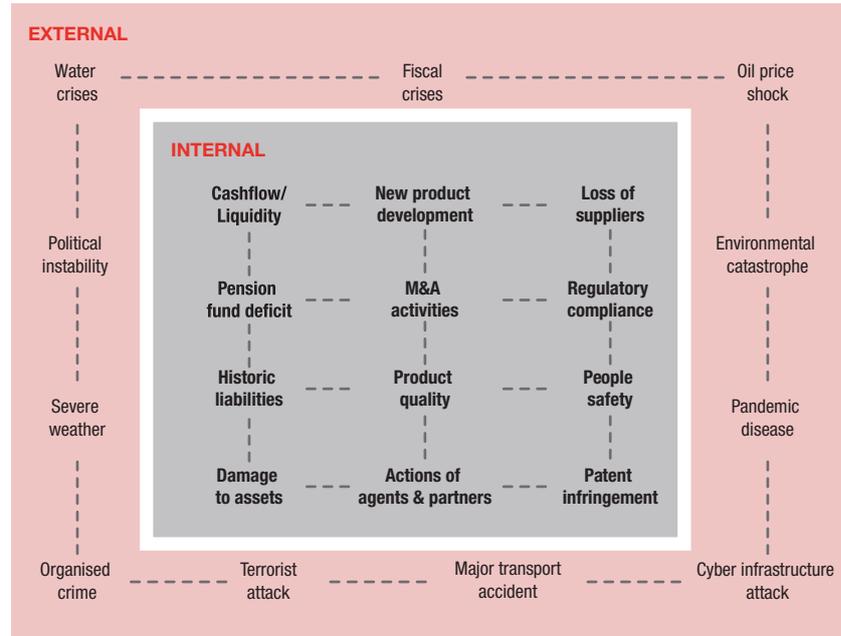
Risk management is the identification, assessment and prioritisation of risks followed by co-ordinated and economic application of resources to maximise the realisation of opportunity or address the impact and/or likelihood of adverse events.

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

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

Figure 1 Internal and external sources of risk



1 illustrates internal and external sources of risk.

No organisation or individual can exist in isolation and consideration of risk must take account of factors which 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 guides.

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 risk sources and there are many different response strategies depending upon the objectives of the business. 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 enhance controls.

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 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 in-house 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.

2.6 Introducing Enterprise Risk Management

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

Research undertaken demonstrates the positive link between mature ERM processes and business value (see references – *The Valuation Implication of Enterprise Risk Management Maturity*).

Risk maturity is about having a sustainable, repeatable and mature enterprise risk management 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. These assessment tools are often used by internal audit teams as well as by risk

managers and typically use five levels of maturity.

Research published in recent years from surveys and the analysis of data from the use of maturity models indicate that mature risk management can be correlated with enhanced business performance.

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 integrated framework, COSO ERM. 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 the COSO Internal Control Integrated Framework.

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.

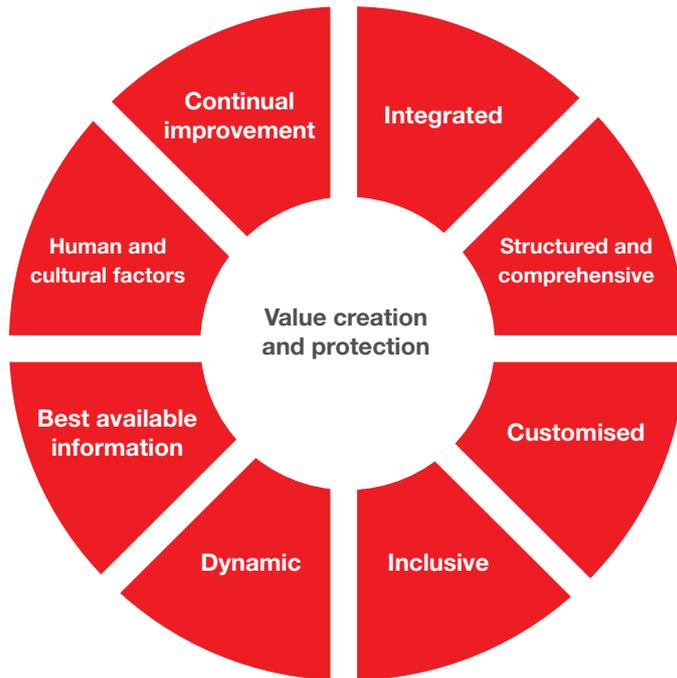
The structure of the COSO ERM is illustrated in Figure 2.

Figure 2 The COSO Framework is a set of principles organised into five interrelated components



3 Understanding risk management principles

Figure 3 The risk management principles – ISO31000:2018



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

ISO31000 contains eight principles which help guide organisation's 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 are considered in more detail below.

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, 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, 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.**

All organisations operate in a different context 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 an 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 organizational 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 which 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.

“Board risk blindness describes when a board fails to engage with important risks, including reputation risk, to the same degree that they engage with reward and opportunity”

Roads to Ruin

4 Understanding governance and framework

4.1 Governance explained

Corporate governance is a code of behaviour expressing how management teams in companies should act and be organised (governed) both 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 upon the stated goals of the 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 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.

“Risk and how it is managed will become a more regular item on the boardroom agenda in the next three years”

Airmic A profession in transformation, survey and report 2017

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.



Figure 4 The risk management framework – ISO31000:2018

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 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

The board provides direction to senior management by setting the organisation's risk appetite. It also seeks to identify the principal (level 1) risks facing the organisation.

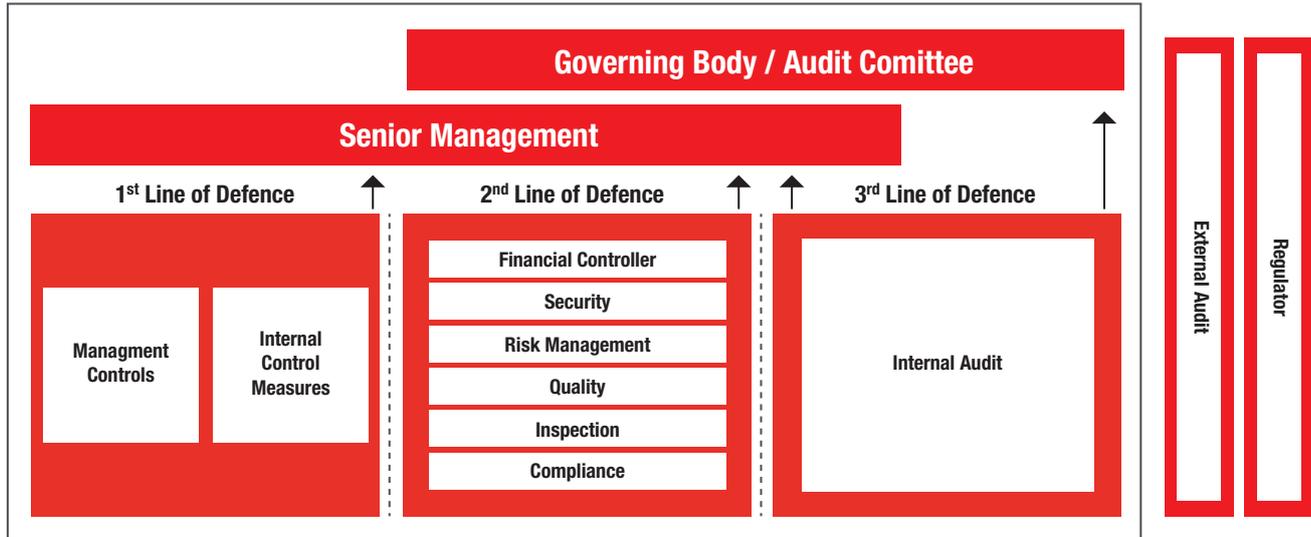
The board assures itself on a regular basis that senior management is responding appropriately to these risks.

The board delegates to the CEO and senior management primary ownership and responsibility for operating risk management and control and embedding an effective culture throughout the

organisation. It is management's job to provide leadership and direction to the employees in respect of risk management, and to control the organisation's overall risk-taking activities in relation to the agreed level of risk appetite.

1. The first line of defence – functions that own and manage risk
2. The second line of defence – functions that oversee or specialise in risk management and compliance
3. The third line of defence – functions that provide independent assurance, above all internal audit.

Figure 5 The three lines of defence model



Source: *The Three Lines of Defense in effective Risk Management and Control. Position Paper. The Institute of Internal Auditors 2013*

The assessment of risks should:

- Be part of the normal business planning process
- Support better decision-taking
- Ensure the board and management respond promptly to risks when they arise
- Ensure shareholders and other stakeholders are well informed about the principal risks and prospects of the organisation.

Financial Reporting Council (FRC) guidance, 'Risk Management, Internal Control and Related Financial and Business Reporting 2014'

4.4 What the Financial Reporting Council requires

For many years, the UK Corporate Governance Code has required the boards of companies to be responsible for determining the nature and extent of the significant risks they are prepared to take in achieving their objectives. There has been a further strengthened focus on risk management. The Financial Reporting Council (FRC) now requires all listed companies to confirm that they have carried out a robust assessment of the principal risks facing their company, and to illustrate how they have applied the Code in their annual reports and accounts.

This explicit regulatory obligation has increased the visibility of risk management at a board level and has brought a higher level of scrutiny to risk management processes. Risk management and related internal control systems must be monitored, with companies carrying out reviews of their effectiveness.

Overall, an effective risk governance framework is essential in order to achieve these objectives, and communication around risk should be at the centre of this framework.





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 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 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 have admitted lying to markets and government officials about vehicle mileage and emissions. Investors in both companies, along with 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.

The sinking of the Titanic – lessons for today from the past 1912: Although the disaster happened more than a 100 years ago, the lessons remain relevant today. There was another ship, the Californian, within 30 miles of the Titanic, and its crew saw flares and intercepted emergency response requests. After the Titanic sank, a U.S. Senate subcommittee and the British Board of Trade concluded that the Californian could have rescued some of the people who were left floating in the water before the Carpathia made it to that location to rescue survivors. Speculation was that the Captain of the Californian didn't realize the seriousness of Titanic's plight, others say it was negligence. In response to the disaster, vessel emergency response plans were implemented by governing agencies in the US and the UK. These plans include required training and emergency response from nearby vessels.

Fukushima 2011: In his combative preface to the report, Kiyoshi Kurokawa, a medical doctor and professor emeritus at Tokyo University, said the crisis was the result of "a multitude of errors and willful negligence", by the government, safety officials and the plant's operator, Tokyo Electric Power (Tepco). Behind the safety mishaps and lack of readiness for a tsunami in a region known for powerful earthquakes, are cultural traits that ensured the disaster was "made in Japan", Kurokawa said.

Co-operative Bank Scandal 2013 and 2018: The disgraced former chairman of the Co-operative Bank has been banned from the City for life after using company phones to access premium rate chat lines and to send and receive "sexually explicit and otherwise inappropriate messages, and to discuss illegal drugs" the Financial Conduct Authority found. The Treasury also announced in March 2018 that it was launching an independent review into how the bank was regulated.

5.3 Communicating roles and responsibilities

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

- Recognising that they are 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.
- 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 new and developing risks, and the effectiveness of controls
- Implement controls as part of day-to-day duties
- Report ineffective and/ or inefficient controls.

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;

Everyone in the organisation should be aware of their role in the risk management strategy for 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 which 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 which allows comparison.

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

“Risk Criteria are the terms of reference against which the significance of a risk is evaluated.”

Definition from ISO Guide 73

Table 1 Risk assessment criteria for consequence

Score	1	2	3	4	5
Consequence Type	Insignificant	Minor	Significant	Major	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.

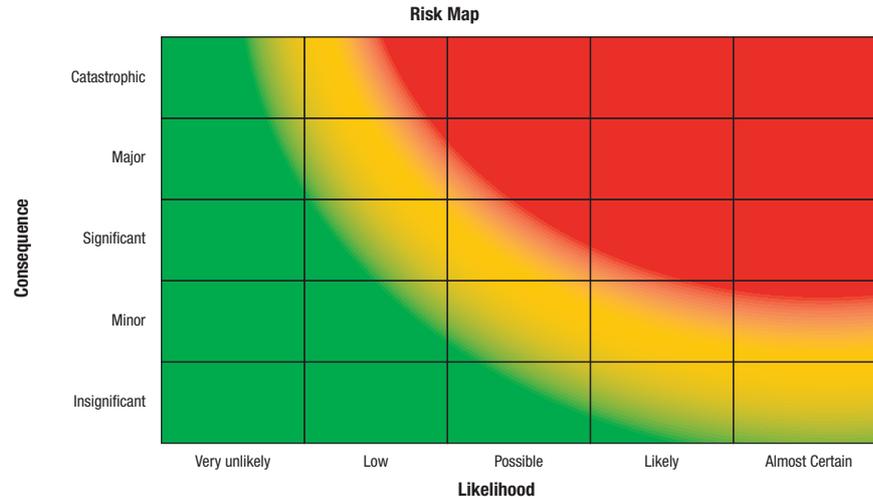
Table 2 Risk assessment criteria for likelihood

Score	Probability of occurrence in next 24 months %	Likelihood expressed in day-to-day language
1	0-10	Very unlikely: Only in acceptable 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 establishment of 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 is sometimes also called a heat map.

Figure 6 A typical risk map or heat map



This form of display is often referred to as a heat map. In such a map the colours represent the following:

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

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 which others might regard as completely unacceptable. Some organisations might view the primary objective as vital and will accept other risks with adverse outcomes.

Risk appetite is the amount and type of risk an organisation is willing to pursue or retain

The expression risk tolerance is also sometimes used.

Risk tolerance is what an organisation does not want to do



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:

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



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. Simple risk appetite statements for the each of the teams might look like this:

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 “Play to win”

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

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 which allow that 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.



7 Risk communication, monitoring and reporting

7.1 Communication 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 risk appetite and supporting 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 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 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 process 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 FRC reporting requirements referenced earlier in this guide, investors increasingly are seeking reassurance that organisations adhere to risk practices which reflect their investment criteria. Relevant areas for attention include climate change, sustainability, corruption and safety. The indexes issued by Dow Jones on sustainability and 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 organisations' annual report.

“The board should define the processes to be adopted for its ongoing monitoring and review, including specifying the requirements, scope and frequency for reporting and assurance...”

2014 Update to the UK Corporate Governance Code, Airmic Guide 2015

“The purpose of risk reporting is to provide information about the company's current position and prospects, and the principal risks it faces. It helps to demonstrate the board's stewardship and governance...”

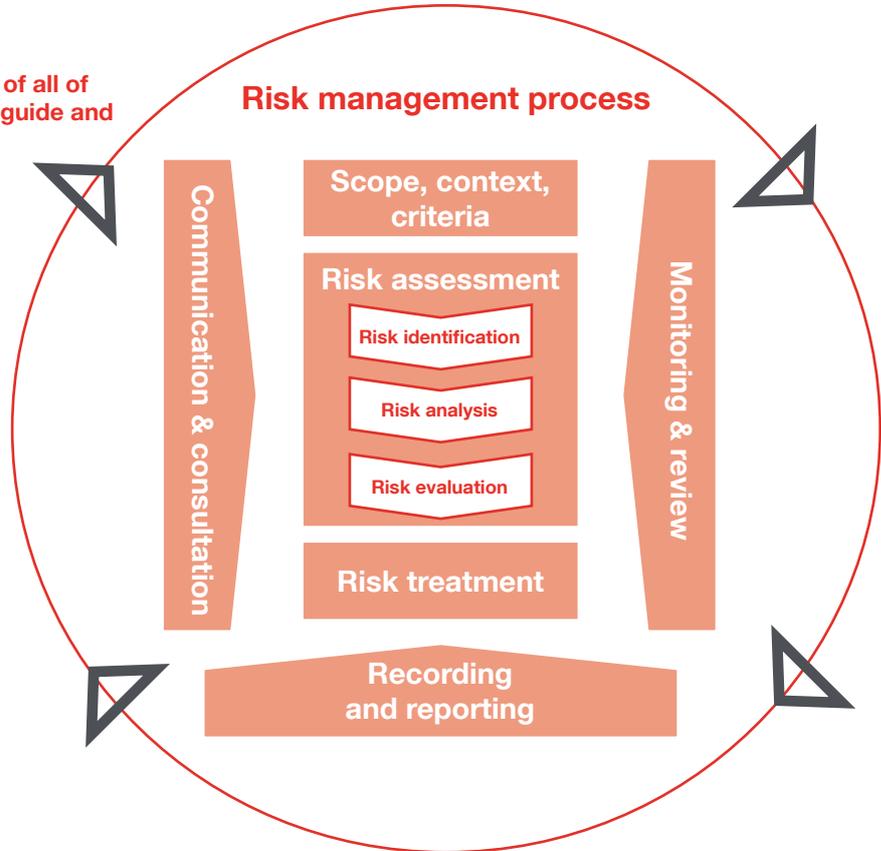
2014 Update to the UK Corporate Governance Code, Airmic Guide 2015

8 Risk process overview

The overall risk process takes account of all of 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. The relevant British Standard, BS ISO22301, was released in 2012 and replaced BS 5759:99. An effective BCM plan should address the following core elements:

- Emergency response
- Crisis management
- IT 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 co-ordination 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

The introduction of the British Standard BS 65000 for Organisational Resilience has helped shape what resilience is and what it means to businesses. 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 Resilience* and illustrates the link between the principles of resilience, business enablers and resilience outcomes.

Anticipate and monitor

The ability to identify risks (both internal and external, including those from third parties) is fundamental for a resilient organisation. Being able to see the evolution of a risk can help ensure appropriate action is taken in a timely manner. In addition, having procedures in place to assess the risk, and also having the ability to monitor and adapt to developments, will help organisations ensure they are prepared to act should an event occur.

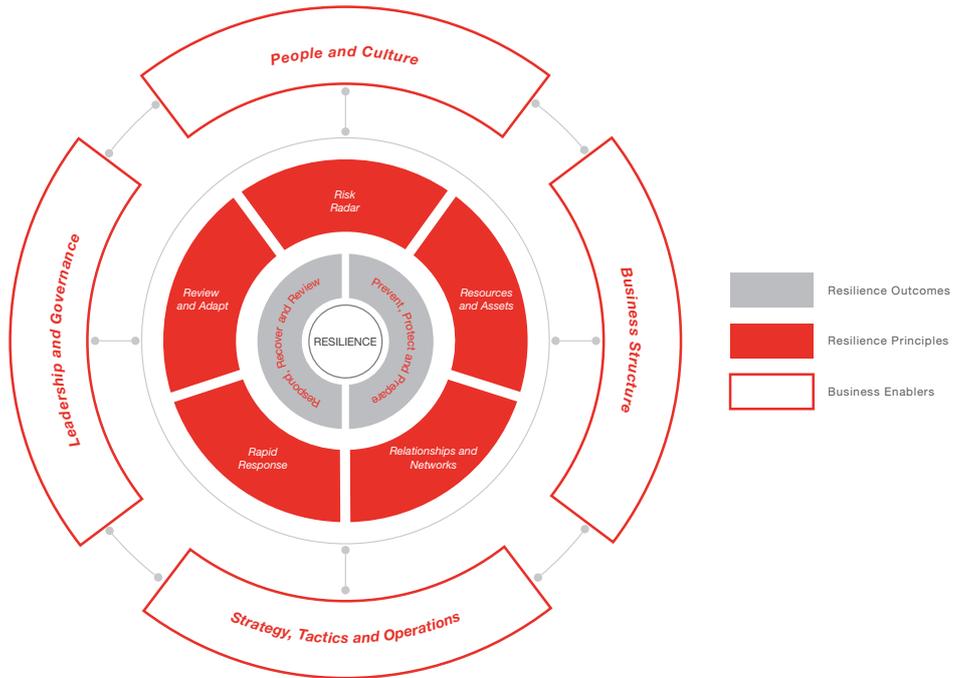
Prepare and align

The ability to share good practice is critical for a resilient organisation. By removing silos, building awareness and sharing knowledge across all departments, an organisation as a whole will benefit. Aligning risk management with business objectives and effective engagement with other parts of the organisation help embed resilience and mitigate a negative event. Oversight of key suppliers and customers will ensure that there are no surprises if an event occurs.

Respond and adapt

Being able to respond is essential but may not, in itself, result in a resilient organisation. A resilient organisation will have the ability to respond in a way that is consistent across all areas, which helps ensure and demonstrate effective management and control of the situation. As every event is unique, an organisation needs to be able to adapt its response, its way of working, and the execution of the business

Figure 8 Resilience outcomes, principles of resilience and the business enablers – *Roads to Resilience, Airmic 2014*



in the event of a negative impact. By being agile, the organisation will be in a position to continue operations in what could be a significantly-changed environment.

Evaluate and review

The ability to conduct a debrief following an event is critical in order to capture the lessons learned.

This should include a review of the actions taken and determine whether any existing processes should be updated as a result. Once captured, these lessons should be shared across the organisation in order to reduce the likelihood of the same problem occurring. The organisation must be able to apply the learning from the event and adapt where necessary. Being prepared to manage these areas will help ensure organisations are able to withstand a disruption; however, for resilience to be truly effective, it must be fully embedded and part of an organisation's culture.

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 organisations 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 Horizon scanning for new and developing issues

As indicated earlier, good risk management requires organisations to monitor the constantly evolving internal and external risk landscape for new and developing risk issues.

Some examples of new and developing risk issues are outlined below.

- **Technological risks** which arise from new and developing technologies and processes. These may include (but are not limited to) risks associated with artificial intelligence (AI), nanotechnology, cyber risk and the internet of things (IoT). Despite significant advancements in AI, with computers now capable of performing more tasks than ever before, future developments in the AI field could present a noteworthy technological risk.
- Nanotechnology also presents a number of issues which range from health implications to environmental risk.
- Cyber risk has been acknowledged for some years as a major concern for many organisations. However, as the risk continues to evolve and affect an increasing number of industry sectors in different ways, it can still be viewed as a new and developing issue.
- Information security and privacy risks related to the IoT also illustrate an example of a new and developing issue.
- **Shifting regulations** bring a number of implications which are associated with compliance and litigation issues. Changes to global regulatory structures can create uncertainty, thereby presenting an important issue which is both new and developing. An abundance of regulatory requirements can make this a difficult issue to tackle, and often an enterprise-wide approach represents a practical step towards addressing this constantly altering risk.
- **Talent availability and intergenerational team working** represents a new and developing issue, and the ability of an organisation to retain the talent required to ensure ongoing success is a key consideration across a number of different industry sectors.

- **Sustainability demands** are likely to increase for organisations, including heightened reporting requirements. This is largely due to greater awareness around environmental, social and sustainability issues. For example, the increasing requirement for Environmental, Social and Governance reporting.
- **Climate change** may lead to a myriad of complex risk issues including natural catastrophe risks, food and water crises, biodiversity loss and ecosystem damage. These impacts affect organisation's risk profiles directly and indirectly depending on the nature of the organisation's business, where business is undertaken and the parties involved.

Whilst organisations face threats from many sources, it is crucial for them to understand the opportunities presented by the changing risk landscape; informed risk-taking will allow the organisation to flourish.

Scenario analysis is now being used to help organisations develop a clearer understanding of how adverse events might impact their objectives. See the separate Airmic guide for more information on this important risk management tool.

“Using strategic scenarios

Where weaknesses or exposures to change are identified within the business model, strategic scenarios can help identify key risk indications that identify that a scenario is in the early stages of development. Organisations can use this to prepare training and awareness programmes across the business at all levels and build a more risk-aware culture. Strategic scenarios additionally can help identify the upside of risk and provide opportunities for the business to develop and grow.”

Scenario Analysis: A practical system for Airmic members, Airmic Guide 2016

11 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.

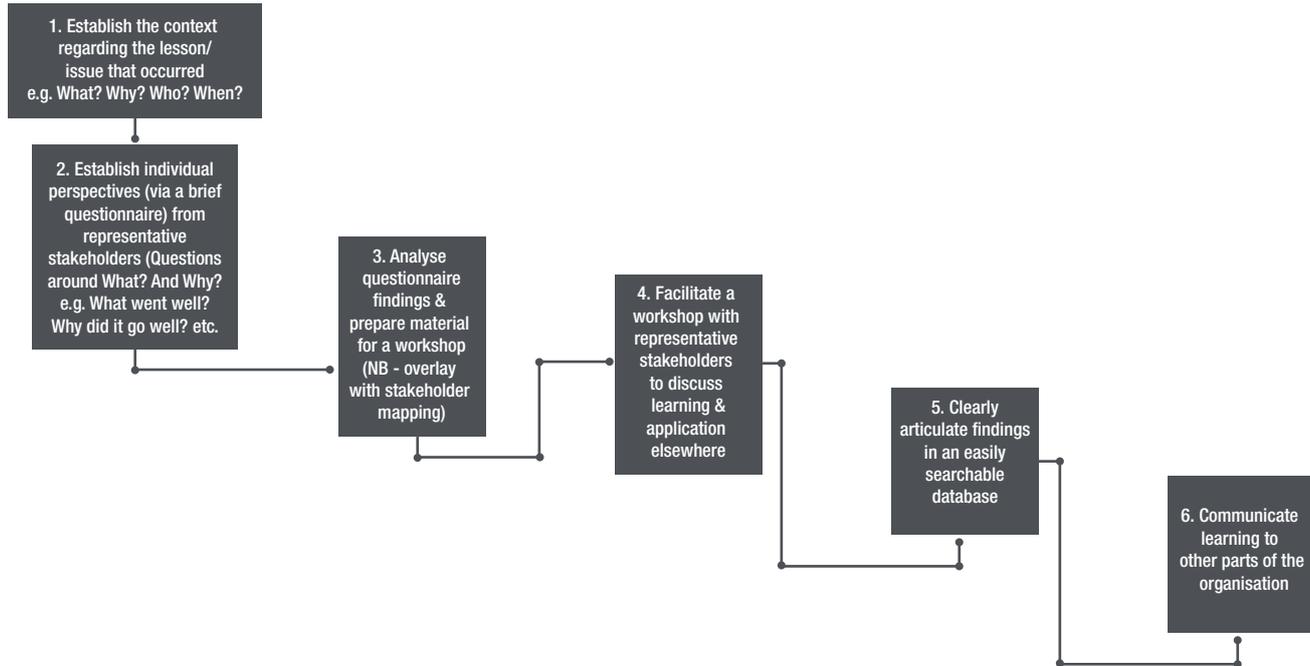
Having an agile risk management framework which can be relatively easily adapted is therefore beneficial. Change is inevitable and it is important that the risk framework reflects the structure of the organisation and is intuitive to use to ensure effectiveness across the organisation. The framework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

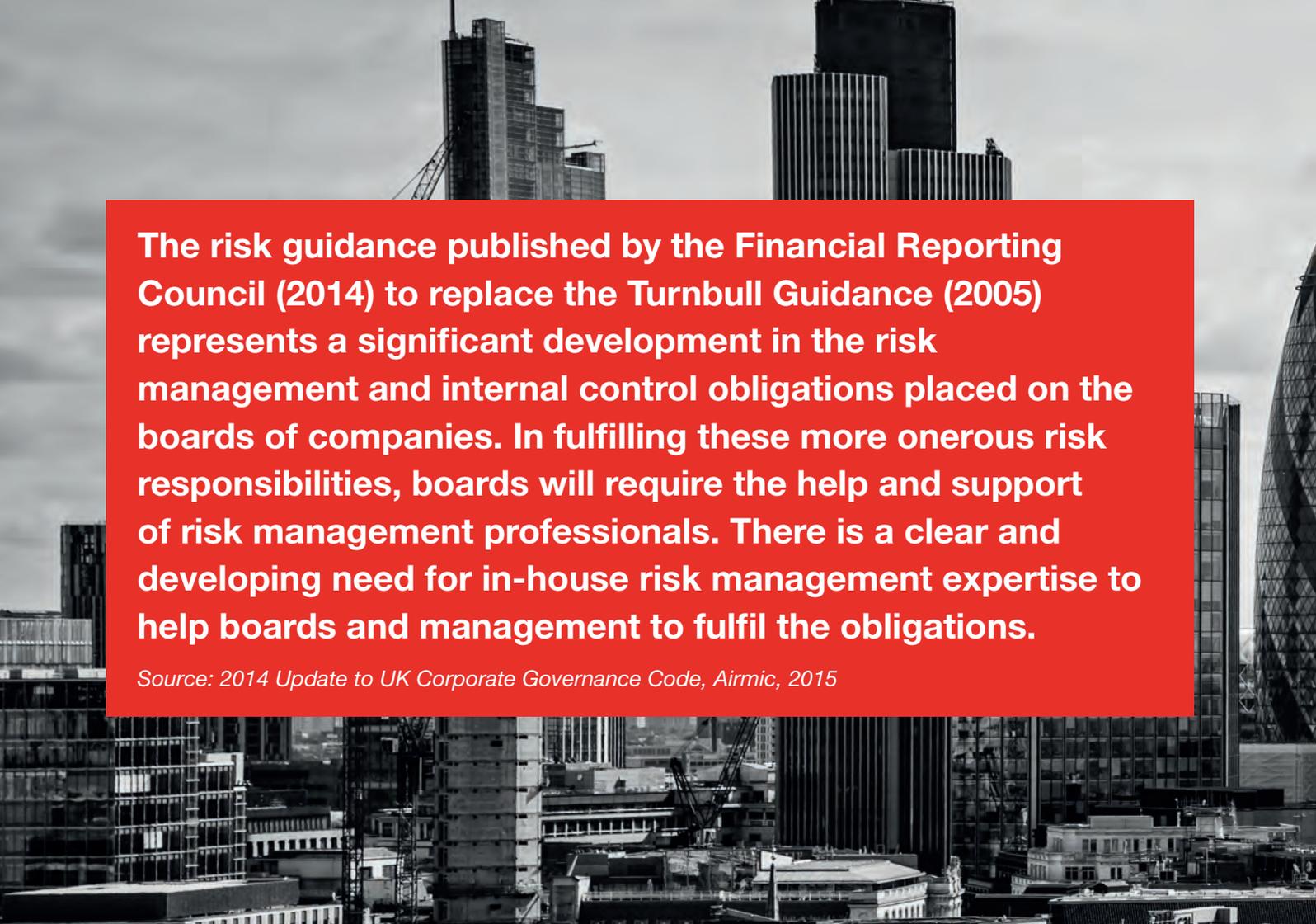
In order to receive accurate and timely information, it is important that members of staff feel free to make their opinions known without fear of blame or recrimination. Executives and managers are responsible for ensuring that an appropriate culture exists within the organisation.

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 have 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 10 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.

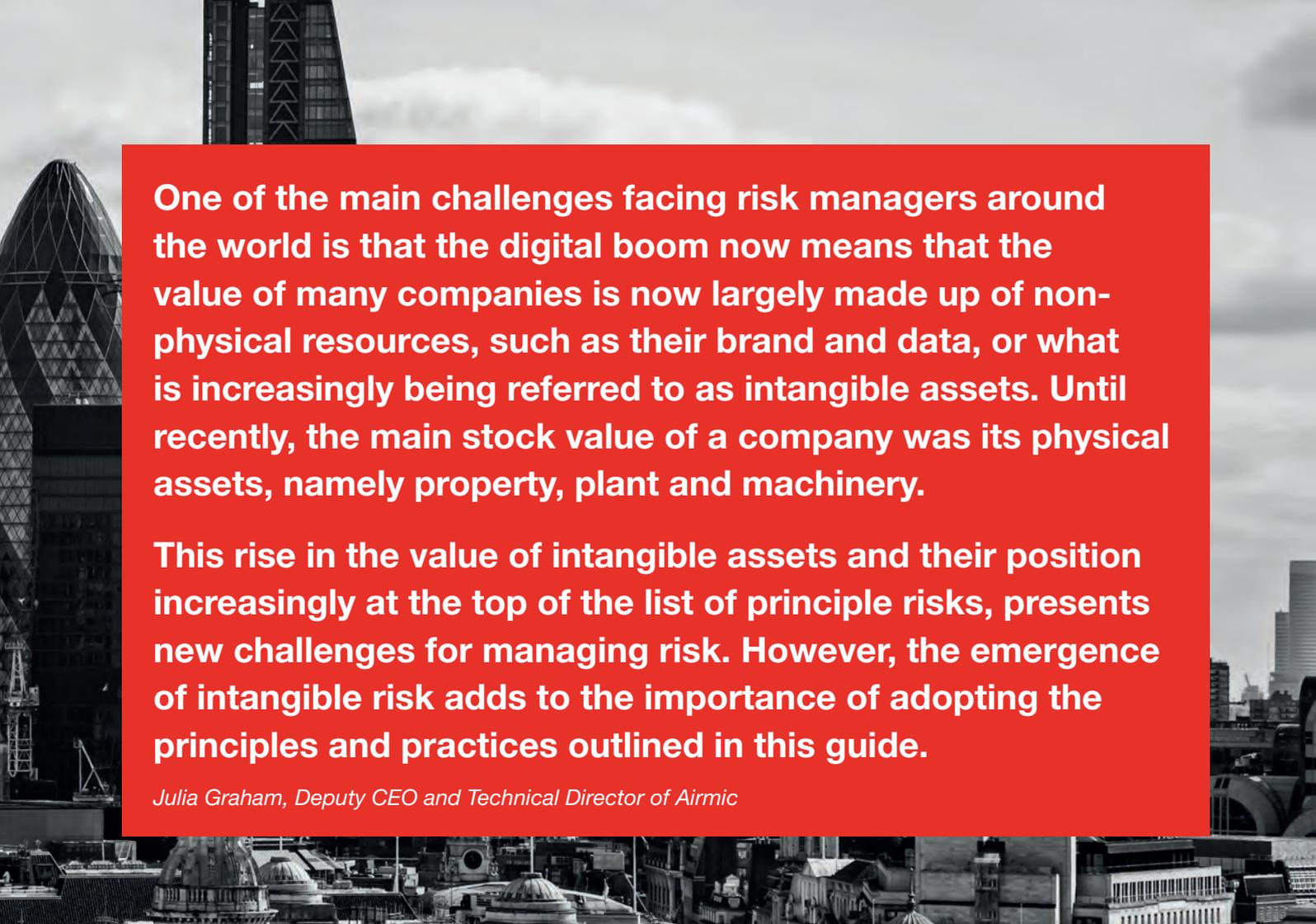
Figure 9 Lessons learned process





The risk guidance published by the Financial Reporting Council (2014) to replace the Turnbull Guidance (2005) represents a significant development in the risk management and internal control obligations placed on the boards of companies. In fulfilling these more onerous risk responsibilities, boards will require the help and support of risk management professionals. There is a clear and developing need for in-house risk management expertise to help boards and management to fulfil the obligations.

Source: 2014 Update to UK Corporate Governance Code, Airmic, 2015



One of the main challenges facing risk managers around the world is that the digital boom now means that the value of many companies is now largely made up of non-physical resources, such as their brand and data, or what is increasingly being referred to as intangible assets. Until recently, the main stock value of a company was its physical assets, namely property, plant and machinery.

This rise in the value of intangible assets and their position increasingly at the top of the list of principle risks, presents new challenges for managing risk. However, the emergence of intangible risk adds to the importance of adopting the principles and practices outlined in this guide.

Julia Graham, Deputy CEO and Technical Director of Airmic

12 Where to look for further information

- **shop.bsigroup.com**
BSI guide, Managing Risk the ISO 31000 Way, by David Smith and Rob Politowski
- **shop.bsigroup.com**
BS 31100:2011, Risk Management – Code of practice and guidance for the implementation of BS ISO 31000
- **www.coso.org**
Committee of Sponsoring Organisations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework
- **www.bsigroup.com**
ISO 31000:2018, Risk Management – Principles and guidelines
- **www.bsigroup.com**
ISO Guide 73, Risk management – Vocabulary
- **www.bsigroup.com**
ISO 22301, Societal security - Business continuity management systems - Requirements
- **www.bsigroup.com**
BS 65000, Guidance for Organisational Resilience
- **www.amazon.co.uk**
Against the Gods – the remarkable story of risk, by Peter L Bernstein
- **www.airmic.com**
Roads to Ruin – A study of major risk events: their origins, impact and implications. A report by Cass Business School on behalf of Airmic
- **www.airmic.com**
Roads to Resilience – Building dynamic approaches to risk to achieve future success. A report by Cranfield School of Management on behalf of Airmic
- **www.airmic.com**
The importance of managing corporate culture - Guide 2017
- **www.nirs.org**
The official report of The Fukushima Nuclear Accident Independent Investigation Commission – The National Diet of Japan 2012
- **www.transparency.org**
Corruption Perceptions Index 2015 published by Transparency International
- **www.sustainability-indices.com**
Dow Jones Sustainability Indices
- **www.airmic.com**
A structured approach to Enterprise Risk Management (ERM) & the requirements of ISO 31000
- **www.airmic.com**
Airmic Scenario Analysis: A practical system for Airmic members - Guide 2016
- **www.airmic.com**
Airmic Guide: The FRC Code
- **www.airmic.com**
Airmic: The Changing World of Risk



6 Lloyd's Avenue
London
EC3N 3AX

Ph: +44 (0) 207 680 3088
Email: enquiries@airmic.com
Web: www.airmic.com
EXP-0005-0318