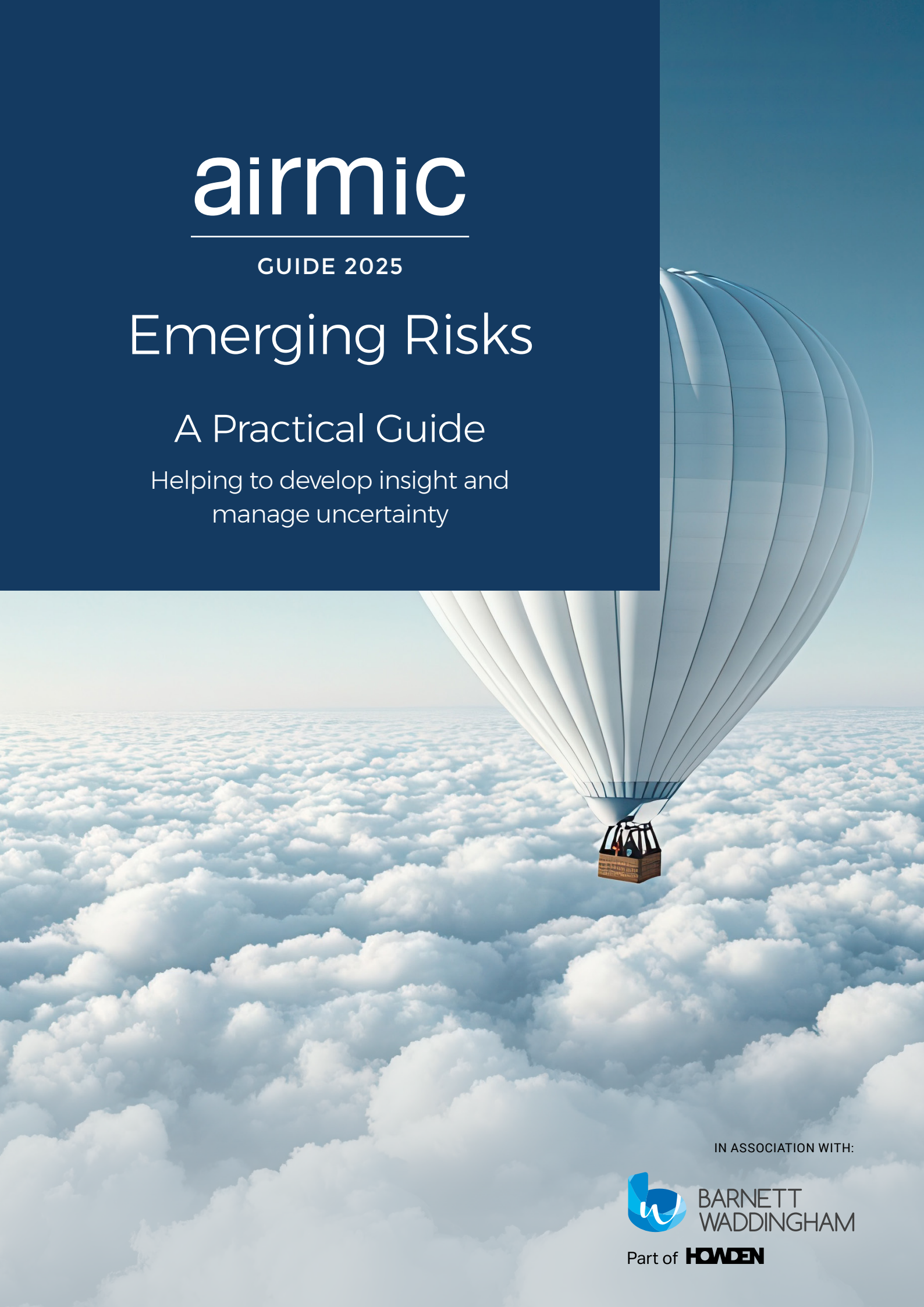
airmic

GUIDE 2025

Emerging Risks

A Practical Guide

Helping to develop insight and manage uncertainty



IN ASSOCIATION WITH:

BARNETT WADDINGHAM

Part of HOWDEN

Acknowledgements

Barnett Waddingham LLP
Our award-winning risk and resilience team is dedicated to helping our clients succeed. We empower clients by providing practical self-help resources, new insights and expert led consultancy on managing risk and developing resilience so they can make better informed decisions when navigating uncertainty.

All our efforts are dedicated to improved business outcomes, whether our clients' needs relate to people, strategy and business planning, cyber and information security, sustainability, business continuity and crisis management or all of these and more.

Our risk and resilience expertise together with our data analytics capabilities provide a range of sophisticated services, from the use of risk management tools, AI and data analysis, through to embedding our consultants into your teams.

For more information visit www.barnett-waddingham.co.uk or contact our Head of Risk and Resilience Services, Harshil Shah at: harshil.shah@barnett-waddingham.co.uk

Contributors
Julien Masselot, Partner, Barnett Waddingham
Karla Gahan, Head of Resilience Services, Barnett Waddingham
Fearghas MacGregor, Principal, Barnett Waddingham
Keith Smith, Senior Risk Consultant, Barnett Waddingham
Sophie Kinson-Williams, Client and Operations Manager, Barnett Waddingham
Marta Vicario-Velez, Risk Consultant, Barnett Waddingham
Adam Gurteen, Graduate, Barnett Waddingham
Lloyd Bartlett, Graduate, Barnett Waddingham
Abigail Norman, Consultant, Authentic Essence
Julia Graham, CEO, Airmic
Hoe-Yeong Loke, Head of Research, Airmic

About Airmic
Airmic celebrated its Diamond Anniversary in 2023 and today is the UK and Ireland's largest and most vibrant risk management and insurance association. Airmic has over 450 corporate members, more than 2,000 individual members, and is supported by a network of leading risk and insurance partners and affiliated institutes, associations, and universities.

We are growing through welcoming both those in the risk and insurance professions and in roles connected to risk and insurance, including those with a primary focus on governance, sustainability, finance, compliance, law, human resources, information security, health, safety and security, resilience and business continuity, and academia. As such, we are in a strong position to represent the views of our members, and to advocate for their needs within business, standards and regulatory bodies, and government in the UK, Ireland and internationally. We are active members of FERMA the Federation of European Risk Management Associations and IFRIMA the International Federation of Risk and Insurance Management Associations.

Our members enjoy access to a wide variety of face to face and online events and learning opportunities, networking, special interest groups and regional meetings, supported by a competency framework and mentoring scheme. Our online library of research materials, guides, papers, newsletters and curated readings, feature work by some of the brightest, most innovative, and experienced talent.

Airmic guides are provided to give an insight and some understanding into different areas of risk. They are not intended to address any particular requirements or issues. Airmic guides are not intended to replace the need for advice nor are they training guides. Airmic does not accept any liability for the content of the guides which are prepared based on the views of the author (who may not be an Airmic employee).

CONTENTS

Executive summary

This guide provides practical guidance on managing emerging risks.

While emerging risks can exhibit quite subtle and not always obvious differences when compared with other risks, we recommend that organisations manage emerging risks as part of their overall risk management system, considering emerging risks alongside other risks.

With typical characteristics of deep uncertainty and limited available information, emerging risks can be difficult to manage – they can materialise quickly, constantly change, and can significantly affect an organisation and its operations. While all risks in an organisation carry some residual uncertainty, with emerging risks, higher levels of residual risk are common. Procedures must be in place for continuous monitoring of these risks to allow the organisation to follow changes and adapt.

We manage risk using information and knowledge. Information comes from the correct and thoughtful analysis of reliable data. Data needs to be verified to make informed decisions. Emerging risk sits in an information and data desert, so misinformation, disinformation and the invalidation of previously verified facts is a reoccurring problem. To address these issues, we recommend that an organisation invests in horizon scanning techniques. To collate, assess and gain insight into how information relates to other information, we recommend the use of scenario analysis techniques.

We can consider the complex concept of knowledge as the ability to apply information thoughtfully and effectively when making decisions. However, emerging risks may have strategic implications, which can bring threats and opportunities, requiring us to level up and develop our knowledge towards strategic intelligence – the ability to make sound decisions for our future best interests.

If the organisation's current objectives cannot realise identified opportunities or they lead to an unacceptable level of uncertainty exposure, then perhaps it's the objectives of the organisation that need to be recalibrated. Recalibration is more likely with emerging risk exposure.

While important, the level of uncertainty is not the only factor driving strategic decision-making, nor is the level of uncertainty the sole controlling factor for choosing when a decision must be taken. However, to simplify strategic decision-making when considering the effect of uncertainty, it may be useful to apply some binary thinking:

Is this a situation where the organisation should use an 'assess and respond' approach? Or is this a situation where the uncertainty is deep, and a strategy of data and information gathering should continue, while the organisation positions itself, keeping as many options open as possible using a 'monitor and adapt' approach?

In this guide, we acknowledge that social change permeates through our organisations and there are many dimensions to the organisation's stakeholder community. For example, we have long recognised the

multicultural dimension as important, and that was a landmark towards what we now call diversity, equity and inclusion (DEI).[1]

Beyond multiculturalism, modern society is increasingly driven by information being transferred and shared. To truly understand and manage uncertainty, every organisation needs to look at its stakeholders, and at the influence and power living in every generation, particularly the younger generations, for whom digital living is all they have ever known.

Standards provide us with systems for establishing risk management within an organisation. Standards and governance guides also provide us with frameworks to govern the effectiveness of that risk management activity.

Within this guide, we address a gap in systems to provide a framework for identifying and assessing changes that give rise to emerging risks. Key to this framework, though, isn't the identification of emerging risks. The key to this framework is identifying and understanding behavioural change.

Strangely, it is common to find organisations investing in risk management but underutilising the value of their risk management activities in decision-making. Because managing emerging risk is notoriously difficult, organisations should maximise their risk management investment by integrating it into the heart of their decision-making processes.

Even after applying effective controls and establishing good resilience practice, some consequences can still overwhelm any organisation. In such situations, and where organisations are simply not prepared to bear all the potential losses, there is often an insurance product that can help. With emerging risk, we often find we are on the edge of where insurance can help, but innovation in the insurance markets continues, and new products and new ways to obtain cover are becoming available.

Aim of this guide

This guide aims to provide users with insights, analysis, tools, techniques and strategies to help with the management of emerging risks, however these are defined in the risk management system and taxonomy of an organisation.

For ease of use, this guide will mainly focus on emerging risk, with just a couple of notable exceptions, which will allow the user to decide when the strategies and techniques apply to managing other risks.

This guide is also a companion to the two other guides in this suite, on Scenario Analysis[2] and Horizon Scanning.[3] Therefore, this guide will avoid unnecessary and unhelpful repetition found in the other two guides.

Finally, recognising that organisations can be quite different in terms of their sector, business model and level of risk maturity, this is a self-help guide, where the user applies the concepts and suggestions to match their own needs and circumstances.

1. What is an emerging risk?

The word ‘emerging’ comes from the verb ‘emerge’ which traces its roots back to the Latin word ‘emergere’ meaning ‘to rise up or to bring to light’ formed from 'ex' (meaning out) and ‘merger’ (meaning to dip or sink), suggesting the idea of something rising from beneath a surface. The concept of ‘emerging’ has evolved over time, and now in everyday use can apply to something being discovered or developing out of an evolving situation, or to someone or something which is becoming more prominent. An example, in the fashion industry, 'emerging' may describe a colour or style developing as a trend. In science, an observed behaviour may be described as ‘emerging’ as an evolving theory among scientists.

The wide range of uses, coupled with differing views and definitions of risk, explains the variation for when the label ‘emerging’ becomes attached to a risk.

When used, what is being communicated is a risk with specific characteristics generated from change, and one that is not fully understood. In addition, the term ‘emerging’ often, but not always, implies something not seen before. Emerging risks can be risks that were thought to be understood, but which are pushed to new extremes or into new contexts, where the limits of past understanding are exceeded.

Regardless of its source and characteristics, an emerging risk remains a risk, and we should consider emerging risks, alongside all other risks, when making decisions.

2. Polycrisis and permacrisis: The prolific engine of risk

The complexity, connectivity and volatile nature of modern society continues to give rise to many risks. There is no reason to believe the level of connectivity between risks will fall, nor any expectation that the high volatility seen across global societies will subside.

In recent years, people have coined two terms to describe this permanent state of bubbling uncertainty, which will continue producing multitudes of risks, including emerging risks, affecting organisations and society at large.

Polycrisis – the combination of 'poly' or multiple, to describe the connectivity and interactivity between sources and crisis, which refers to the state of change, which is the source of uncertainty.

Permacrisis – which speaks to the ongoing nature of change.

3. Managing in polycrisis and permacrisis

When faced with multiples of any item, humans group items according to characteristics, label the groups and, to the maximum extent possible, manage those items as a group. This is a strategy humans have developed to reduce the amount of cognitive energy exerted in managing and navigating within our natural environment. This field has seen much accomplished work, and in risk and decision-making, we often turn to Herbert Simon's work on Bounded Rationality.[4]

Accountancy is a good example of how people and professions manage a multitude of items as a grouped set. Organisations place any item labelled with a financial value in their accounts and, while payroll differs from physical assets, the accounts system, run by accountants, captures the financial effects of both.

Managing multitudes of risks is no different to the accounts example where risk types and labels are used to assign and describe groups of risks in a way that is helpful for their management.

So, while risks have important differences, they also often share recognisable similarities with other risks, which allows them to be managed better as a group. Emerging risk is really just one of these convenient groupings that humans create to help manage the number and complexity of risks faced. And as risks may have many characteristics, any single risk may be a member of many groups. For example, the risk of theft from a construction site is a risk for the project. It is a theft risk that general security measures may help to manage; it is also a financial risk as there is a cost to these items stolen.

As emerging risk is just one of many groups, and like accountancy which can manage finances across every part of the organisation, it is not surprising that the strategies, tools and techniques outlined in this guide may have value for other risk types too.

4. A fresh world view on the management of uncertainty

In past decades, the management of risk was predominately the management of threats. Emphasis was also traditionally on managing the threat through direct action and controls that were in place to prevent untoward events from occurring. In this guide, we have taken a broader and more widely accepted view, helping an organisation to manage the uncertainty that remains around opportunities it may want to realise. With emerging risks, we recognise there is greater uncertainty to manage, but the reason most organisations willingly engage with emerging risks is for the breadth and value emerging opportunities bring.

To make the most of this guide, users should remain mindful of the following:

- Threat management is important, but is just one lens on managing uncertainty. Opportunity management is as important as managing threat and, frequently, threats and opportunities are inseparable, requiring both lenses to be used in unison.
- Management of risk is not just taking action to limit the likelihood of a risk occurring; considering the organisation's resilience to residual consequences is just as important. Every risk carries residual consequences which are effects that remain even after mitigation.
- Long-term protection, creation of value and building resilience are all reasons why organisations should invest in emerging risk management.
- Emerging change is a strategic issue. Rather than remain on a fixed course, if the effects of uncertainties are unmanageable or unpalatable when assessed against the organisation's appetite for risk, then the organisation should review its strategic objectives.

5. Sources of emerging risk

Socio-technical

Technology, and more specifically, the interaction between technology and people, is the source of many emerging risks. Although not initially identified as a source of emerging risk, Emery and Trist studied interactions between people and the technology they used in mining during the late 1940s.[5] This type of interaction became known as socio-technical because there was a human perspective, influenced by societal factors, affecting the adoption and use made of technology. Even then, Emery, Trist and their colleagues recognised the importance of this interaction, leading to socio-technical design as a practice in its own right.

Since that time, the technology in society has become much more complex, but the idea of designing technological systems for their use and usability in society remains an important field. On the other hand, mistakes, underestimates, overestimates, misuse and even pure genius mean that the introduction of any complex technology to a wide population of users is a source of emerging risk.

A good example of an emerging risk, and simultaneously, an emerging opportunity, occurred when mobile phones changed from analogue to digital, with the creation of GSM in 1987. As part of that new technology, sending short messages of 144 characters became an option by simply marking the data packets sent and received as text packets rather than as voice packets. While the industry included it as a feature, at the time of inception for GSM, no one fully realised how popular this feature would become.

The feature of short messaging was user-friendly and well-designed from the start.[6] And now, when we look back on how useful the ability to send a short message is, to confirm arrangements, confirm deliveries, and pass numbers, addresses and any other small piece of data, it is hard to see why the opportunity was not wholly apparent to the mobile phone industry in 1987. In contrast, the major benefit the industry saw in a technical feature which allowed them to tag packets of data to be counted as something other than a voice packet was for an introspective industry use. The industry saw this feature as a way to update SIM (Subscriber Identity Module) cards over the air without the user having to do anything.

Not only is this a good example of an emerging risk that poses both threats for those who were not able to capitalise on the new technology and huge opportunities for those who were, it is a good example of why it is important to consider how people's behaviour may change.

We will revisit this behavioural point again as a principle in the framework section. When considering behavioural change, it is important to do so without being too constrained by the behaviour of the time. When GSM was first created in 1987, phones were just phones, not the pocket computers and cameras we carry around today, so the primary use expected for this 'mobile phone' was simple voice telephony. To gain the insight, the industry needed to step away from 'present applications' and think about what this

messaging system could do for person-to-person communications, in order to assess how societal behaviours may change. Often called 'out of the box' thinking, this is really the ability to take a critical look at what is important.

Geopolitics and ESG

While we have long recognised the fast pace of technology as a source of emerging risk, recent geopolitical and social changes have revealed significant threats and opportunities that are unrelated to purely technological development.

In some quarters, trust has become a rare commodity in international trade. The pressure on societies and the desire to grow economies that foster a better lifestyle have disrupted some important relationships in the fragile globalisation process started in the 1960s. For those seeking information on trust, the Edelman Trust Barometer is a helpful resource to access.[7]

Alliances have become fractured, tensions have risen in the South China sea, minerals and rare earth elements have become highly sought after, and financial strength has moved east. Today, geopolitics and home-grown political violence are a growing concern that can disrupt even the best-laid plans of any organisation.

And geopolitical events are not the only changes to society that need to be factored into risk and resilience planning. Consider, for example, the decades-long growth of interest in the environment, social matters and governance as a connected triple captured in the term ESG, first used in a World Bank document.[8] In ESG, we see the true effect of complex and connected risk on show. Failure to manage risks in these areas can not only reduce investment in an organisation, but with deep changes in socially responsible behaviour, organisations can sustain irrecoverable reputational damage, particularly as regulation tightens and forced transparency rises.

Liability and the growth in shared accountability

In law, litigation around environmental issues is also rising steeply.[9] Organisations are being held accountable for acts and decisions made before society responded to the climate crisis. Assets, designed and built to provide many years of service, have their lives shortened by a reduction in demand or legal cases brought against the organisation for the environmental impact the asset has caused. This risk is called 'stranded asset risk'.[10] Even if an organisation can tolerate and recover from reputational damage, and many cannot, the costs of litigation and losses arising from stranded assets are quantifiable risks.

Beyond climate change, we also see litigation rising in several other areas of shared liability. Obesity and drug dependency, for example, are increasingly important areas of concern in global societies.[11] Organisations judged to have contributed to these societal problems often bear responsibility for them, leading to liability. In response, we see efforts within the insurance industry to extend cover into areas of liability and introduce insurance products aligned with services to limit the damage of both risks and emerging risks.

The digital world – Cyber risks

The wholesale digitisation of our lives has created benefits and opportunities that cannot exist in a purely analogue world, but with digitisation, we opened an additional source of risk.

People have bundled online fraud, hacking and ransom attacks – to name a few – into the catch-all phrase 'cyber risk'. While many cyber risks are now understood, each day new cyber risks appear, meaning there are new emerging threats to face each day. We can therefore consider new cyber risks as emerging risks that fit both our categories of new to organisations and, when they first appear, new to the world.

The other feature that makes cyber risks quite a unique class of emerging risk is the fact the risks arise from the active and malicious intent of criminals, exploiting technology and societal norms. This means we must regularly review controls, as criminals constantly seek ways to circumvent them.

Managing cyber risks is complex, involving both technical barriers and social awareness, as many attacks these days use social engineering to gain access to systems.

Published in 2025 by the UK Government Department for Science, Innovation and Technology (DSIT), the Cyber Governance Code of Practice[12] was created to support boards and directors. The Code sets out the most critical governance actions that directors should address. It is an initiative that is supported by training that helps boards and directors to strengthen their understanding of how to govern for cyber security risks.

Besides the code, there is also a straightforward set of practices from the UK Government that everyone can adopt, called Cyber Essentials.[13] As the name suggests, these just cover the essentials, and organisations should recognise the complexity of the battle with malicious actors and implement other measures to protect themselves against understood risks and new emerging threats.

With its ongoing, emerging risk credentials, cyber threats are a strong candidate for being a permanent horizon scanning topic.

Enterprise Risk Management and emerging risk

Enterprise Risk Management (ERM) is a system or an approach to managing risks across the organisation or enterprise. More traditional risk management focuses on managing risks individually in silos. Organisations should include all internal and external stakeholders in their enterprise risk stakeholder wheel.* This is to maximise the advantage of managing risks both individually and collectively for the impact they may have on the organisation. However, this is not an ERM guide; this guide simply emphasises the importance of managing emerging risks within the organisation's ERM system. For further reading on ERM and the general management of risk, see the Airmic Risk and Risk Management Explained guide. We have provided

* The stakeholder wheel is a recognised graphical technique for capturing who is involved and how their role relates to the organisation.

the link to this document in the Further Reading section.[14] While individuals and organisations apply the term 'emerging risk' in nuanced ways, two common uses allow us to create a helpful guide for most situations, even those with refined understandings. The first use is when dealing with a risk that is new and developing for an organisation, while the risk is not new to other organisations. The second and more troublesome case to address is when a risk is new and developing without ever being managed by any organisation before.

In both cases, there is inevitably a lack of sufficient information or knowledge for the risk to be managed appropriately. As inferred by the word 'emerging', there is also a change taking place that either invalidates past knowledge or takes the organisation into uncharted areas.

Two fictitious but plausible narratives may help to explore both the common features and the notable differences in these two cases.

Illustration 1: Activities new to an organisation but known and understood by others in the world.

Organisation A has traded in fresh food for many years. It has an established market in its home country, and it understands how that market operates, but recognises limited growth opportunities. To build sales, the organisation takes the strategic decision to become a first-time exporter of its products. This decision naturally exposes the organisation to risks which are new to it and its stakeholders, leading some within the organisation to use the emerging risk label in connection with these new risks arising from the extra activity. However, exporting is not new to every organisation and there is a large body of reliable information and people with knowledge who could help this organisation identify and manage these new emerging risks. The task is therefore one of acquiring true and trustworthy information and developing reliable access to the required knowledge, drawing on the existing pool to understand and manage the risks. This is especially important in a world where misinformation can spread quickly. Misinformation is false or misleading information spread without the intent to deceive. It often happens when people unknowingly share incorrect facts, rumours or misinterpretations. (Unlike disinformation, which is deliberately created to mislead, individuals who believe something is true are the usual source of misinformation.)

Illustration 2: Activities new to the organisation and new to the world.

A small university research group makes a breakthrough in applying its established expertise in Artificial Intelligence (AI) research. From a strong background of research and sound innovation, the team creates a machine learning tool for athletic development.

Using the early version of the AI tool it had developed, the team gains data from a set of small-scale trials. These early results suggest that the tool could help people train better, with fewer injuries and faster skill development results.

As a world first, only the laboratory's own small-scale trials provide all the data that has ever existed. Knowledge about how this new technology may affect the wider population does not exist. On the other hand, availability of such an important training aid, even as a first-generation tool, is enough to generate a high level of commercial interest.

With credible claims of success, media interest and the commercial opportunity the tool offered, other research bodies and large commercial organisations can start properly financed and well-founded research studies. But trustworthy results are inevitably going to take time to emerge, and the world never waits.

In the absence of verified information, speculation and false claims proliferate. Driven by money, fame or simple delusion, people write about the technology, extrapolating the small data sets to make claims that are yet to be proven.

Organisation B, a well-intentioned sports club whose members will benefit if the technology works, would like to make the most of 'first mover advantage.'[15] However, with a rich mix of some reliable information, along with misinformation and disinformation, the emerging risks that Organisation B faces are new to the world.

While both illustrations are quite different, there are common threads for both organisations, which means both are using the term 'emerging' correctly. Both will need to follow a process to explore and source trustworthy information that can become knowledge to reduce uncertainty and drive better decision-making.

From data to strategic intelligence

We receive free access and applications daily, and online sellers now add us to marketing lists with every purchase, as if our intention was to cultivate a relationship with them rather than simply buy a product. What they want, of course, is your data, who you are, what interests you and, most of all, what you spend your money on. Left as raw data, all this data has little value, but processed and mined, organisations can turn data into information, and information is the key ingredient for decision-making. But what decisions should we make?

Here, we introduce another concept, that of knowledge. In this context, knowledge is both the information you gain, added to the information and facts you already had about how to use the new information. This may seem circular, so an example may help. If a layperson receives information that the temperature in the room is 40°C, then they conclude the room is hot. However, if a heating technician receives this information, they may conclude the room is indeed hot and the controls may require repair. Same new information, but two different levels of interpretation, based on previously held knowledge.

This is something we may identify with experience and expertise, which the technician has and the layperson does not. When we raise our game to strategic decision-making, then we move to a new level. Now, we don't just want to have knowledge to interpret what we see now. What we want is to have the knowledge of foresight to determine how the future may unfold. This is the level of strategic intelligence, and this is the level we need to manage emerging risks.[16,17]

The changing external context, slower in export markets, potentially faster with the AI research, means that even some previously accurate information may become outdated and unreliable, so that both organisations will need to keep reviewing and refreshing the knowledge they are building. On this journey, both organisations will want to make fast progress as these are commercial opportunities, but both will need to avoid taking on board misinformation and disinformation, which may lead to poor decisions. Both will need to ensure they have sufficient access to reliable knowledge to navigate the developing nature of their markets.

In reviewing the two case studies and with a little imagination, we can understand how common emerging risks are and how important they are for any organisation to manage. The illustrations also show that the emphasis and driving force for engaging in managing the threats is to realise the extensive opportunity both emerging contexts offer.

Other risk types and their labels

There are other types of risk that share some of the characteristics of emerging risks and that may therefore benefit from the techniques in this guide. However, as this is a guide for managing emerging risk, we have limited inclusions to some noteworthy examples.

Frontier risks

The widespread and developing use of technology and the connections the internet has facilitated may explain the rise in risk complexity and interconnectivity. Recognising that some technologies have led to radical change and expecting this trend to continue, the World Economic Forum (WEF) created a new label - frontier risk[18] - to define emerging risks from the newest paradigm-shifting technologies that breach new territories or shift societal forces. As an emerging risk, they are characterised by unknown likelihood, unknown impacts – or both. Such risks could manifest as an extreme version of a traditional risk or as a completely new phenomenon, and the onset could be rapid, gradual or non-linear.

Because frontier risks are a subset of emerging risks, we do not need to interpret the presented ideas separately.

High Impact, Low Probability (HILP) risks

High Impact, Low Probability (HILP) risks are rare events that may result in catastrophic impacts that are characterised by a lack of precedence, high levels of uncertainty in their predictability and combinations of effects, often coming as surprises or shocks. They may not meet defined thresholds for mitigation actions and will require innovative, creative approaches to raise awareness, leverage established capabilities, and enhance both short- and long-term preparedness. As they are of low predictability, they can be dismissed by organisation leaders as risks that affect others but not their own organisation.

HILP risks can be emerging risks but are not always emerging risks; the low probability nature of HILP risks often means they share poor information availability with emerging risks.

For example, the risk of a major bank IT failure that affects its customers' ability to pay bills is low, but not unheard of. Such a risk might surprise some, but it's not emerging, because we understand these risks and how to manage them. If a bank fails, the organisation that uses that bank may not be able to run its payroll and may then become liable for employee losses.

As with any risks, the ERM system should embrace the management of HILP risks and, with the shared characteristic of inadequate management information, the management of HILP risks may also benefit from the strategies and techniques included in this guide, along with concepts in the two other guides on Scenario Analysis and Horizon Scanning, which may prove useful.

Rising tail risks as emerging risks

Aside from discrete distributions that only have fixed values, with no graduation between discrete events, all other types of distribution are continuous. In a continuous distribution, the probability of the event occurring can take any value between two limits.

As examples, the number of sweets a child takes from the sweet jar is a discrete distribution, as the child may take one, two or maybe ten sweets, but cannot take ½ a sweet. The height of a set of children in a class, however, is an example of a continuous distribution, as any child may have any height across a range, with one child being the smallest and another being the tallest to define the range.

While a risk event may have a discrete set of outcomes, the most common distribution for risk events, across time and impact, is the 'normal distribution'. Other statistical distributions occur, and these arise from biases which favour a particular set of outcomes.

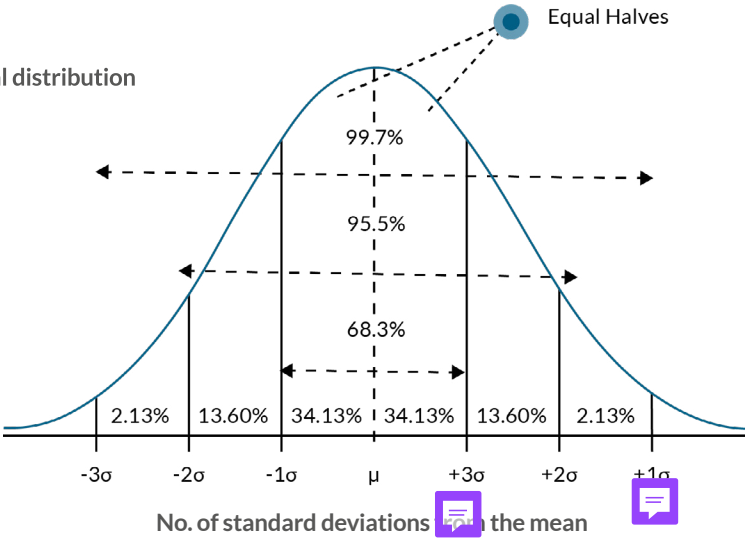
Figure 1 is the normal distribution curve, and it has several properties commonly used in statistics and the assessment of risk. The most commonly understood property is the average, which is found by drawing a line down from the very peak of the normal distribution curve. This value represents the outcome that occurs 50% of the time if an infinitely large number of events were to occur. The other property that is useful is the standard deviation, which is a measure of how much spread there is.

For example, if Figure 1 charts the height of children in a class, the mean (u) may be 1.2m with a standard deviation of 10cm. This means 99.73% of the children in that class were between the height range of 90cm (mean minus 3 standard deviations) and 1.5m (mean plus 3 standard deviations). In a risk situation, if financial losses for a risk event were on average £1 million, with a standard deviation of £150,000, then the same curve can show that 99.73% of losses will be between £550k and £1.45 million.

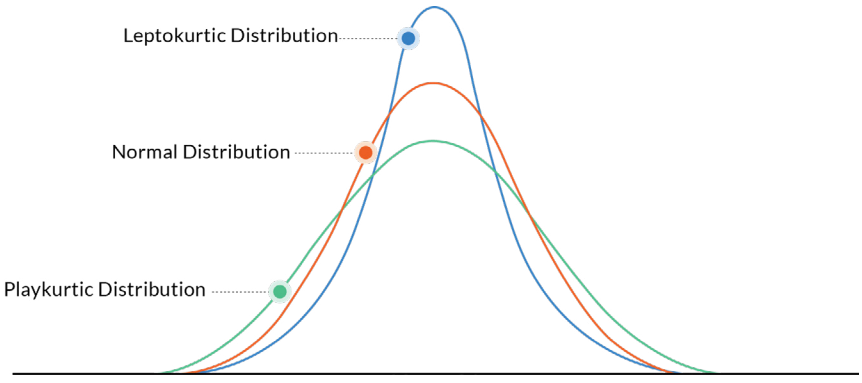
Sometimes, we find the distribution isn't perfectly normal, and the curve is either wider or narrower in the midsection. This shape difference makes the distribution's tails higher or lower than for a normal curve. Mathematicians describe this 'shape' quality of the curve as the 'kurtosis' of the curve. The issue here

Figure 1:

Shape of the normal distribution



Kurtosis



is that while the mean and standard deviation may stay the same, assessments based on an assumption that this is a normal distribution, when it isn't, lead us to over- or under-estimate the likely occurrence of extreme values. With threats and losses, the more troublesome problem is where the distribution is fatter (Platykurtic). We avoid much of this problem if we identify a 'fat tail' distribution from the start, as this allows the assessment to consider the differing kurtosis from the outset. A serious problem arises, though, when a complex change process leads to unnoticed changes in the distribution's kurtosis. An example of this is seen with climate change, where the kurtosis of weather patterns changes in ways that are not fully understood at first. This leads to communities experiencing weather that used to be seen once in fifty years, for example, occur twice in twenty years, causing additional losses and damage the community was not ready for.

A good resource for investigating and understanding different distributions used in risk management is Risk Analysis: A quantitative guide.[19]

As a further example of how these tail risk changes matter in society, Swiss Re, the international provider of reinsurance, insurance and other forms of insurance-based risk transfer, conducted a study and found that the post COVID-19 mortality rates are yet to return to pre-COVID levels.[20] In 2024, four years after the pandemic began in 2020, many countries worldwide are still reporting excess deaths. This impact appears to be independent of healthcare systems and the general health of the population. This trend is also evident even after accounting for shifting population sizes, the range of reporting mechanisms and the death classifications that make inter-country comparisons complex. There is also likely to be a degree of under-reporting of excess mortality because of limitations in the record-keeping systems used.

If these changes in tail risk occur over time, they are emerging risks either as events that we have seen before but that are occurring more regularly, or events that are new to society. We may also consider COVID-19 'new to the world', because this disease differed significantly from past diseases.

Treated as emerging risks, some strategies and techniques in this guide, along with concepts in the guides on Scenario Analysis and Horizon Scanning, may be useful to spot when tail risk is changing.

6. Including emerging risks in Enterprise Risk Management

Enterprise Risk Management (ERM) is about managing all the risks across the organisation in an integrated system. An integrated approach is important because the connected organisational environment gives rise to many interconnected emerging risks. When complex connectivity occurs, risks still need to be managed with an individual risk response, but also from a broader view, taking into consideration effects on other connected risks and how any risk response may affect the whole organisation's position.

The choices we make often create risks we could otherwise avoid, as we can always choose to follow a different path to avoid those risks. However, this cautious approach is not always the best choice, as it frequently reduces our opportunities.

For example, an opportunity for a precision engineered parts manufacturer to enter a new market is a change the organisation is choosing to make. Making that choice offers opportunity but also exposes the organisation to many uncertainties, which we articulate as risks. Some additional risks and uncertainties that matter to the organisation are unavoidable. For example, the organisation will probably need to add new members to the team, generating Human Resource (HR) activity and recruitment risks. Production may have to invest in new equipment to meet increased demands, and that new equipment may need new practices to manage safety. Delivery channels may need to change and if the new market is in a foreign country, then culture risks arise too. And we have only just touched the surface of the many risks involved with such a venture. We might easily understand some of these risks, but others will almost certainly go unforeseen and misunderstood. However, with a new venture, the organisation is also likely to add new emerging risks to the list the organisation was already facing. In our example above, there will inevitably be some emerging risks that arise in the new market environment, such as technology risks, competition risks and geopolitical risks.

While important, including all risks in an ERM system does not mean we must treat all risks the same. We must assess and manage each risk according to its uncertainty, our knowledge and the organisation's objectives. For example, a safety risk only offers the threat of harm, but a strategic risk is a complex mix of both threats and opportunities, which should be engaged with for the overall opportunity it offers.

7. Strategy under uncertainty

When integrating emerging risks into an ERM system, the key characteristic that makes them a group to be managed together is not having all the information we need to understand and manage them. Conversely, when making strategic decisions, organisations must consider emerging risks alongside established risks and objectives. In addition, regulators and ratings agencies may also require emerging risks to be commented upon as a group, as part of the organisation's risk governance process.

In developing an organisation's risk framework, this dichotomy of inclusion in decisions and treatment as a group, requires flexibility in record-keeping and reporting. Emerging risks are best evaluated against consequences and plausibility criteria, where established and understood risks are frequently characterised with a tighter assessment based on impact categories and likelihood. The trick is to have a flexible framework and process that does not force impact and likelihood assessments on risks until that level of information is available.

At the highest level of response, we can only choose one of two decision-making strategies, and that choice should be based on the level of uncertainty we have identified.

We label one level of uncertainty 'deep uncertainty'. This is where the context is complex, even chaotic, and our information base is inadequate. With deep uncertainty, the ideal choice for our decision-making strategy is one of 'monitor and adapt', as this allows for more information to be collected and options to remain open, and reduces the likelihood of a major decision error.

The alternative to 'deep uncertainty' is 'shallow uncertainty', where the context is more straightforward and our information, though limited, is actionable. With shallow uncertainty, a decision-making strategy based on 'assess and respond' will probably yield better opportunity management.

Because concepts such as deep and shallow uncertainty can be difficult to quantify, we suggest adding structure to the assessment needed to choose between 'monitor and adapt' and 'assess and respond' strategies.

A starting point may be to look at the range of uncertainty faced to consider where the uncertainty comes from.

- A lack of understanding about how the situation fits within our world view (ontological uncertainty)
- A lack of actionable knowledge (epistemological uncertainty)
- Uncertainty arising from the inherent randomness of the situation (aleatory uncertainty)

These uncertainties may also manifest as any combination of:

- Uncertainty about the impact the risk may have if the risk occurred
    - Where that impact may fall
    - How serious a threat or how good the opportunity may be
- Uncertainty around whether the risk will ever occur or uncertainty about when the risk events will occur
- Uncertainty about how to manage the risk
    - Whether risk owners can manage it with a direct response, or whether a resilience response is required
    - What level of expertise or training is required for risk owners to manage the risk

The nature and collective level of uncertainty we have for any risk should not only shape our strategy for managing the risk but also shape how we integrate the risk into our ERM system.

You can also adopt the structure in Table 1 or use it as a basis for your organisation's approach. We suggest assigning one of the following levels of uncertainty shaping the situation under consideration, as this will help decide on how to respond. [21]

Level	Description	Likely strategy choice	Uncertainty characteristics
A clear future	A single future is emerging. The path to take is clear	Simple strategy to navigate towards the future, while monitoring for unexpected changes	Predominantly characterised by understandable risks and emerging risks that are unlikely to deliver surprising outcomes
Alternate futures	A few specific futures are equally likely	Strategy relying on analytics to separate options and assess the value of different outcomes	More uncertainty: therefore, keep options open until a decision is required, or we have enough information to make a sound decision
Range of futures	Future expected to manifest within a range of distinct possibilities. No distinct, obvious outcomes are available to work with.	A cautious strategy, keeping options open where this is possible. Active horizon scanning and regular updating of scenarios to maximise understanding	Likely to be characterised by emerging risks with unpredictable outcomes and risks we may understand, but which also have deep uncertainty
Ambiguity	There is no sound basis for forecasting the future	Data will be collected and monitored. Avoiding decisions as they may limit future options. Active horizon scanning and regular updating of scenarios to maximise understanding	Likely to be characterised by emerging risks with unpredictable outcomes and risks we are yet to recognise

8. The role of Gen Z and future generations entering the workplace

In 2016, Klaus Schwab, the founder of the World Economic Forum, declared we were on the brink of a technological revolution that would:

> "Fundamentally alter the way we live, work and relate to each other."
>
> (Klaus Schwab, World Economic Forum, 2016)[22]

He sensed the transformation would be so profound that he labelled this as the fourth industrial revolution, after the electronics, IT and automated production era, widely recognised at the end of the 1960s as the third industrial revolution.

Organisations are now far less dependent on people as assembly workers. Even in small organisations and sole traders, we must be people who are multi-disciplined, IT literate and socially aware. The older generations gained these skills through post higher-education training, much of it in socially simpler times and with simpler technology. Compare this with the generation leaving higher education today, who have grown up with advanced technology in their homes and in their hands. This generation grew up with their social profile online and in their pocket. As for all the excitement around expectations for AI, Gen Z is already using these early generative AI implementations as an integrated part of their educational and lifestyle toolkit. This is the generation who will be the powerhouse of future organisations in the fourth industrial revolution.

In a recent small-scale study undertaken by Barnett Waddingham, we looked at the differences in attitude and expectations this newest generation will bring to the organisations they join. We found there are important differences across the generations, and not just accommodating but utilising these incoming strengths and fresh insights will be key if organisations are going to keep up with the speed and scale of change in this fourth industrial revolution.

Many interesting findings emerged from this small-scale study and this smaller study built upon similar research undertaken by Barnett Waddingham's benefit specialists.[23] Here are just three of the factors that emerged as general themes from a range of Gen Z people drawn from across different vocational areas.

- Although this generation readily embraces technology, they are increasingly mindful of its potential misuse and harm to society. This finding is in line with another 2024 study carried out in the same age group by the British Council. In interviews carried out by Barnett Waddingham, the dangers associated with misinformation and deep fakes were a repeated concern, voiced for all generations, including their own.

- Unlike past generations, who saw a distinction between work and personal life, Gen Z people are building on expectations that initially emerged in the millennial generation. In both the survey and in interviews, we found this new generation wants to feel valued, accepted and included in the workforce. Operationally, and given the potential insight they bring, we may soon see this need for inclusion quickening the demise of age-centric hierarchical organisations.

- An interesting finding emerged about the topic of sustainability, although in discussing the research findings, we acknowledge the language used may have affected this result. The survey and interviews showed that concern for sustainability and climate change was more natural and ethically rooted than formulaic and learnt. There was no immediate recognition of formal sustainability infrastructures such as the UN Sustainable Development Goals, but there was a personal expectation for organisations to 'do their part' and to be held accountable in issues around care for the environment, human rights and personal well-being. Organisations' recognition of and care for mental health was a powerful theme emerging from the research.

For any organisation keen to make the most of future opportunities, these are important results, because while the driver of change is socio-technological, the harnessing and the taming of technology and social change, for now at least, will still rest with humans. You can find more information on future generations in the British Council's Next Generation publication.[24]

9. Data collection

Data collection should be based on the scope of information needed to understand the risk and to drive informed decision-making. This will include, but should not be limited to, answering the following questions:

- How much impact will the risk have and in what areas if an event occurred?
- When may the first risk event occur and how frequently thereafter?
- Will the information needed to manage the risk be available ahead of the event or will this information arise in real time?
- What expertise will be required to manage this risk and do we have it in our organisation? This last question is important because emerging risks may require new skills that are not readily available, either in your organisation or anywhere.

Understanding the uncertainty distribution and assigning uncertainty levels (as shown in Table 1) helps reveal the type and quantity of information needed for sound decision-making to achieve valid objectives.

The Horizon Scanning Guide provides more guidance on assessing the information gap and the steps needed to structure your data collection. The Scenario Analysis Guide[2] provides more guidance for creating the right approach and selecting the right scenario analysis technique to apply.

As the data, information and knowledge develop, the risks, as currently understood, may fracture into several more specific risks. We can place some sufficiently understood risks, after fracturing them, onto the organisation's list of understood and manageable risks.

For example, consider an organisation that wants to export its products to a new, but safe and stable country. Initially, the organisation identifies transportation as a source of significant risks, but pre-project work to understand the issues involved allowed this high-level transportation risk to be broken down into more specific parts.

For example, risks associated with road transport and with overseas shipping, each of which needs to be managed differently. When analysed further, the organisation feels it has a good understanding of road transport risks, which are like the risks it manages for its current operations. The overseas shipping risks, however, remain 'new to the organisation', and the organisation may choose to classify these as emerging risks for the organisation. In road transport, the organisation switches to use a strategy of assess and respond, relying on its past experience, but with the overseas shipping, where it has identified uncertain areas that it is yet to understand, the more cautious assess and respond strategy is used to ensure the organisation does not make a substantively poor decision.

10. Monitoring for change

We should monitor and reassess all risks in the ERM system based on their characteristics, propensity to change and importance to the organisation. Emerging risks also need close monitoring because sharp changes in context and invalidation of previously reliable information are also characteristics, particularly those that are 'new to the world'.

For example, active diplomacy, a potential source of emerging risks, can instantly eliminate rising geopolitical threats and open up new opportunities. Equally, diplomacy can fail just as quickly, allowing the situation to degenerate into conflict. Trade tariffs are a good example of geopolitical risks that some organisations may label as emerging risks. Governments normally establish tariffs, and changes don't occur without warning; however, in volatile political environments, tariffs may suddenly affect organisations, altering the international outlook or disappearing altogether. Only by monitoring for change can an organisation ensure it remains both compliant and efficient.

11. A framework for emerging risk management

You can only manage a risk, whether emerging or otherwise, if you have identified it. ISO 31000[25] sets the process for risk management, starting with the context, both internally and externally. This crucial step precedes any risk identification phase. With the identification of emerging risks likely to affect the organisation, and with significant potential for subtle effects to stir below the easily observed surface, this context evaluation step is even more important. Practitioners often refer to these subtle effects as 'small signals', as they often have little obvious significance at first, but once recognised for what they are, become useful risk or change indicators.

Experts wrote ISO/TS 31050[26] specifically for emerging risk management; it provides specific guidance, building upon the process outlined in ISO 31000. We recommend using both standards in any ERM system.

However, standards alone are insufficient as they do not cover all the important issues, and standards do not contain detailed guidance on how to implement the processes called for. To implement risk management properly, we should employ a selection of tools, techniques and frameworks for both established risk and emerging risk management. Figure 2 provides a framework that specifically addresses both risk and emerging risk in a practical ERM implementation. The framework specifically aids in identifying, assessing impact, assessing likelihood and determining timing. A well-developed body of knowledge, accessible and applicable to any organisation, underpins each step in the diagram.

As the data, information and knowledge develop, the risks, as currently understood, may fracture into several more specific risks. We can place some sufficiently understood risks, after fracturing them, onto the organisation's list of understood and manageable risks.

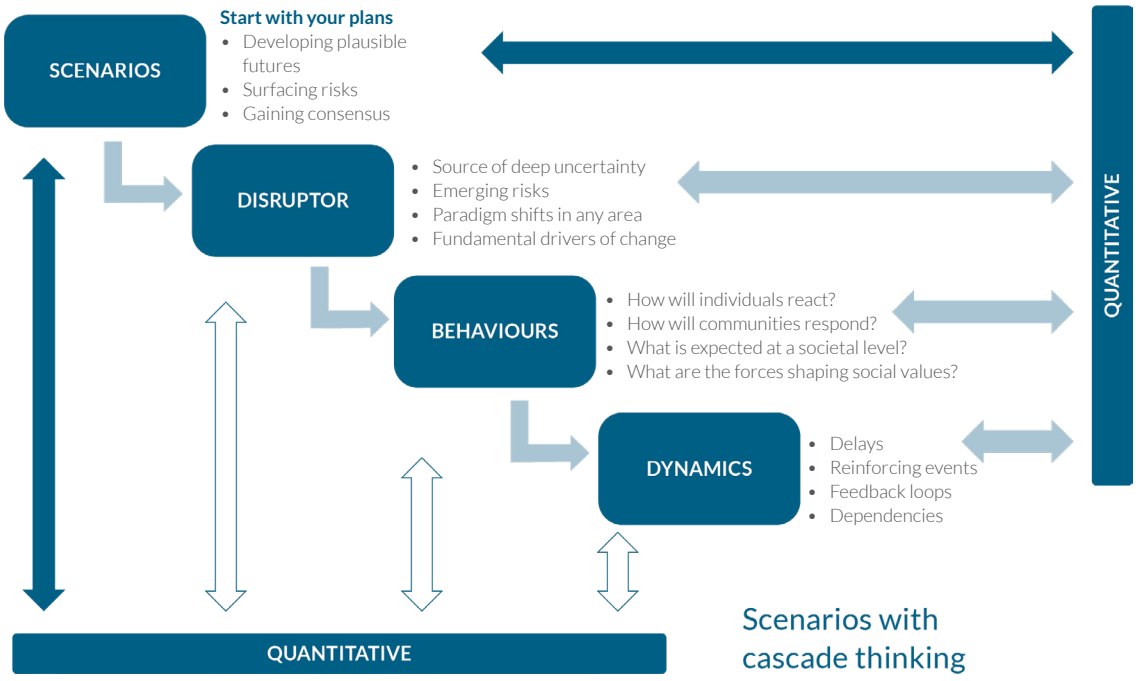


Figure 2: This framework provides for a structured approach to the assessment of emerging risks (based on original by Keith Smith)

While depicted as a cascade, treat this model as only having a notional flow from top to bottom. We expect at each stage that new information and insight will augment the qualitative and quantitative data, and this will determine the best stage to re-enter the cascade flow.

Scenarios

The starting point is with the plans you currently have. If you are not using scenarios, we highly recommend using scenarios. The Scenario Analysis Guide will help you establish and use scenarios in your organisation.

Scenarios allow relatively easy communication of complex interconnected situations and facilitate the development of deeper insight. Scenarios also help users develop a more thorough understanding of the information required for better decision-making.

Your plans, no matter how simple, are going to suggest a direction the organisation expects to take. You likely supplemented your plans with a discussion of the risks, and you may have listed these risks in a spreadsheet, database or text document. This suffices to start the process, providing a baseline scenario from which your organisation can construct other scenarios and, through them, explore the full range of plausible outcome.

Disruptions

Knowing the direction the organisation plans to take, and with the depth of contextual understanding a scenario can provide, the organisation can identify disruptive changes that may exist or be emerging within society. For example, in recent years, significant advances in machine learning have emerged, creating a mix of both threat and opportunity for all organisations. At first, particularly when people are becoming interested in the technology, media hype surpasses the actual capabilities of any technology and so an environment of misinformation clouds true insight into what is possible. Here, a hype cycle, which is a visual technique covering the adoption of technology, and a technique attributed to Gartner, may help.[27]

Hype cycles target technology, yet misinformation surrounds any type of disruption, so validation to separate fact from fiction is a necessary step.

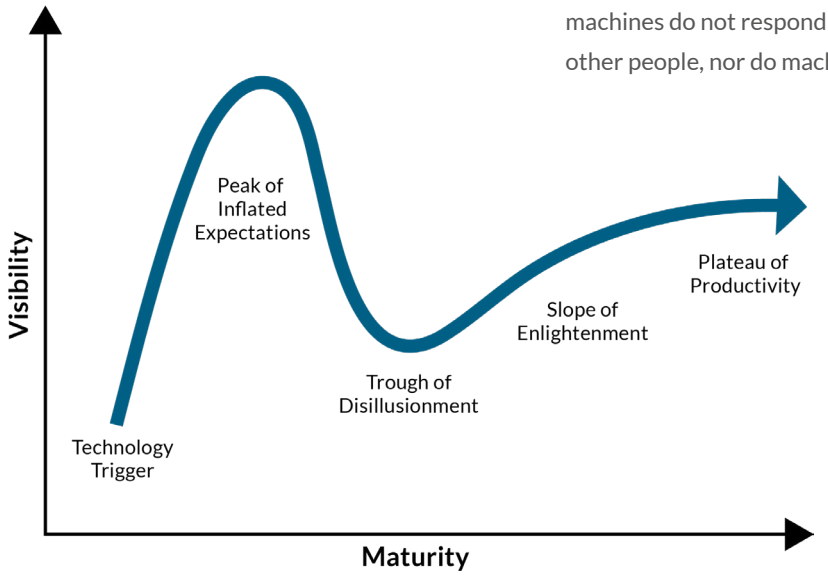


Figure 3: The Gartner hype cycle

We can avoid misinformation and disinformation, deliberately misleading information, by validating information against multiple trustworthy sources.

Once separated from the hype, misinformation and disinformation, or at least with an appreciation of the hype that may surround a disruption of any kind, the type and level of disruption to investigate is usually easy to identify. Here, the use of a structured thinking tool such as PESTLE (Political, Economic, Social, Technological, Legal and Environmental) will help ensure that identifying disruptions is relatively comprehensive and systematic.

Remember, each category in the PESTLE or any other similar thinking tool are sources of change, and not disruptions, so the aim is to develop a list of disruptive effects that apply to your organisation using each category. For example, the 'L' for Legal is an opportunity to consider risks that emerge from the legal space when considering a disruption. If we revisit machine learning as a disrupting technology: machines do not respond to the peer pressure from other people, nor do machines fear the law, so many

risks arise to ensure decisions made by machines do not run counter to accepted societal values. To identify less prominent disruptions, use foresight techniques. The Horizon Scanning Guide will be a valuable resource for evaluating disruptions, as it includes techniques for harvesting the data as well.

Behaviours

Threats and opportunities arise from how people behave in response to the changing context. Indeed, the connection between disruptions and behavioural change is so strong, if there are no identifiable changes in behaviour at the personal, social group or societal level, then the disruption is void and unworthy of attention.

Identifying and assessing behaviour changes that are yet to occur is surprisingly difficult to foresee with full clarity. Each of us has a limited world view, no matter how educated we are or how much we have travelled. Internal biases also hinder our ability to understand behaviours from a different perspective. For simplicity, we can think of any individual, even the brightest in society, as having an 'alternative mindset blindness' problem.

A good example of how this 'alternative mindset blindness' affects our ability to forecast behaviour, and an example of how widespread that blindness can be, occurred with the transition to digital mobile phones.

In the early 1990s, with the then new GSM phones becoming available, the Subscriber Identity Module or SIM card controlled the subscriber's information and billing. Unlike the analogue phones that GSM replaced, the phone itself had no personal characterisation features, all personalisation was in the SIM.

At first in some European states, it was easy to get a SIM card, with instant credit and billing scheduled at the end of the month. Criminals with a different world view than the originators of this scheme exploited the easy access to cheap SIM cards and used the cards with no intention of paying the bill. The company blocked each fraudulent card upon discovery, but this could not happen before the criminals had already sold calls to expensive international destinations. Using the same phone, the criminals replaced the blocked card with a fresh, unused card whenever one stopped working. This limited their costs to the deposit value of the cards, whereas before SIMs existed, a criminal would have to buy a complete phone.

While not an easy step to navigate, the behavioural step is very important and, done well, will allow many risks to be identified and assessed for impact. Tools and techniques associated with the discipline of behavioural economics may be helpful in this step. Of course, because we each have our own blind areas, asking others from different backgrounds to contribute broadens our view. Diversity brings benefits in many areas, but behavioural assessment is one area where they are obvious. Using ethical hackers is a good example of how engaging with people who think differently from others works well.

For any disruptive change, one should break down the behaviour changes into different levels. This is because humans show emphases of different behaviours when acting alone or in social groups, when moving from friendship groups to work teams and when acting as a public member of society.

For example, when alone in a safe environment like our home, with our favourite song playing, we might dance, sing along and even pretend to play an imaginary instrument during the best parts. Yet at work, while we may notice the same song being played, and our relationship with our co-workers may be good, few of us will burst into song, dance and strum an imaginary guitar.

While human behaviour is complex and will never fully fit into either levels or groups, without providing some structure, the task is impossible. While imperfect, we suggest the assessment of behaviours should be on the same three levels described above.

Here are those levels along with some suggested subcategories that may be relevant in some circumstances. This is not an exhaustive list of categories that may be useful, nor will each assessment need each of these categories to be considered. This list simply provides a baseline starting point for your work on behavioural assessment.

- How will people react as individuals?
    - Changes in routine
    - Changes in beliefs
    - Changes in values
- How will people behave as members of societal groups?
    - As a member of an organisation
        - Within a team (at work, within a sport or other team-orientated environments)
        - Within a work friendship group, where conversation may revolve more tightly around work issues and co-workers
        - Within a business unit
    - As a member of the organisation
    - With family
    - In friendship groups that will have attracted different degrees of loyalty and commitment
- How will people behave as a member of society?
    - As an individual in that society
    - As part of a political, religious, protest or other affinity group within society

Dynamics

Significant change within society is rarely instant. New technologies, no matter how good they are, need to gain a following. For example, while adults now have a mobile phone, in the first few years, having a mobile phone was a luxury for a select few who could afford the high costs. As more people gained mobile phones, prices came down, services and coverage improved, and adoption rates climbed. Now, nearly everyone has a smartphone, and additional issues around mental health and social bullying are emerging, which serves to illustrate the constant nature of adoption and change.

Similarly, people need time to adapt to pressures within society for social change. Scientists have known for many decades that climate change results from human activity, yet human responses range from acceptance and activism to outright disbelief

worldwide. The widespread acceptance of climate change as a real and serious problem is steadily growing, changing beliefs and behaviours, but society will never reach complete acceptance by everyone.

These behavioural changes also play out in different ways. We change our own behaviour and then expect others to change too. People struggle to understand why the behaviour of others does not follow their own. We raise our expectation that people in power, such as governments, will drive change in areas we cannot affect, and we will level judgements on those who do not think the same as we do.

Besides the hype curve, which also helps in the assessment of timing, the adoption curve shows a pattern of how society adopts things. It was originally used to describe the adoption of new food products in the 1950s, but the concepts are the same for anything a society needs to accept. These concepts can also be helpful in quantifying the economic impact of social change, as it can help estimate proportions of society who will buy into the change and when.

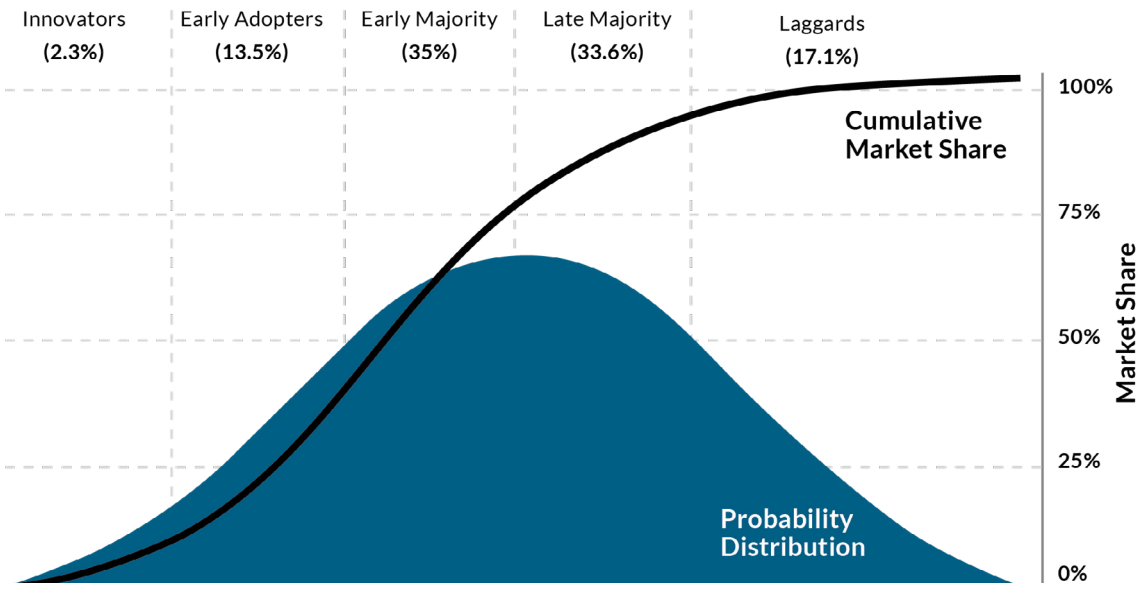


Figure 4: The product adoption curve with origins back to 1956 agricultural produce

As the future unfolds, it becomes clearer which factors and events are affecting the adoption of new behaviours. For example, a new fashionable clothing line may become popular among a certain age group, until something causes a rejection. It may be work practices, where it's found that children working in appalling conditions produce the items, or the product has a negative impact on animals or the environment. These events then create a back pressure, reducing and even ending adoption if the negative reaction is severe enough. As these factors change with time, tracking how behaviours are changing and what is changing them is an ongoing process in tracking risks.

Jay Forrester, a university professor, identified these positive and negative pressures, establishing the field of study now known as systems dynamics back in the 1950s, so there is a long history of study in this area.[28] Again, this is not a perfect science, but the use of systems dynamics will help an organisation understand the major forces involved. Understanding these forces also helps if the organisation wants to invest in efforts to hasten or slow down change.

Researchers in systems dynamics developed a simple and useful diagram method to help visualise the interaction of these pressures, enabling an estimate of the change's pace. These diagrams are called Causal Loop Diagrams (CLD).[29] Lines connect in these diagrams between the entities being influenced and the entities exerting the influence. People normally label those lines to show whether the influence is positive, reinforcing the change, or negative, suppressing it. Organisations can tailor the diagram with additional information. Figure 5 is a partial CLD for the adoption of electric cars. To be useful, a more comprehensive version would be required, but this suffices to illustrate the diagram's potential.

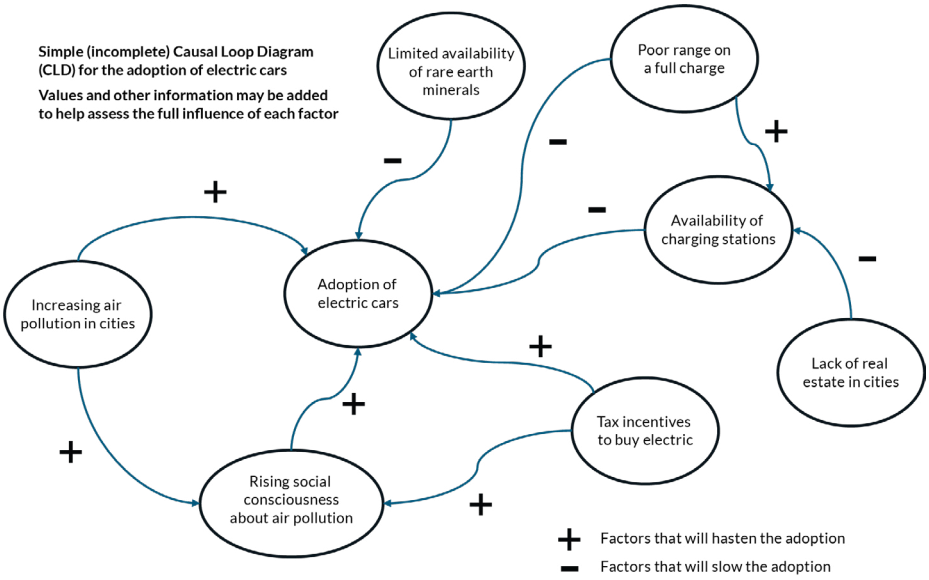


Figure 5: A partial Causal Loop Diagram

People usually keep this type of diagram in its subjective form, but an organisation can estimate the effect and use a mathematical combination method to calculate a numeric estimate of when an event will take place.

12. Bow tie diagrams and emerging risk

Bow tie diagrams originated from the field of safety risk management but have since transitioned into the mainstream of risk management because they present useful information in a clear and concise way.

The bow tie diagram's balanced nature – causes on the left, consequences on the right, and the risk event in the middle – makes it very easy to read. The addition of controls and actions connected by lines adds to both clarity and usefulness, because gaps in the control environment are immediately obvious. This generic example (Figure 6) shows a typical bow tie diagram layout.

While most bow tie diagrams show threats, with controls, actions and post-event responses to mitigate their organisational impact, the same technique can apply to opportunities.

While useful for all risks and arguably useful for opportunities, the bow tie diagram is a particularly useful technique to use when assessing emerging risks. By their nature, emerging risks are either new to an organisation or new to every organisation, as they stem from either new strategic ventures by an organisation, fresh developments in social change or technical advancements. This 'newness' quality means people are not always quick to pick up on subtle connections. Because the bow tie is such an excellent tool for highlighting gaps, its use in emerging risk management is recommended.

One other benefit to highlight in using bow tie diagrams in emerging risk management is their

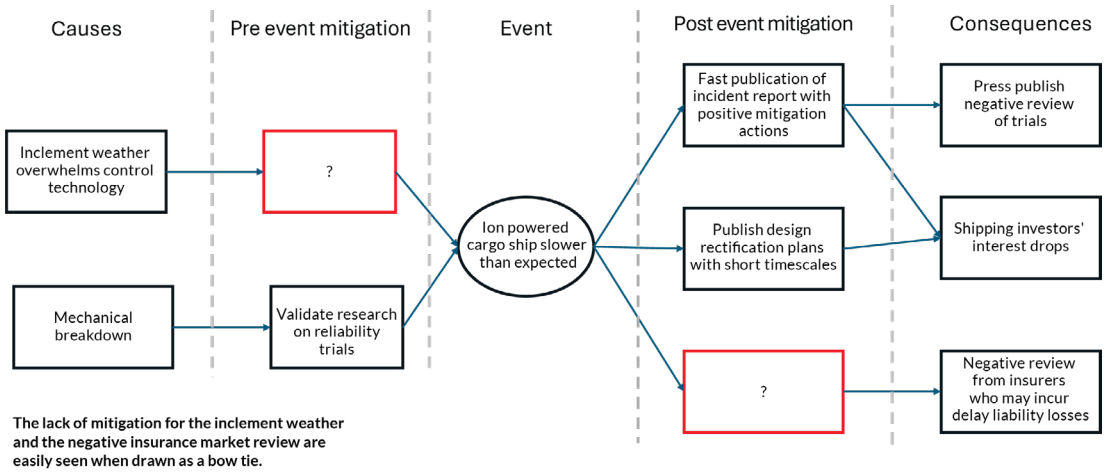


Figure 6: A generic bow tie diagram

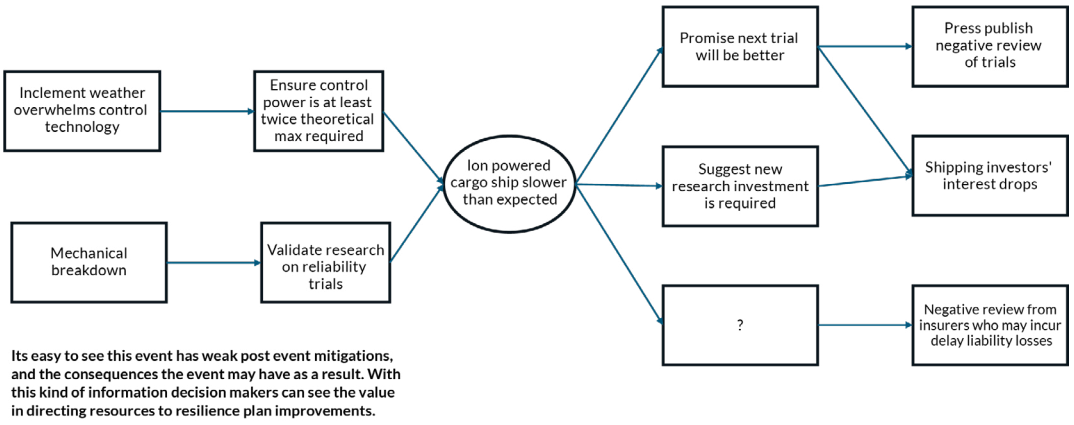


Figure 7: In this example, the weakness in resilience measures is easy to see

With these benefits, we recommend the use of bow tie diagrams across the organisation for many types of risk and opportunities. usefulness for assessing and communicating weaknesses in resilience planning. Consider figure 7 above. This threat-centric bow tie diagram shows two causes, each of which contributes to a moderate likelihood of a risk event occurring. This information alone is useful as, along with an assessment of the consequences on the right-hand side, it drives the decision-making on how much effort to invest in managing the risk.

Further examination of the post-event activities in Figure 7 reveals that current plans will not be that effective, leaving the organisation vulnerable to reputational and financial losses. With this information, the organisation has the clarity it needs to review the actions it takes, should the risk event occur, and an opportunity to assess its resilience to accept the lasting residual impact it must bear, even after taking action.

13. Insurance and emerging risk

Insurance creates value for society, and the insurance industry is developing and improving as a tool for managing emerging risks.

Insurance is a contract whereby an insurer promises to pay the insured a sum of money if specified events occur in the future. Businesses buy insurance to protect their assets and income streams; to protect the assets of the directors and officers of their organisation; to pay compensation to third parties in the event of a claim against the organisation; and, in certain circumstances, because it is a legal obligation.

Insurance offers financial protection, incentivises proactive risk mitigation, and promotes resilience across industries and communities. As insurance evolves alongside the complexities of modern risks, it moves beyond a safety net to become a dynamic enabler of recovery and adaptation, especially when it includes specialist services like those for cyber risk. Insurance also helps enable organisations to take more risk-pursuing opportunities, pushing society forward.[30] The premiums invested in the capital markets also help to finance businesses and projects that are important to society.

This section explores how to leverage insurance in this context, and further reading on insurance may be found in the further reading section.[14]

Risk transfer

Insurance acts as a financial safety net by transferring the financial burden of emerging risks from individuals and organisations to insurers. This safety mechanism empowers businesses and individuals to focus on recovery and ongoing operations rather than facing overwhelming financial losses.

For instance, consider cyber insurance. The number of cyber incidents affecting businesses continues to grow at a frightening rate, affecting ever more sectors of the economy and both large and small companies alike. No longer is cyber security concern the domain of traditional target sectors (such as financial services or data-rich businesses), as the General Data Protection Regulation (GDPR) legislation has created data management obligations for almost every business. These challenges have therefore created a significant escalation in demand for cyber insurance.

Most cyber policies cover both first-party and third-party losses. Cover for first-party losses usually includes cover for cyber crime investigations, data recovery, reputation management, notification costs and extortion payments. They may also cover business interruption caused by a cyber incident. Cover for third-party losses usually includes damages and settlements, and defence costs for claims of a breach of the GDPR. However, given the significant cyber exposures facing companies, as evidenced by the significant losses incurred by cyber insurers in recent years, the cost of cyber insurance has increased.

Parametric insurance and captive insurance

Traditional indemnity-based insurance is based on asset values, deductibles, sublimits, and policy terms and conditions. Claims are paid when assessed indemnity losses exceed the retention held by the insured, and settlement can take weeks, months or

even years, particularly when a loss involves complex business interruption situations.

Parametric insurance is 'index-based', meaning that coverage is against pre-agreed event parameters. Once the independent, verifiable index level is reached, the policy is triggered and the insurer quickly pays out the pre-agreed sums.

As the sophistication and availability of data improves, new ways of gauging risk continue to open up. While data will usually come from an independent third-party, the insurance industry is becoming more confident in using data from clients, offering new ways of indexing. Parametric insurance is no longer limited to financially sophisticated organisations, and examples of parametric solutions used in captives are also emerging.

A captive is a special-purpose legal entity licensed as an insurer and established primarily to insure a proportion of the risks of its sponsor – often a corporate parent, group, partnership or public entity. It is a risk-bearing vehicle and can be either an insurance or a reinsurance entity. In addition to being used for insuring or reinsuring the risks of its parent, a captive can be used to insure or reinsure the risks of third parties, such as customers, suppliers or subcontractors.[31]

One of the main strengths of a captive is its inherent flexibility. A well-structured captive can respond quickly and effectively to the changing demands of its parent or fluctuations in the insurance market, making it more suitable for emerging risk. A captive can adjust cover retention levels or amend insurance scope when required, offering a rapid response tool that keeps pace with change.

Risk mitigation and innovation

Insurers play a vital role in encouraging policyholders to adopt measures that reduce their exposure to risks. For example, businesses that install advanced cyber security systems or homeowners who invest in flood barriers may qualify for premium discounts. These incentives not only benefit the insured by lowering costs but also encourage proactive behaviour that minimises the likelihood and severity of emerging risks.

Insurers continuously develop new and tailored products to address the evolving nature of risks and innovate the types of coverage being offered. For instance, insurers have designed specialised insurance solutions for emerging technologies, such as autonomous vehicles, renewable energy installations and systems, or supply chain disruptions. These innovations help businesses and individuals adapt to changing risk landscapes while ensuring that they remain protected against unforeseen events.

Data and analytics

Insurers use advanced data analytics and predictive modelling to assess and understand emerging risks, but also to predict their impact. By sharing insights derived from these analyses, they can help businesses and individuals better prepare for potential risks. The emergence of Artificial Intelligence to predict cyber security vulnerabilities

and share those findings with policyholders not only enhances the service provided to clients but also creates a sense of collaboration and partnership.

This collaboration is also a strong asset when liaising with governments, industries and other stakeholders to address large-scale risks. Public-private partnerships can be particularly effective in managing systemic risks such as pandemics, climate change or infrastructure failures, developing risk-sharing mechanisms and pooling resources to provide subsidised coverage for high-risk areas.

Building resilience

Insurance is a critical tool for building resilience by providing financial support in the aftermath of adverse events. The payouts received can help businesses and communities recover faster, rebuild infrastructure, resume operations and regain stability quickly. By promoting financial stability, insurance allows stakeholders to focus on long-term adaptation to emerging risks rather than being overwhelmed by immediate challenges.

Regulatory compliance

New regulations and compliance requirements accompany many emerging risks. Insurance can help organisations manage these obligations by offering specialised policies, such as environmental liability insurance or coverage for data protection fines. This not only ensures compliance with legal standards but also mitigates financial and reputational risks.

When engaging with insurers to secure coverage for emerging risks, it is crucial to communicate as clearly as possible your understanding of the risks and demonstrate proactive measures to mitigate them. Highlight your preparedness by sharing data, outlining risk-reduction strategies such as cyber security upgrades or physical defences, and emphasising your commitment to resilience. This approach not only builds trust but can lead to better terms, such as premium discounts or tailored coverage solutions.

Collaboration is another key element: it is worth exploring opportunities for partnership with brokers and insurers, as sharing insights that can help refine insurers' risk models and help you stay informed about innovative products such as parametric insurance or specialised policies for emerging technologies. Working with brokers or specialists can provide valuable expertise, while negotiating terms and understanding claims processes ensure smoother handling of future incidents. By adapting and embracing forward-thinking strategies, companies can position themselves as informed and proactive stakeholders in managing emerging risks.

14. Reporting on emerging risk

Risk universe

Even for a small organisation, the breadth of risk, the levels of uncertainty involved and the extent of information held vary enormously. An organisation will have important but relatively easy risks to manage, such as avoiding the risk of an employee spending the organisation's money on personal items. An organisation will also have strategic and complex risks to assess, such as when to expand into new geographies or when to invest heavily in new technology.

A risk universe diagram is just a simple picture that seeks to collect all these meaningful risks, although in practice, people often omit safety risks from risk universe diagrams, so the name is not fully justified. In addition, as these are high-level diagrams, people generally draw risk universe diagrams as a diagram of risk sources, rather than of named risks. For example, a risk universe diagram may have an entry labelled 'legal' which then breaks down to subsets, for example, employment, contract, product liability, etc.

There is no single way to draw a risk universe diagram, and the format can highlight views that organisations feel are important. Some diagrams place risks into named categories such as strategic, operational, etc., but there is no obligation to do this. While there are many reasons why an organisation may draw a risk universe diagram, there are two benefits to highlight.

First, this is a subjective assessment of the main risk areas. ERM embraces holistic management of risk, so a 'map' of the risk universe is a helpful supplement to other risk information. From the perspective of emerging risk, this holistic view may help to picture which areas are likely to be affected most by emerging change. The second, more practical purpose, is to use the diagram to explore prospective decisions. Did we cover all the relevant areas?

Accommodating emerging risks in risk registers

Risk registers come in many forms and with a varied list of information attached and included in the register.

Risk registers as a topic have become contentious for the wrong reasons. When simply a list of risks that are uninformative, uncollated, unmanaged and dry, the technique can be dangerous, because people convince themselves that this is management. On the other hand, a set of thoughtfully characterised risks, collected, collated and with actively reviewed plans, is a useful tool. Not knowing the set of risks faced or relying on remembering all the risks that apply – the opposite of having an explicit register of risks – is also unlikely to help decision-makers make informed decisions.

Describing the characteristics of a good risk register is out of scope for this document. What is in scope, however, is to describe how a risk register should accommodate emerging risks.

The characteristics of emerging risks are many, but the difficulty of assigning impacts and likelihood to emerging risks is the main issue with risk registers. With this limitation, attempts to assign quantified values to categories such as cost, date of impact and

likelihood are challenging. Filling those fields on the risk register form is distracting; this alone justifies placing emerging risks in a separate register, where descriptions of potential consequences and plausibility replace impact and likelihood assessments.

The other reason to hold emerging risks as a separate set is so that the organisation can articulate its general strategy to deal with the emerging future. This may be for regulatory or for rating agency assessment, but there is value in senior management explicitly discussing this strategy without a regulatory mandate. The reason for this is that emerging risks are often indicators of high uncertainty about how the future may unfold. Without an explicit discussion, there is likely to be a divergence in how senior management perceives and leads its teams into the future.

Heat maps

Heat maps generate a lot of controversy. On the one hand, they can be useful for visualising risks by plotting the impact and probability of risks using risk criteria benchmarks on two axes creating a matrix. This simple method displays risk levels, and top management often uses it for a quick overview. However, the convenience these matrices offer can come at the cost of depth and accuracy of the data visualised, leading to potentially misguided decision-making. With emerging risks, frontier risks and HILP risks, the oversimplification required to create heat maps can lead to several problems.

With emerging risks, meaningful assignment of impact and likelihood values through quantified risk criteria measures is frequently impossible, and the effort invested is rarely worthwhile. Emerging risks are generally best characterised by a description of consequences alongside a description of how plausible the risk is.

Similarly, frontier risks, which are a subset of emerging risks, are also very difficult to assign to a risk criterion – plausibility assignments generally work better.

HILP risks, which are frequently complex, can suffer from the oversimplification of heat maps. Figure 8 shows how a threat-centric heat map collects HILP risks into the bottom right-hand corner. This category (19) is the right place for safety risks, which are treated as a special class, within an As Low As Reasonably Possible (ALARP) management strategy, but not the best place for all HILP risks to be seen and managed.

Figure 8: An example of a heat map, widely used in risk management

Instead of heat maps, or to supplement them, reports that have either a page or half a page dedicated to each significant risk can provide decision-makers with much better-quality information. Using this alternative approach, we can show a risk's impact and likelihood, its consequences and plausibility, and a more detailed synopsis for the management of HILP risks.

Risk connectivity diagrams

One driver identified in both the rise of emerging risk as an area to be managed and as a factor that can make managing emerging risks difficult is the connectivity between risks. Connectivity means that when one risk event occurs, it changes the environment in ways that change the profile of other risks.

A risk connectivity diagram is not just useful for the risk team as an internal way to look at risk. An appreciation of how risks interrelate is important for decision-makers at every level.

Figure 9 is an example of a risk connectivity diagram. It is a simple diagram, but its importance lies in facilitating and promoting an investigation into how each of these risks influences other risks. This helps make informed decisions.

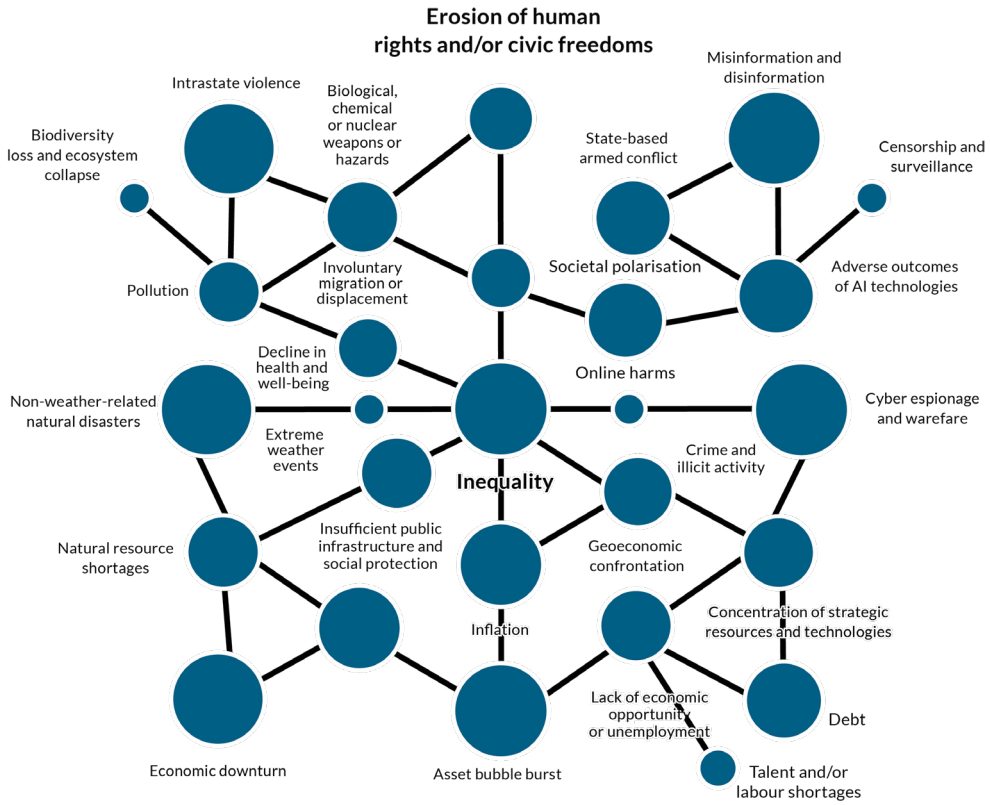


Figure 9: Risk connectivity is an important factor to consider when making decisions

Scenarios

We make no apology for revisiting scenarios under this heading of reporting. Reporting on risk is about informing decision-makers, and scenarios are great communication tools.

Scenarios need not always be lengthy reports and, often, especially for reporting, we can build scenarios around two simple axes, with the horizontal axis representing one aspect of the problem being explored and the vertical axis representing another.

Figure 10 is an example of a simple, two-axis scenario approach that may work for reporting. This two-axis format promotes a well-focused discussion, and discussion helps ensure that a sound decision emerges. The danger, of course, is that it's also a good way to make misinformation and disinformation believable, as it takes on a sense of certainty when presented this way. So, validating the assumptions being made is important with any risk, and recognising that information may become invalid at some later date is additionally important when discussing emerging risks.

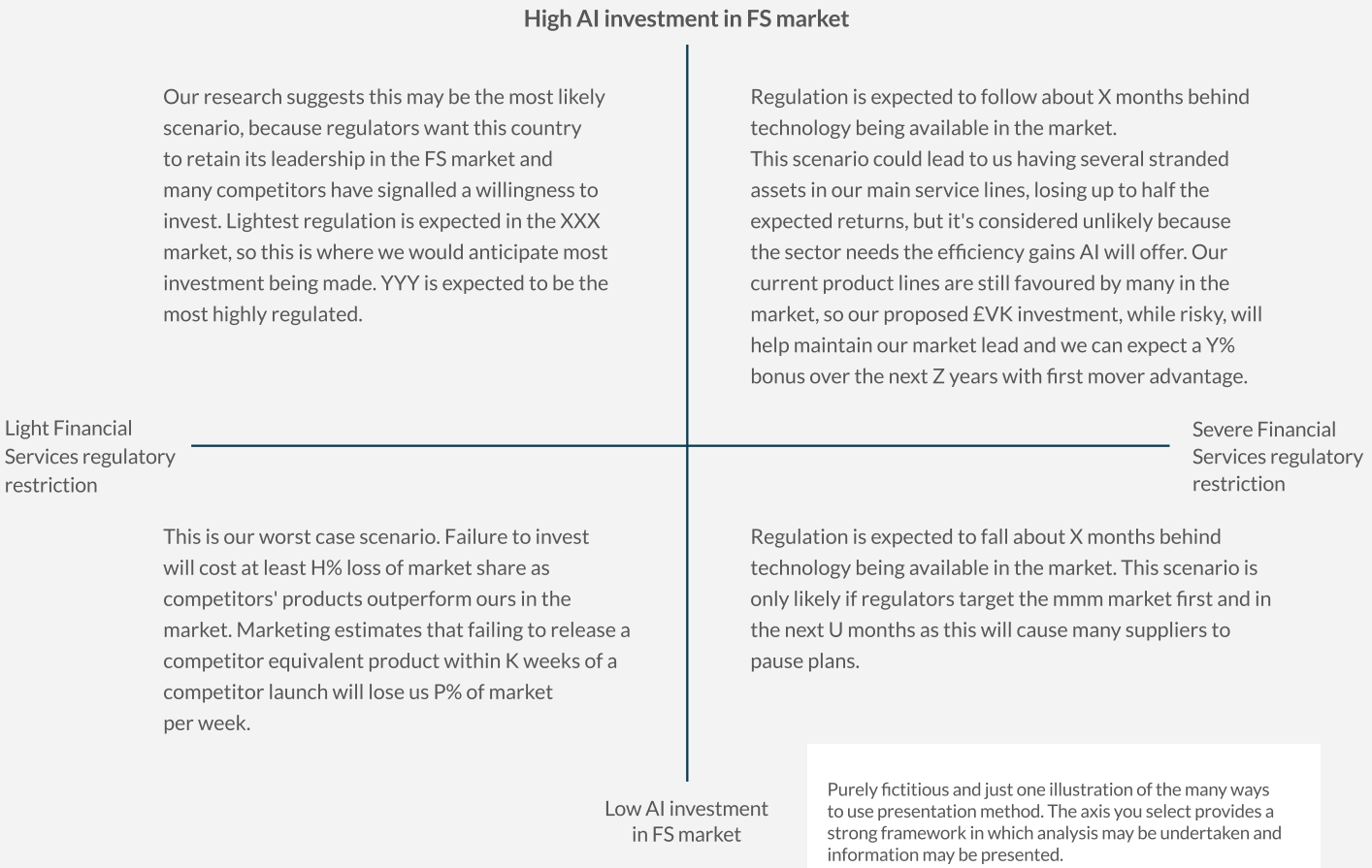


Figure 10: A purely illustrative example based on a fictitious analysis

15. Decision-making under uncertainty (taking action)

Collecting good-quality information is only worthwhile if your organisation can use it to make better decisions. It is surprising how many organisations cannot, or do not, use the information they have available when making important decisions. These are some of the common mistakes that are made:

- The organisation has good information but doesn't fully understand how to leverage it.
- Someone possesses information, knowledge or even strategic intelligence, but others exclude them from the decision-making process.
- Those involved in the decision lack training in decision-making under uncertainty; such decisions are their responsibility, but they may not have the requisite expertise or experience.

We can address the first mistake by investing in analytical and interpretation skills. This investment may need to be in analytical technology but is often more likely to require investment in skills training and knowledge development. Many people in decision-making roles only have basic data analysis skills. It may also be the case that people with good data analysis skills exist within the organisation, so the skill required by others may simply be one of analytical literacy.

The second problem requires the organisation to reflect on what matters. Problems such as this arise, but they simply shouldn't.

The last is a recognition of a common problem. Few organisations invest in developing decision-making skills and, in the past, when decisions were easier to make, this may have been justified. That time has passed, and decision-makers need to develop skills in decision-making.

Here are a few considerations that decision-makers may find helpful when making decisions. You can find further guidance in the risk management handbook by Kogan Page.[32]

Which strategy should we adopt? Should we monitor and adapt, or do we have enough information for rational choice between options?

Does the decision have to be made at this point in time? This is not a licence to pontificate, but it's a valid question, as sometimes the later decision may benefit from new information.

- Is there sufficient information to make a valid decision? Few decisions benefit from complete information. For most other significant decisions, there is still a threshold below which a decisive choice between options is little more than a guess.
- Is the decision affected by biases? This challenge is easier said than done, as we are often unaware of our biases. If time allows, validating the decision with others can help counter personal biases.

- Is the right person deciding? And this is not a question of seniority, but one of appropriateness based on a combination of information access, knowledge and expertise. If a decision needs to be made in real time because the key information will arise in real time, consider the expertise and preparation that is required by the decision-maker.

- Based on research undertaken on real-time decision-making by incident commanders in the fire service,[33] applying the three decision tests below, before implementing the decision, also improves the quality of the decision taken. These tests are valuable whether the decision is to be made in real time or after longer consideration. It is, however, acknowledged that it may not be possible to apply these tests in fast-moving real-time situations, which is when the organisation needs to be thoroughly confident in the expertise of the decision-maker.

1. How do we expect the decision to change the future?

2. Will the decision limit future options?

3. Is the benefit worth the investment of resources?

Applying these three retrospective questions before implementing the decision will help reduce decision-maker remorse.

The further reading section[34] includes further information on the important subject of decision-making under deep uncertainty.

16. Closing remarks

Managing emerging risk is strategic, difficult and, as with any risk, dependent on the information you have. Whether it's because the risk is new to your organisation, or new to the world itself, the challenge with emerging risk is gaining the data, translating that into information and building the knowledge to apply that information to where you can rightfully claim to have strategic insight or strategic intelligence.

Central to managing emerging risk are the information and knowledge-building steps, carried out in an environment where that data and information may not yet exist, may be inaccurate or may even change in its relevance. Our recommendation for managing this dynamic situation is to use horizon scanning and scenario analysis as features of your emerging risk management system. Whether the scenarios you use are complex, quantitative reports or simple qualitative 'shared stories' around specific issues, scenarios facilitate the sense-making environment most people need to make the most of the information they have.

Although this guide does not cover it, risk governance remains critically important to the management of all risks, including emerging risks. We would recommend that organisations download and follow the recommendations in the Risk Coalition's work on Risk Governance 'Raising your game'. The further reading section contains a link to this document.[35] In addition, experts have refined the UK Corporate Governance Code over many years, and many of its principles are worth reading, even for organisations not bound by its requirements. We have also included a link to this in the further reading section.[36]

In any substantial subject, no single guide is definitive, but we hope this guide contributes value by framing the issue, offering insights into managing uncertainty, and providing a practical framework for information collection and analysis.

References – For further reading

This is a guide for practitioners and decision-makers. For this reason, we have avoided standard styles of academic referencing, and we have sought to include easy-to-read, internet accessible articles, rather than lists of fundamental academic literature. However, rigour remains important, and the articles chosen are from trustworthy sources, some of which were peer reviewed in academia. We made this choice for readability, and users of this guide can be assured that its concepts are based on knowledge established through rigorous academic and industrial practice.

1. **The origins of diversity, equity and inclusion:** https://www.thisisdei.com/blog/dei-origins-how-diversity-equity-and-inclusion-evolved
2. **Airmic Guide (with Barnett Waddingham and ORIC):** https://www.airmic.com/technical/library/scenario-analysis-practical-guide
3. **Airmic Guide (with Barnett Wadingham):** https://www.airmic.com/technical/library/horizon-scanning-practical-guide
4. **Herbert Simon. Bounded Rationality:** https://link.springer.com/chapter/10.1007/978-1-349-20568-4_5
5. **Socio technical origination. Trist and Emery**: https://www.tandfonline.com/doi/full/10.1080/14697017.2018.1553761#d1e191
6. **GSM SMS.** http://www.gsmhistory.com/vintage-mobiles/
7. **Trust in International Trade:** https://www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf
8. **World Bank originates the term ESG:** https://www.thecorporategovernanceinstitute.com/insights/lexicon/what-is-the-history-of-esg/
9. **Rise in litigation over environmental damage:** https://www.lawgazette.co.uk/practice-points/beware-the-rising-tide-of-environmental-and-human-rights-litigation/5121968.article
10. **Stranded assets: https:**//www.annualreviews.org/content/journals/10.1146/annurev-environ-012220-101430
11. **Obesity increasing globally:** https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(23)02750-2/fulltext
12. **Cyber Risk Code of Practice:** https://www.gov.uk/government/publications/cyber-governance-code-of-practice
13. **Cyber Essentials:** https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
14. **Airmic EXPLAINED Guide (with Marsh):** Risk and managing risk: https://www.airmic.com/technical/library/explained-guide-risk-and-managing-risk
15. **First mover advantage:** https://www.emerald.com/insight/content/doi/10.1108/jbim-03-2021-0165/full/html
16. **Managing innovation. Data to strategic intelligence:** https://www.iso.org/standard/72621.html
17. **Knowledge management standards:** https://www.iso.org/standard/68683.html
18. **WEF use of frontier risks:** https://www.weforum.org/stories/2021/06/frontier-risks-identifying-early-warning-signs/

19. **Risk Analysis. A quantitative guide:** https://www.amazon.co.uk/Risk-Analysis-Quantitative-David-Vose/dp/0470512849
20. **Swiss Re 'post event' impact of Covid-19:** https://www.swissre.com/institute/research/topics-and-risk-dialogues/health-and-longevity/covid-19-pandemic-synonymous-excess-mortality.html
21. **Levels of uncertainty:** https://hbr.org/1997/11/strategy-under-uncertainty
22. **The fourth industrial revolution:** https://www.weforum.org/stories/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
23. **Barnett Waddingham benefits study:** https://www.barnett-waddingham.co.uk/comment-insight/research/benefits-trends-for-2025/
24. **Next generation research:** https://www.britishcouncil.org/research-insight/next-generation-uk
25. **25. ISO31000:** https://www.iso.org/standard/65694.html
26. **ISO/TS 31050:** https://www.iso.org/standard/54224.html
27. **Gartner hype cycle:** https://www.gartner.com/en/research/methodologies/gartner-hype-cycle
28. **Origins of systems dynamics:** https://systemdynamics.org/origin-of-system-dynamics/
29. The basics of drawing Causal Loop Diagrams: https://thesystemsthinker.com/causal-loop-construction-the-basics/
30. **Airmic EXPLAINED Guide (with Arthur D. Little and QBE):** Risk Appetite: https://www.airmic.com/ technical/library/explained-guide-risk-appetite
31. **Airmic EXPLAINED Guide (with Artex):** Captive insurance: https://www.airmic.com/technical/library/explained-guide-captive-insurance
32. **Risk Management Handbook, Kogan Page:** https://www.koganpage.com/risk-compliance/the-risk-management-handbook-9781398610613
33. **Applying quality control tests before implementing a decision:** https://www.cardiff.ac.uk/stories/ improving-decision-making-in-the-emergency-services
34. **Decision making under deep uncertainty:** https://www.sciencedirect.com/science/article/pii/S0040162521003711
35. **Risk Coalition. Raising your game:** https://bw.riskportal.app/resources/raising-your-game
36. **The UK Corporate Governance Code:** https://media.frc.org.uk/documents/UK_Corporate_Governance_Code_2024_a2hmQmY.pdf

airmic

Marlow House
1a Lloyd's Avenue
London
EC3N 3AA
+44 207 680 3088
enquiries@airmic.com
www.airmic.com