Royal Academy of Engineering

Building resilience:

lessons from the Academy's review of the National Security Risk Assessment methodology

Foreword

As engineers, we look to understand the systems around us, and their components, and to consider what could possibly go wrong. The critical next step is to discuss how we can make it better: to identify the layers of protection and mitigations that can be put in place to reduce risk. Safety and security are paramount, especially where there is potential for casualties, loss of life, and environmental damage. Engineering systems haven't always been safe; we've learned from tragedies and continuously seek to design safer systems and improve our practices by creating a culture that is open about near misses and enables others to learn from them too.

Assessing risk at an engineering plant or global company is inherently different to assessing the risks facing a country. However, by taking a systems approach to the review, and taking the time to really understand the different user perspectives, we have been able to exchange ideas and good practice from different domains and provide recommendations to strengthen our national risk assessment methodology.

This review has been an opportunity to learn from a diverse range of industry sectors, academia, and government. Through these conversations and case studies, we have been able to draw out crosscutting themes, such as facilitated collaboration, the active exploration of uncertainty, transparency of assumptions, and openness to challenge from different perspectives. These themes are woven through the Academy's seven **principles for good practice**.

The principles can be considered for use by others, including industry, to test their risk management processes, training, and dissemination of the information in their organisations. Consideration of the case studies, and how they relate to alternative situations, will bring insights from different perspectives.

Implementing these principles will not necessarily be easy, as risk, resilience, and organisational culture are closely intertwined. With the lived experience of the COVID-19 pandemic, now is the time to foster a resilience-oriented culture that drives action to make the UK a safer, more prepared nation for everyone.

I'd like to thank the Academy policy team, the project quorum, external reviewers, and all of the contributing stakeholders for enabling us to bring together such a comprehensive analysis of the National Security Risk Assessment methodology and well-evidenced proposals for improvement. We stand ready to help bring the experience of engineers to the business of implementation.

Professor Joan Cordiner FREng FRSE
Chair of the Royal Academy of Engineering NSRA Methodology Review Quorum

Contents

Executive summary

The Academy is the UK's National Academy for engineering and technology. It provides progressive leadership for the engineering community and delivers independent expert advice to government built upon the knowledge within our Fellowship and networks.

In January 2021, the Cabinet Office's Civil Contingencies Secretariat commissioned the Academy to undertake an external review of the methodology behind the National Security Risk Assessment (NSRA). The NSRA outlines and assesses the most significant risks facing the country and informs plans to mitigate those risks. This report sets out the lessons learned from an engineering perspective on the UK's risk assessment methodology.

Risk assessment is highly interdisciplinary, and we believe there are valuable lessons that our engineering review can contribute. Engineers are trained to examine complex systems, assess risks and their propagation, and construct systems for safety and resilience. Building upon the Academy's existing work on risk and resilience[1] and our Fellowship's cross-sector experience, we examined a range of practices from industries such as nuclear and chemical and explored a breadth of risks close to engineering, from cyber threats to flooding. Through case studies and interviews with major private and public sector risk owners, we drew out lessons relevant to risk owners of all types and focused on techniques for scenario design, exploring interdependencies, and building organisational resilience. Through this research, we developed a set of **principles for good practice** that direct organisations to employ a joined-up approach to risk assessment that strengthens resilience in practice, helping to build toward the government's goal of "making resilience a national endeavour, so that as a country is we are prepared for the next crisis, whatever it might be".[2]

The NSRA is the government's biennial assessment of the top hazards or threats that could feasibly cause significant harm and disruption to the UK. It is developed through a cross-government exercise that collates information on what reasonable worst-case manifestations of these risks might look like and assesses their likelihood and potential impact. Government departments and local resilience forums then use this information to create response plans and build response and recovery capabilities.

Resilience describes the ability to anticipate, assess, prevent, mitigate, respond to, and recover from hazards, threats, disruptive events, and civil emergencies.

Lessons from the review

Scenario-building techniques can be used to actively explore uncertainty. These techniques are invaluable in understanding the broad impacts of risks, allowing for more strategic, least-regrets planning. Scenario-building methods such as 'red teaming' and 'grim storytelling' can help identify different facets of risk, help overcome individual biases, and build decision-making capability for managing risks as they arise and change. These techniques often use participatory exercises and workshops that may be accessible to many organisations.

Methods used to explore interdependencies highlight the links between risks, identifying cascades or unforeseen secondary impacts, which can then be mitigated against. Many of the interdependency case studies in this report rely on modelling and data analysis, which may require specialist skills; however, interdependency mapping can also be achieved through participatory exercises that bring together a diverse set of stakeholders. These exercises reinforce relationships between stakeholders outside of crisis times for better resilience and emergency response. Furthermore, they encourage stakeholders to consider interdependencies more widely in their work.

By defining a risk appetite and fostering a culture of resilience thinking, organisations can begin to manage uncertainty itself rather than specific manifestations of risk. Joined-up approaches that look at the whole system are needed to engage with interdependencies and strengthen links across the risk and resilience landscape. However, embedding a joined-up approach across an organisation requires buy-in from stakeholders and may require significant resources.

Call to action

We are calling upon all those with a stake or responsibility in risk management to reflect upon the extent to which the following principles for good practice are incorporated in their risk assessments, and to act upon them. All organisations, both in industry and government, need to consider how their risk assessment processes translate into action and prepare them for a broad range of impacts. Risk assessments should be clearly communicated to and challenged by diverse stakeholders so that dependencies and vulnerabilities can be identified, understood, and planned for, increasing our societal resilience to a wider range of risks.

Principles for good practice

1. Ensure a joined-up approach

Building a shared understanding of risk and resilience activities across organisations can provide opportunities for collaboration so that prevention and mitigation strategies deliver greater resilience than individual actions.

2. Encourage participation and communicate clearly

Collaboration is critical when building networks for fast response to emergencies. Bringing diverse stakeholders together can help identify interdependencies, groups facing disproportionate impact, or cascades of consequences that one person, team, or department alone might not anticipate.

3. Focus on impact

Decision-making should be driven by impact and preparedness – linked to capability across prevention, mitigation, response, and recovery – with less focus on likelihood.

4. Explore interdependencies

By bringing together risk owners from different parts of the system with a variety of experiences and expertise, interdependencies can be uncovered and planned for that may not be revealed when risks are assessed in isolation.

5. Consider a range of scenarios

Considering multiple scenarios can help with robust planning and in identifying a range of different response capabilities that might be needed. It also supports the exploration of cascading risks and consequences with systematic impacts.

6. Embed new data and metrics

Data is vital in informing likelihood and impact assessments, providing early warnings, and in monitoring unfolding emergencies, but confidence in the data must be high and models must be carefully evaluated and paired with real-world information.

7. Review based on need

The timeline for assessing risks should be set based on need – how sensitive those risks are to technological and societal changes – rather than on a standard time interval. Assessments should be responsive to any change in the provision of mitigations, and reviews should incentivise long-term planning.

1. Introduction

Organisations manage risk every day, and those risks evolve as society, technology, and the environment all change. In an increasingly interconnected world, local, national, and global disruptions can have unforeseen impacts that can be challenging to prepare for. This report aims to address these challenges by bringing resilience to the heart of the risk dialogue. It highlights examples of good practice in risk assessment from across sectors and proposes a set of **principles for good practice** that organisations can use to build resilience into their assessment practices.

This report builds upon an earlier review, conducted by the Academy, of the methodology behind the government's NRSA (see Context, below). In producing that review, we built a deep understanding of risk assessment practices through developing case studies and interviewing risk owners from a broad range of industries. This report draws together the evidence and lessons learned from the review, showcasing examples of good practices relevant to all those who play a role in assessing, managing, and responding to risk across industries, government, and beyond.

Within the broad field of risk assessment, the evidence presented in this report focuses on (1) good practice in relation to scenario development, (2) interdependency mapping, and (3) embedding resilience thinking. Each of these three themes is explored in detail through case studies, discussion, and consideration of their key takeaways. The remainder of this section gives a brief overview of each of these themes.

Context

Building on our report *Critical capabilities: strengthening UK resilience*,[1] the Royal Academy of Engineering was commissioned by the Cabinet Office's Civil Contingencies Secretariat to undertake an external review of the methodology behind the 2019 NSRA. The NSRA is "a classified document which lists and assesses the impact and likelihood of the most serious risks facing the UK and its interests overseas".[2] It is produced in conjunction with all risk-owning departments and agencies. The Civil Contingencies Secretariat, part of the Cabinet Office, is responsible for coordinating the biennial production of the NSRA and the public-facing *National risk register* (NRR).[3] The NSRA and NRR facilitate critical risk management and contingency planning at national and local levels, providing an evidenced picture of risk that aids decision-making and proportionate provision of response capabilities.

The methodology used to produce the NSRA has evolved over time. The Academy examined the methodology used for the 2019 iteration of the NSRA, making recommendations for application in the 2021/22 NSRA cycle. The review focused on several key themes: scenario design; concurrent, compound, and interdependent risks; assessment timescales; and cross-cutting issues such as the use of data, diversity and inclusion, and processes for input and expertise. Our review of the 2019 NSRA methodology took a user-centric approach to ensure that any proposed changes would best meet user needs; the review methodology is outlined in Annex II of this report. The understanding we built of the 2019 NSRA through this approach is outlined in Annex III, while the specific recommendations we gave for the NSRA are given in Annex IV, respectively. Many of these recommendations were implemented for the 2021/22 NSRA cycle.[4]

Actively exploring uncertainty through **building scenarios** is invaluable in understanding risks and the breadth of their impacts, allowing for more strategic, least-regrets decision-making. Scenario development can be used to build decision-making capability for managing risks as they arise and change. Analysis of near misses, 'foresighting', and horizon-scanning methods can be brought together to build a picture of emerging risks and to identify trigger points for mitigating action. The case studies in Section 2.1 of the present report show how methods such as red teaming and grim storytelling can help identify different facets of risk and help overcome individual biases.

The case studies in Section 2.2 illustrate the benefits of techniques that are used to bring stakeholders together to **understand interdependencies**. These methods help to raise awareness of the links between risks, build relationships between stakeholders, and identify disproportionate impacts or cascades of consequences that one person, team, or department alone might not be able to anticipate. They further encourage stakeholders to consider interdependencies elsewhere in their work. Interdependency mapping exercises can also assist when considering how chronic and acute risks may interact or potentially compound each other.

To consider resilience holistically, it is not enough to simply understand a risk and its different possible manifestations. This understanding must be translated into action across prevention, response, mitigation, and recovery to reduce vulnerabilities at all levels. The **resilience thinking** case studies in Section 2.3 explore how organisations define a risk appetite and build collaborative cultures that embed resilience in their thinking, preparing to manage uncertainty rather than specific manifestations of risks.

Building upon this evidence, this report identifies seven **principles for good practice** in risk assessment, presented in Section 3. These principles are designed to be applicable to risk assessment methodologies across all sectors and to aid organisations in evaluating their current practices. They are given alongside implementation considerations for risk owners looking to act upon them. In addition, we present an **alternative approach**, in Annex I, that considers how all these principles might be brought together holistically. We include a **call to action** for these principles to be embedded in organisational risk practices to improve resilience.

2. How is risk managed?

Risk management is an established discipline. A range of qualitative and quantitative approaches for exploring the risk of threats and hazards are in use across industry, academia, and in public policymaking. Our review of the 2019 NSRA specifically examined challenges pertaining to scenario design, mapping interdependencies, assessment timescales, the use of data, diversity and inclusion, and the processes for input and expertise. We explored these challenges through a set of 17 case studies (Case studies 1–17) which were identified and developed through structured interviews, expert input, and desk research. Each case study is context specific, often developed for a particular purpose or to answer specific questions. Together, they gave valuable insight into the application of different methods and the lessons that had been learned in practice. The following sections present these case studies under the themes of **building scenarios**, **understanding interdependencies**, and embedding **resilience thinking**.

Building scenarios

'Scenario building' describes a suite of techniques used to develop ideas of what might happen in the future.[5] In the case of risk assessment, scenarios are useful in identifying risks and exploring uncertainty, consequences, and interdependencies. Often, scenario work focuses on realistic but extreme, or worst-case, scenarios – terms that are defined by the specific user or organisation. For the 2019 NSRA, building reasonable worst-case scenarios (RWCSs) is an integral part of the methodology. Scenario building is also an established part of other countries' national risk assessments,[6] and is used across industries, organisations, and industrial processes too. Scenarios provide context to manifestations of risk and are used to quantify the impact and likelihood of those manifestations for comparison. They are not, however, predictions and are often subject to significant uncertainty.[7]

In addition, scenarios are used as foresighting tools to explore uncertainty, from user design testing through to the future-proofing of infrastructure.[8,9] They can be used to help refine strategic thinking or as the basis of practical exercises, such as wargaming, to test skills, experience, and the ability of decision-makers to respond to future threats. This section explores effective applications of scenario building through case studies under three themes:

Decision-making and uncertainty
Case studies 1, 2

Beyond the foreseeable
Case studies 3, 4, 5, 6

Exploring variation
Case study 6

Following the case studies and examples, a set of **key takeaways** for scenario building is outlined, including the benefits, challenges, and limitations.

Decision-making and uncertainty

Scenarios used to support decision-making are often represented by two 'axes of uncertainty' – typically, likelihood and impact – and presented as a matrix. To ensure this matrix is meaningful, the uncertainty of each axis needs to be clearly defined.[10] Defining uncertainty should be an exploratory process: first, identifying the wide range of internal and external uncertainties, and then prioritising those that may pose the most significant opportunities or risks.

Questions such as "What are the drivers of change?", "Which drivers are most important?", "What do the axes of uncertainty need to communicate?", and "Who is important?" may be useful. It can be helpful to ask decision-makers to define what is important, or to explore what would cause the greatest regret, and adjust the focus of this activity accordingly.

Robust scenarios often pull together significant amounts of data and sometimes use modelling to project into the uncertain future. However, looking beyond the present situation may require expert input and carefully defined scenario boundaries when examining variation across future pathways. With both modelling and expert input, it is crucial to ensure assumptions, limitations, and biases are well understood in order to give confidence in the validity and value of generated scenarios. Case studies 1 and 2 both demonstrate methods for building detailed scenarios that help future-proof decisions by creating business cultures that recognise uncertainty, enabling long-term strategic and least-regrets decision-making.

Case study 1 – Shell Scenarios
Shell Scenarios have been developed as a tool with which to envision the future. They stretch individual and organisational thinking by asking "What if?" questions that test the boundaries of their thinking. The scenarios are a bank of plausible but challenging descriptions of potential futures, developed through extensive engagement with a diverse set of experts, that are intended to support strategic decision-making and ensure a balanced and resilient view at times of significant yet uncertain change.[11] These scenarios are developed based on the business need; understanding the purpose and types of decisions the scenarios inform, as well as the timescale, is viewed as crucial. For example, three long-term views, up to 2100, focus on energy and climate change. Shorter-term scenarios have also been produced following key events, such as COVID-19, to explore the dynamics of the crisis and to ensure that the business maintained a balanced view for decision-making.

Case study 2 – National Grid ESO Future Energy Scenarios
National Grid Electricity System Operator's (ESO's) Future Energy Scenarios (FES) presents four scenarios for energy demand and generation from now to 2050, highlighting the range of credible pathways for the evolution of the UK energy system and informing many processes, including low-regrets decision-making and network investment decisions, at the national and local levels.[12] The four scenarios present a range of progression toward net zero, exploring variation across "speed of decarbonisation" and "level of societal change" parameters. They are based on a combination of top-down and bottom-up modelling that draws together a broad range of data sources and extensive stakeholder engagement and open consultation to reflect the market view, societal trends, policy, and technological trends that are likely to affect energy demand and supply.

Beyond the foreseeable

In a fast-changing world, it can be challenging to imagine those scenarios for which there is no historical precedent. Where the risk is distant, extreme, or difficult to imagine, methods used to think about risk and build preventative, mitigative, or response capability need to consider optimism bias to ensure it is avoided.[13,14] Techniques exist to facilitate these discussions and explore the limits of imagination. For example, disaster scenarios can be developed by drawing on an understanding of the whole system and exploring the impacts of a failure at key points, as described in Case study 3. Alternative scenario outcomes can also be explored through "What if?" analysis (see Case study 6).

Case study 3 – KPMG realistic cybersecurity scenarios

This assessment of cybersecurity risk was carried out to help an insurance provider understand and manage their exposure to a systemic risk of cyberattack. It was used to inform decisions on diversification of their insurance portfolio (reinsurance) and ensure confidence that, if a major, systemic cyber event were to occur, the financial reserves of the insurance company would not be exceeded by the cost of the damages. Severe but plausible 'realistic disaster scenarios' were developed from seven generic cyberattack routes. They explored what could go wrong and the resulting impacts, as well as focusing on points where risk might aggregate. Different assessment methods were used, depending on how far reaching the threat was perceived to be. Predictable threats were mathematically modelled based on past events and the effectiveness of the controls that were put in place. Logical but unrealised threats were explored with a creative brainstorming process. Severe and unpredictable threats were explored based on impact and response.

There is also evidence that scenario-based training and learning can support rapid knowledge transfer between different roles, improving planning and response capability.[15] Developing scenarios is a means to understand risk and uncertainty, but also to develop a particular skillset and practice for crisis management – as exemplified in Case study 3 and Case study 4.

Case study 4 – Grim storytelling

'Grim storytelling' is a structured imagining of narrative, real-time situations in which all options available result in a negative or undesirable outcome. Through brainstorming, focus groups, analysis of past events, and creative exercises to stimulate lateral thinking, decision-makers explore what could have been done differently, and how the risks and benefits would have changed. This immersive process is intended to be carried out in short, regular sessions to encourage interactive learning and enable people to make decisions when faced with the unexpected and incomplete situational awareness.[16] Throughout, it is important to maximise the utility of narrative learning, leveraging ambiguity and uncertainty in scenarios to push learners to gain novel insights and expand their 'experiences' – increasing the repertoire they can draw on in the 'real world'.

While developing and exploring scenarios, it is important to remain aware of people's cognitive biases. Individuals and teams can have biases, beliefs, and flaws in logic that can lead to key information being missed or dismissed, leading to flawed decisions. Red teaming is an approach to assist teams to stress test and uncover those biases and limitations, as outlined in Case study 5.

Case study 5 – Red teaming

'Red teaming' is the application of a range of creative and critical thinking techniques to complex problems.[17] A 'red team' has the objective of subjecting an organisation's plans, programmes, and assumptions to rigorous challenge. It provides an independent and structured scrutiny that can enable a thorough analysis of the facts and lead to more informed decision-making. This approach can help uncover biases, challenge assumptions, identify flaws in logic, widen the scope, identify alternatives, and stress test plans. Techniques can be adapted to the project, but often include phases of information gathering, sense-making, decision-taking, and planning.

Exploring variation

Scenarios can be a useful tool to explore alternative futures; however, it can be challenging to capture all possible variation and uncertainties will inevitably remain. Providing structure to how uncertainty is explored allows for a systematic way to ensure that the different variables are considered and to sense-check scenario outcomes. One example of this is through "What if?" analysis, described in Case study 6.

Case study 6 – 'What if' analysis

"What if?" analysis is a specific example of red teaming. It uses systematic, multidisciplinary team activities and structured brainstorming to identify "What could possibly go wrong?" and the associated consequences. "What if?" analysis begins with a problem statement and then imagines the losses and gains that may result. From these, associated risks can be identified and evaluated based on their relevance and balance.[18] This type of analysis is a well-established technique in the chemical industry, used to identify major issues and encourage a conversation about the acceptability of the risk.[19]

Nightingale Hospital in the Manchester Central Convention Complex © thisisjude.uk 2020

Key takeaways

In many organisations, scenarios are a critical tool used to bring stakeholders together and to consider uncertainties. The case studies in this section present different uses of scenarios, depending on the questions that need to be answered and the complexity of the problem. Across the case studies, several key takeaway messages have been identified, as summarised in the following table.

Benefits	Challenges and limitations	Considerations for scenario development
→ Generating multiple scenarios enables low-regrets and strategic decision-making where there is uncertainty. They can also encourage indicators of change or triggers for action to be monitored as a situation evolves over time. → Scenarios provide a way to explore uncertainty in different dimensions and come to a collective opinion about what is important. → They are a mechanism to bring together different stakeholders with different perspectives to explore the breadth of impact. This can build a culture of understanding about the uncertainties and provide scrutiny of implicit assumptions. → Developing scenarios can be a mechanism to upskill responders as building an understanding of what could possibly go wrong can enhance decision-making capabilities in times of crisis.	→ Robust scenarios can be resource intensive, requiring large amounts of data and expert elicitation. → Where data is unavailable, the results may be perceived as unrealistic. → The number of scenarios explored can result in user assumptions about whether one is more probable, or whether these represent the only likely variations of futures. → In order to encourage exploration, likelihood is not typically considered as part of scenario development. In fact, for a detailed scenario, it may be almost impossible that it would occur in that exact form.	→ What is the purpose of the scenario? What decisions will they inform? → How will different parameters affect the outcome? → Who should be involved? → What challenge, external input, and review can be brought in to ensure the scenarios are robust and to minimise risk of groupthink? → How can the scenarios inform preparedness and response capability? → Where should the scenario boundary be drawn? Can interdependencies be considered?

Understanding interdependencies

Hazards and threats do not exist in a vacuum. Interdependencies exist across all systems, in the form of physical, digital, geographical, or organisational links that enable the transfer or sharing of risks, failures, or mitigations.[20] Interdependencies may be simple – for example, between the production and the availability of raw materials – or highly complex, such as between raw material availability and geopolitics. Interdependencies are a precondition for cascading risks[i] or unintended consequences. An understanding of interdependencies is critical for organisations seeking build resilience. Interdependencies may exist:

- between risks – for example, rainfall may trigger flooding and landslides
- between systems – for example, flooding may hinder transport services, or electricity outages may affect communications networks
- between response capabilities – for example, emergency services provision depends on transport services and communication networks
- across the wider consequences – for example, disruption of transport services may disrupt the provision of goods, or fatalities may cause public outrage.

Linkages between systems, such as between different utility services within a city, can lead to substantial complexity.[21] Risks may occur simultaneously, build cumulatively, or cascade. Hazards may be related to each other through:[22,23]

- triggering relationships – one hazard directly triggering other hazards; a series of triggering relationships can form a cascade or domino effect
- amplification relationships – one hazard changing the risk landscape and thereby increasing the probability of other hazards occurring
- compounding relationships – where hazards that coincide in space and/or time have an impact greater than either one in isolation.

Any two hazards or threats may be connected by any combination, all, or none of these relationships. The analysis of interdependencies is still developing, with the British Geological Survey finding that limited literature or practice exists for assessing multiple hazards ('multi-hazards').[23] However, within the existing literature, a range of qualitative, semi-quantitative, and quantitative multi-hazard assessments have been carried out, with examples found in civil and structural engineering or for critical infrastructure such as energy.[24]

This section outlines several methods used to understand interdependencies through pragmatic case studies developed through interviews with practitioners to share insights and identify lessons. These techniques include:

Network mapping
Case studies 3, 7

Interaction frameworks
Case study 8

Impact modelling
Case study 9

Bayesian networks

Interdependencies and data
Case studies 10, 11

Scenarios and narratives

Following the case studies, the key lessons for analysing interdependencies are outlined, including the benefits, limitations, and challenges.

i These terms are defined in Annex V – Glossary

Network mapping

An interdependency map can be built by identifying links between components in a system and establishing the nature of those relationships. Dependencies and interdependencies between risks or underpinning infrastructures can be mapped collectively, using techniques such as design structure matrices, and through workshops, as used in studies mapping infrastructure interdependencies in cities.[21] Network maps can also be built using databases, or using evidence gathered through a survey exercise, but this requires assumptions to be made where data isn't available. In Case study 7, a layered network-of-networks map was created based on available data on the UK's infrastructure networks. Once a map has been developed, it can be analysed to identify risk clusters or vulnerabilities. These can then be assessed using probabilistic approaches, or quantified using techniques such as Monte Carlo simulations.[25]

Network maps can also be used as a model for testing failure and impact under different conditions or events. For example, modelling can be used to map the propagation of single-point failures through the network map to assess the risk of cascading failures. This can draw on performance and failure data for system components, or on assumptions; for example, by considering worst-case scenarios, as illustrated in Case studies 1 and 7.

Case study 7 – Resilience study for the National Infrastructure Commission

A study was carried out for the National Infrastructure Commission to identify vulnerability characteristics in the architecture of the UK infrastructure network and to develop a model to assess their relative importance.[26] This model was designed to provide tools to identify locations and assets at greatest risk to help identify opportunities to reduce network vulnerabilities, enhance resilience, and evaluate the effectiveness of these options. A 'hazard neutral' approach – looking at the impacts irrespective of their cause – was taken to look at all single-point failure events in electricity and digital communications networks and their propagation into other networks, including water, rail, and road. This model was also used to explore vulnerabilities under future scenarios, such as different electricity profiles by 2050, and to examine the conditions for large-scale disruptions. As there is a lack of available data on the interdependencies between these networks, notional links had to be made between network assets to capture the physical and cyber dependencies. In most cases, the links from one asset toward another were created by assuming connections based on proximity.

Interaction frameworks

Hazard interdependency matrices are qualitative or semi-quantitative approaches used to examine the relationships between hazards. Relevant hazards within defined boundaries – for example, geographical boundaries – are identified and their relationships are examined and put into a matrix to communicate the interactions and influences between hazards. The matrices often draw on a mix of multidisciplinary information, including historical data, modelling, interviews, and workshops, to bring in expert knowledge and experiences from those on the ground. Quantification and probabilities can be included, although this may be limited by the data and modelling available.[27] Only a small number of regional hazard interactions studies exist, with one example given in Case study 8.

Although creating these frameworks can be viewed as resource intensive, understanding these links is vital to understanding the risks and making informed decisions. Part of the value of the process is the convening element, bringing together different groups and perspectives to the discussions.

Case study 8 – Regional frameworks, with application to Guatemala

This study examined the potential for interactions between natural hazards, such as earthquakes and landslides, at a regional scale in Guatemala.[28] The study brought stakeholders together, fostering coproduction and dialogue to encourage stakeholders to think outside of their silos and to embed the results of the study into their relevant organisations. The potential interactions between hazards were documented and qualified as triggering or increasing the likelihood of another hazard. These interactions were identified by drawing on literature, analysis of case studies in civil protection bulletins, interviews, field visits, and through workshops. This evidence was analysed and presented in a matrix. This methodology added value by embedding thinking about interdependencies into diverse organisations through including them in the process.

© BP

Impact modelling

Hazard impact models are frequently used in meteorology to produce impact forecasting. These models draw on risk algorithms that bring together hazard, vulnerability, and exposure to assess what the impact of a particular hazard or multi-hazard might be. The UK's Natural Hazards Partnership and the World Meteorological Organization have produced guidance and frameworks for multi-hazard impact forecasting.[29,30] An example is the UK Met Office's vehicle overturning model, which is described in Case study 9.

A hazard impact model draws on data describing the hazard and data on geography and vulnerabilities – including population data and transport networks, for example.[31] Above a certain threshold at which the hazard is deemed significant, local data from within the area of exposure can be drawn upon to produce a more detailed measure of vulnerability, or the extent to which area is likely to be impacted, providing a forecast of impact severity. Different hazard scenarios may be run through the model to produce a measure of risk based on their differing levels of impact.

Bayesian networks

'Bayesian networks' are quantitative probabilistic models that map interdependencies between elements and assign a numerical weight to each relationship as a means of quantifying the dependency. They have been used to examine supply chain risk, environmental risk, and patient safety and diagnosis, for example.[33,34,35]

Bayesian networks have been proposed as a method to examine cascade failures or assess the failure probability of a component in the network caused by a cascade. Like any model, the challenge with Bayesian networks lies in determining the conditional probability or probability distribution assigned to each relationship. These can draw on data and probability modelling or expert elicitation to assign a numerical weight to the relationship between events. Many techniques exist to elicit auditable and replicable estimations from individual experts.[36] These processes can be supported by a degree of automation, as is possible with the use of algorithms, machine learning, and databases.[37]

Case study 9 – Met Office weather warning system

The Met Office warning system is used daily to provide weather risk warnings across the country. It informs local responders and the public of weather-related risks in order to enable preparation and response. Probabilities of an event are modelled and tested with scenarios to provide a relationship between probability and impact level. Interdependencies – in particular, concurrency – are considered through modelling and expert elicitation. Alongside meteorological data, other data sets, such as demographic and traffic data, are used to feed into impact models that generate impact probabilities; for example, for the risk of a vehicle overturning based on the wind direction or the traffic profile on roads at different times of day. Close collaborative relationships with local responders and partners bring in local knowledge and enable expert assessment of likely and worst-case scenarios and key uncertainties; for example, those caused by flooding, or location-specific concurrent events such as a mass gathering, or a significant number of heavy vehicles parked at Dover because of Brexit-related border closures. This more subjective qualitative information is brought together with the objective quantitative model to produce a warning level.[32]

Interdependencies and data

Data, in all forms, is vital for understanding risk, likelihood, and impact. Understanding interdependencies can help uncover new data sets that can be used to fill gaps (eg using health indices and postcodes to complement data sets from primary care). Live data can be used to develop real-time risk indicators, as demonstrated in Case study 10; however, consideration should be given to the readability of the data, the behaviours that it could drive, and the implications for compound or concurrent risks. Data can also be an important tool when trying to identify those who will be disproportionately impacted by different risks, as will be demonstrated in Case study 11.

Scenarios and narratives

Interdependency maps and methods can be challenging to communicate, especially where there is high uncertainty and complexity. Several visualisation techniques have been proposed to facilitate communication and decision-making.[21,41] Furthermore, scenario building is a valuable tool with which to explore interdependencies. Narratives from scenarios can support discussions about interdependencies and deliver value for participants as they collaboratively identify and assess interdependencies. In cases in which lots of appropriate data is available, models can be employed to explore several scenarios, analyse networks, and investigate the propagation and impacts of risks throughout a system.

Case study 10 – COVID-19 population risk assessment

NHS Digital developed the COVID-19 Population Risk Assessment, building on the University of Oxford's QCOVID risk prediction model, to provide a data-driven approach to identify populations at the greatest risk from COVID-19.[38,39] Oxford conducted the research using the Q research data set of seven million people.[40] Implementation on a national scale brought together wider data sets for population representation, including data from GPs and secondary care settings. Where data was missing, a huge amount of work was conducted to fill gaps where possible. Where gaps remained – for example, ethnicity or BMI data – the precautionary principle was applied to ensure patients at risk were not missed. A review process was also put in place to identify clashing data. Risk factors were drawn from first-wave COVID-19 infection and hospitalisation data and peer-reviewed research. A real-world feedback loop enabled performance evaluation and model iteration for improvement.

Key takeaways

Risks should not be examined in isolation; interdependencies, vulnerabilities, and subsequent cascades need to be considered in order to really understand their potential impact. These case studies present several different methods that can be used to understand interdependencies, depending on the availability of data, the purpose of the model, and, critically, what decisions it will inform. Across the case studies, several key takeaway messages have been identified, as summarised in the following table.

Benefits	Challenges and limitations	Considerations for interdependency mapping
→ An increased understanding of interdependencies and possible compounding and cascading effects is critical to inform decision-making. → The process of bringing stakeholders together to map interdependencies, although resource intensive, provides value by raising awareness and encouraging stakeholders to consider interdependencies more widely in their work. → Where the process breaks down silos by bringing together different perspectives, the understanding of the risk and effectiveness of mitigations can be improved.	→ Interdependency mapping and analysis is resource intensive, complex, and may be limited by availability of data. → It is important to clearly define boundaries for interdependency mapping to manage complexity and acknowledge limitations or assumptions in the mapping.	→ What question is the interdependency mapping answering? What decisions will be made from the analysis? Which systems and boundaries should be explored? → What data is available? How should additional data be collected? Which method or combination of methods would be appropriate (qualitative, semi-quantitative, or quantitative)? → Who should be involved? → How can the process deliver most value? → What are the limitations and assumptions? → How could the outputs be best communicated and used?

Resilience thinking

Risk assessments typically identify, evaluate, and prioritise risks based on their likelihood and impact. Coordinated action can then be undertaken to minimise the likelihood or impact.[42] However, across sectors and organisations, there is a movement away from discrete risk assessment and toward creating a holistic culture of resilience. Holistic approaches to risk management bring together prevention, mitigation, response, and recovery across the entire risk assessment cycle. Rather than being purely defensive, this is about building capabilities in learning, agility, and adaptability to respond to threats and hazards as they evolve.[43] Resilience thinking is a more risk-agnostic approach: taking a systems view, designing resilience into the system, ensuring critical services can remain operational in times of stress, and considering capacity for recovery.[44]

The case studies in this section offer a view of how industrial, government, and academic organisations approach risk assessment and the tools they use to do so:

Industry
Case studies 11, 12, 13, 14, 15

Policy and planning
Case studies 16, 17

Some common themes appear across the industry case studies: the use of multiple methods to analyse risk and vulnerabilities, data-driven models, triggers for action, expert elicitation, a well-defined risk appetite, the use of scenarios, and visualisation tools.

Following the case studies and examples, the key lessons for considering resilience holistically are outlined, including the benefits, limitations, and challenges.

Industry

Different industries use a range of complex quantitative and qualitative techniques to assess risks and to identify opportunities to reduce those risks, whether it is investment in equipment, establishing a suite of emergency measures, redesign, or increasing insurance premiums. Together, these measures define the industries' risk tolerance, which is regulated to be low in sectors such as chemical and nuclear, as explored in Case study 12 and Case study 13, respectively. Examples taken from the insurance industry and the oil industry are given in Case study 11 and Case study 14, respectively. Case study 15 explores the 'bow tie' visualisation tool that is often used to communicate risk in these industries.

Case study 11 – Insurance industry[45]

The insurance industry uses likelihood and impact of risks when assessing the probability of a loss occurring within a given period. This informs risk management, including controlling exposure and portfolio approaches. Risk assessments draw on data, models, scenarios, and expert input to assess exposure to risk, 'realistic but extreme' scenarios, and magnitude of losses. Each of these components has pros and cons – the key is the ability to pool them and deploy them appropriately to answer the specific question at hand. To manage uncertainty, different models are used to model the same risk to identify gaps and quantify a range of uncertainty. The process will vary depending on the insurer and on the nature of the risk being assessed. For risks such as car accidents, there is a lot of past data to inform assessments, whereas long-term or infrequent risks, such as climate change, pose a greater challenge and require specialist modelling. The market comes together to prioritise emerging risks and monitor trends. Underwriters can keep an eye on trends and escalate what they hear from clients on the ground, while risk functions carry out horizon-scanning exercises and literature reviews to identify areas for further investigation. Regulators can also encourage action and form part of an important feedback loop in the aftermath of a hazard.

Case study 12 – Chemical industry

Risk assessments are carried out at chemical plants to reduce the risk to employees, the environment, the public, and the business from accidents caused by any number of triggering events. The risk is assessed in terms of what could possibly go wrong regardless of the trigger; for example, irrespective of whether the trigger is a hurricane or equipment failure. 'Layer of protection analysis' (LOPA) considers the measures in place that either prevent an event from developing in severity or mitigate its consequences and impact.[46] LOPA is designed as a simplified risk assessment method, a middle ground between full quantitative assessment and qualitative assessment that can be used for prioritisation for more in-depth assessment of serious risks.[47] LOPA explicitly considers the preventative layers, protective layers, and emergency response capability. These processes inform risk management practices, including mitigations and preparedness for both the plant and the local area.

Case study 13 – Nuclear industry[48]

The UK nuclear industry takes a risk-based approach to regulation. Several techniques are used to maximise safety; these begin within the design process, where considerable effort is expended to achieve passive safety and intrinsic security. 'Design-based accident analysis' is then used to discuss possible but very unlikely accident sequences that were not fully considered in the design process. Probabilistic methods and consequence assessments are used to look at the effectiveness of the safety measures in place to protect operators and the public against such accidents and to demonstrate the fault tolerance of the facility. The consequence assessments inform risk management practices, including mitigations at design and operational levels and preparedness. The cumulative risk is calculated across the site to demonstrate compliance to the 'as low as reasonably practicable' principle.[49]

Case study 14 – Data-driven monitoring system to manage well integrity[50]

Real-time pressure, temperature, and fluid flow data from hydrocarbon wells is brought together into a single colour-coded display to understand the potential risk of well failure, to inform the priority actions for planning and maintenance, and to see progress over time. The traffic-light warning system is used to provide clarity for the people who need to act; when the warning light is red, shut-in of the well may be required. Compound risk is also considered; for example, if multiple wells in close proximity show an amber warning, then the risk is considered high enough to warrant well integrity investigations and possible shut-in. A grey colour is used to signify where there was not enough data to make an assessment – this is to encourage action to be taken to find out more information. Bringing together multiple data sets allows higher value metrics to be produced, with more granular information sitting under each colour warning so that the sources of concern can be identified. Review timelines for integrity assessment are used to encourage timely reporting and ensure enough attention is given to all wells, including those that appear to be functioning well.

Case study 15 – Bowties

Visualisation tools can be effective in communicating complex risks. 'Bow tie analysis', illustrated in Figure 2.1, is one risk visualisation tool used in high-hazard industries. It depicts pathways from the causes of an event to the consequences. It is useful for creating a shared understanding of the mitigations that are already in place to reduce the likelihood or impact of the risk.[51] The bow tie method is used to illustrate risk analysis in the Norwegian Directorate for Civil Protection's 2019 *Analysis of crisis scenarios* report.[52] In the report, it is used to describe a timeline for the course of events and it captures the triggering event, the range of cascading effects, and the associated vulnerabilities. It also provides an assessment of the level of uncertainty about the event occurring and the consequences.

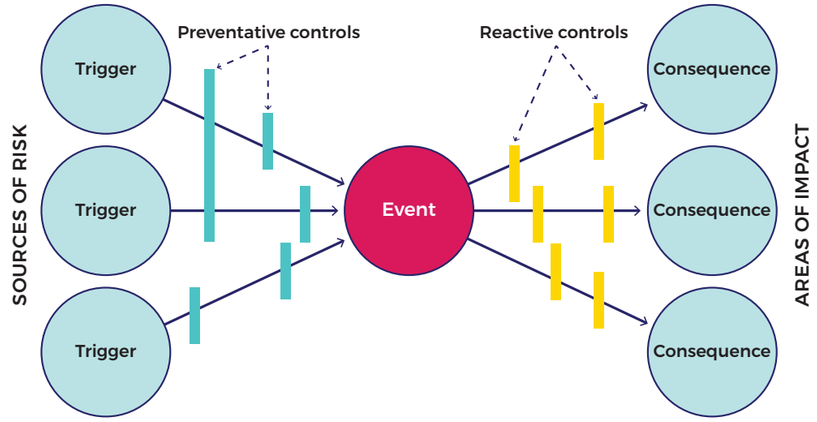


Figure 2.1 | An example of a bow tie visualisation. Adapted from *Risk management – risk assessment techniques, British Standards Institution* (2nd ed.)[53]

Policy and planning

Beyond risk assessment, organisations are building resilience-driven cultures, moving away from assessing the likelihood of certain events and toward being prepared for the unknown, with Case study 16 an excellent example.

Case study 16 – Thames Estuary 2100 (TE2100)

The TE2100 plan sets out an adaptive strategy for managing tidal flood risk in the Thames Estuary over the next century. To manage uncertainty over the century, the strategy makes recommendations for a number of possible climate futures, with a decision-making framework to encourage planning for a wide range of resilience actions. These include improving flood defences, but also nature-based solutions and sustainable land use management.[54] The plan brings together evidence to outline a flood management strategy and implementation plan that spans a large range of stakeholders and clearly attributes ownership between the national and local levels. The strategy identifies trigger points that prompt action and/or review. It is internationally recognised as a leading example of a climate adaptive strategy that enables policymakers and practitioners to plan, monitor, and review how to adapt to flood risk over time.

In risk assessments based on likelihood, high-likelihood annual events inevitably draw more attention. Resilience-oriented theory aims to address this limitation by starting with the assumption that all future events are unexpected. Framing risk in alternative ways is proposed to provide a means of stress testing plans and assumptions; for example, using an impact–capability matrix rather than an impact–likelihood matrix, or focusing on possible impacts of a threat or hazard and then considering how well a system can respond to it. Frameworks for resilience-oriented theory are still in development, as shown in Case study 17.

Case study 17 – Resilience-oriented theory

Resilience-oriented approaches assume that future events are inherently unexpected, contrasting with more traditional risk approaches that focus on the risk of what is more likely to happen in any one year.[55] As such, they focus on resilience and preparedness against unforeseen events, with much ongoing research converging toward this approach. For example, in 2020, a series of round-table discussions were held to bring together senior professionals in government, industry, and academia.[56] These round-tables provided an environment in which to explore the impacts of stresses on infrastructure systems, interdependencies across infrastructures, how organisations would respond, and the cascading effects of decisions made in response. They included testing the concept of using an impact versus capability-to-respond matrix, rather than using likelihood as the main way to prioritise attention.

To apply resilient thinking, and to increase the resilience of societies, Karin de Bruijn et al.[45] proposed the following set of principles should be implemented in the context of extreme weather events:

- adopting a systems approach
- looking at 'beyond-design' events, which push infrastructure beyond the conditions it was designed to withstand
- building and preparing infrastructure according to the 'remain functioning' principle
- increasing recovery capacity by looking at social and financial capability
- remaining resilient into the future.

Key takeaways

Embedding resilience thinking into risk management helps increase preparedness for the future. The case studies in this section present approaches taken by different industries to consider risk, prevention, mitigation, and response more holistically so that they may identify actions that will improve the resilience of the system and highlight where data and visualisation can enable this. Annex I **details an alternative approach with which to embed resilience thinking at the heart of risk assessment**.

Benefits	Challenges and limitations	Considerations for resilience thinking
→ typically a collaborative process. → action-focused to reduce risk and build resilience. → provides frameworks to manage the inherent uncertainty of risk. → takes a broader view of the future and doesn't discount risks based on probability or likelihood.	→ resource intensive, both in terms of people and data. → regulators are often used to set a risk appetite and hold actors to account. → requires culture change to embed resilience thinking.	→ How can the risk be understood in enough detail? What timeline is most relevant for the purpose of the risk? → Who needs to be part of the conversation? Would external facilitation be beneficial? → How would risk and resilience be brought together? What capabilities would be required for prevention, mitigation, response, and recovery? How would proportionality be determined? → Are principles needed to encourage consistency across different risks? How might that be communicated? → What is an appropriate review timeline? How can changes in the risk be captured? → Do there need to be clear triggers for action? What data needs to be collected? How should these be conveyed? → Who might be disproportionately affected? Are any additional measures required? → How can a joined-up cross-organisational approach be implemented with transparency, collaboration, governance, and ownership?

3. Principles for good practice

Bringing together the evidence collected on scenario building, understanding interdependencies, and resilience thinking, key lessons were identified for the assessment of complex risks. These lessons were distilled into seven **principles for good practice**, presented here, with applicability to all risk assessment, risk management, and resilience endeavours.[ii]

This section explores the rationale behind each of these principles and considers how they may be successfully implemented. The principles are:

1. Ensure a joined-up approach

2. Encourage participation and communicate clearly

3. Focus on impact

4. Explore the interdependencies

5. Consider a range of scenarios

6. Embed new data and metrics

7. Review based on need

We call upon all those with a stake or responsibility in risk management to consider how these principles may be applied within their own organisation, and to act upon them.

ii These principles build upon a set of specific recommendations presented in the Academy's review of the 2019 NSRA methodology, which are given in Annex IV

1. Ensure a joined-up approach

To be well prepared for future emergencies, the interconnected nature of risk and resilience needs to be considered holistically. Changes or decisions made about risk appetite affect resilience and vice versa. Effective feedback loops should be put in place to ensure that the dynamic nature of risk and preparedness is accounted for.

Where a risk or impact spans the responsibility of multiple organisations, teams, or individuals, it is critical that they are all involved in characterising the risk in order to understand the breadth of potential consequences and cascades. Building a shared understanding of risk and resilience activities across organisations can provide opportunities for collaboration so that prevention and mitigation strategies deliver greater resilience than individual actions. This will also build important relationships and networks that can be called on in an emergency.

Many risks need to be assessed over longer time frames to allow sufficient time to develop response plans, deploy effective mitigations, and to account for the evolution of risks over time. Joined-up strategies are needed across multiple timescales to ensure complementary approaches to prevention, mitigation, response, and recovery.

Considerations for successful implementation

- An active focus on resilience, placing it at the centre of stakeholder thinking, should be encouraged, as a common resilience culture can help to unify approaches.
- Transparency and clarity in governance and leadership will be important to ensure accountability and openness to challenge and scrutiny.
- Efforts should be supported by clear guiding principles on resilience, standards for data sharing,[57] and the adoption of a shared terminology to build a collaborative risk and resilience community.

2. Encourage participation and communicate clearly

Risk assessment should be a participatory exercise. Opportunities for collaborative exercises with internal and external stakeholders should be sought. Input into risk assessments can be limited by the fact that those doing the analysis may be disconnected from the responders, or because external experts are unable to contribute because of security or commercial concerns. The benefits of bringing in external expertise – whether in the form of emergency services, academics, or individuals with lived experience, for example – include minimising groupthink and providing a robust challenge function by leveraging diverse perspectives. Different perspectives, supported by evidence and data from within and across sectors, can reduce gaps, improve oversight, identify vulnerabilities, and ensure the process and understanding of the risk is robust.

It is important to clearly communicate the purpose of any assessment and to secure buy-in for the process in order to maximise its value and build a good, shared understanding of its outputs and outcomes across the stakeholder base. Ownership of risk and responsibility for response must be clearly articulated. Risk assessments should be a tool for organisations to define their risk appetite and begin a conversation about trade-offs. A lack of transparency with respect to risk appetite can create grey areas regarding the level of planning that is required, particularly for unlikely but high-impact events. Discussions about acceptable levels of risk can help support least-regrets decision-making and support prioritisation and planning for interdependencies.

Beyond individual organisations, the wider sector, infrastructure, and supply chains are all part of the risk picture and need to be considered when seeking participation and communicating risk.

Considerations for successful implementation

- Mechanisms to involve diverse perspectives should be introduced.
- Sufficient time should be ring-fenced for internal and external engagement to ensure challenge can be meaningfully considered and changes are incorporated.
- Feedback mechanisms between external experts, assessors, and responders should be established to share lessons learned and good practice.
- Assessments need to be accessible and easy to use so that different end-users can effectively navigate the information. It should be clear what users are expected to do with the information, linking to other prevention and mitigation activities.
- The opportunity to encourage conversations about acceptable levels of risk should be explored.
- Any criteria or thresholds used during assessment – for example, to decide which risks require more thorough analysis – should be clearly articulated.

3. Focus on impact

To better manage uncertainty, decision-making should be driven by impact, rather than likelihood, and by preparedness in terms of capability across prevention, mitigation, response, and recovery. This mindset can enable a risk management and resilience culture that focuses on identifying key planning actions rather than concentrating on the likelihood of a particular hazard or threat when the exact nature of an emergency is highly uncertain, or data is limited.

Impact assessments should identify common consequences that exist across multiple risks, as well as any risk-specific impacts. Common consequences might include casualties, disruption of services, costs, and public reactions. By working through different risks and scenarios, drawing on existing evidence, data, and expertise, the spread and magnitudes of these impacts can be explored. Common consequences can then be mitigated for in a coordinated, risk-agnostic fashion, building general response capabilities and resilience. Any risk-specific impacts and mitigations can be addressed, drawing on the common consequence planning where appropriate.

Impact assessments should be conducted with bottom-up input from across the whole organisation, with appropriate external input, challenge function, and information sharing. Impact assessments should in addition aim to identify any population groups that may be disproportionately impacted.

Considerations for successful implementation

- Uncertainty, and the reasons for that uncertainty, should be stated explicitly.
- Pilots and experimentation should be explored to introduce and embed resilience thinking into organisational capability. We explore an **alternative approach** to risk assessment that focuses on impact and preparedness in Annex I that has been proposed to be trialled in such a pilot.
- Disproportionate impacts on certain population groups need to be considered, and input from these groups should be sought to ensure impact is fully understood.

4. Explore interdependencies

A single disruption or event may trigger cascading or concurrent consequences that can result in additional challenges for emergency response. These challenges may not ordinarily be revealed when risks are assessed in isolation. By bringing together individuals from different parts of the system with experience and understanding of their own risks, interdependencies can be uncovered and planned for.

The interaction between risks and the potential for cascade failures can be examined with qualitative or semi-quantitative approaches, while quantitative approaches require careful consideration of underlying assumptions and limitations. The risks with the greatest number of interdependencies could inform red teaming and emergency response exercises.

Interdependency mapping can also be an effective mechanism to understand and plan for the interplay between acute risks and chronic risks such as climate change.[58] Chronic risks require a different approach to risk assessment, planning, and management because of their slow onset and long timescales.[59] These risks and associated response capabilities should be monitored over time, with trigger points identified for any interventions. Consideration of interdependencies between chronic and acute risks and vulnerabilities would then capture those elements of chronic risk relevant to response planning and any secondary effects (eg where climate change impacts may disrupt supply chains).

Considerations for successful implementation

- The mapping of multiple interdependency layers (between risks, impacts, and planning assumptions or core capabilities) and the connections between them should be considered, with clearly stated assumptions and evidence. This should involve external input throughout and care over how it is built, analysed, and communicated.
- Wider interdependencies, including with external organisations, infrastructure,[60,61] and supply chains,[62] should also be explored, building on their experience. However, defining the right boundaries and engaging the right stakeholders are critical to discovering relevant lessons. Pilot exercises could be useful in scoping this exploration and in informing future work.
- Interdependency analysis could usefully inform scenario development, the design of emergency response exercises, and help identify compound risk events and vulnerabilities.

5. Consider a range of scenarios

Multiple scenarios should be developed to explore the uncertainties of high-level risks, setting out and explaining the anticipated worst-case scenario alongside several other plausible manifestations. Considering multiple scenarios can help with robust planning and identification of the range of different response capabilities that might be needed. It also supports the exploration of cascading risks and consequences with systematic impacts. The assumption that planning for higher-level risks will cover lower-level variations should be challenged.

Creating a playbook of scenarios paired with effective response capabilities could be a helpful tool to support better least-regrets decision-making ahead of, or in the early moments of, an emergency when uncertainty is high. For high-level risks, it will be important to understand what decisions need to be made ahead of time, and to identify and enable access to the best data streams and evidence to support the decision-making process.

Embedding a diversity of perspectives into the process, bringing in external stakeholders and using trained facilitators where possible, enables the identification of assumptions, impacts, and uncertainties that could otherwise easily be missed. When scenarios are co-developed in this way, evaluation of the response and recovery process will help to identify where vulnerabilities lie, what assumptions and uncertainties exist across the entire emergency cycle, and where specific interventions – for example, programmes of work or capability building – may be needed.

Considerations for successful implementation

- Adequate resource should be allocated to develop a broader set of scenarios.
- Guidance with clear criteria on producing scenarios should be shared, and should focus on identifying where additional capability is required.
- Scenarios should be subject to external challenge and scrutiny, and, where possible, trained facilitators should be used to encourage open discussion and debate.

6. Embed new data and metrics

If the purpose of a risk assessment is to drive better preparedness, then progress should be formally monitored to assess how well it meets this purpose. Evaluation metrics should be established that capture the impact of any methodology change or mitigations put in place in response to identified risks. Where an assessment has been used to prioritise action or investment, the magnitude of anticipated risk should be seen to change and potentially decrease, as impact (or likelihood) reduces, and preparedness increase, as the mitigations and prevention plans are put in place. Where there has been no change, this should be flagged, and the reasons should be investigated.

Data is vital in informing likelihood and impact assessments, providing early warnings,[63] and in monitoring unfolding emergencies. The role of data varies depending on the risk. Internal data on near misses, data on external major events, or data collected by other organisations may be valuable for planning and preparedness, and incorporating these data streams should be explored. Where possible, live monitoring can be used to understand and anticipate potential failures,[51] and digital twins[62] could be built to allow for emergency stress testing.

However, data that might ideally be incorporated may not exist or not be collected at all. Assessment cycles offer a good opportunity to identify and establish new high-quality data streams for the risk assessment and response.

It is also important to ask the right questions of aggregate data. An element of qualitative judgement will always be required when working with data and models, particularly for risks with high uncertainty or poor data availability or quality. Where new data and models are used, confidence in the data and models must be assessed and risk owners must have the analytical and assessment skills for robust decision-making. Data streams should always be supplemented with real-world information, mixed methods, and taking a broad view to make good decisions. Appropriate measures should be taken to ensure data is stored and used ethically and securely, with mechanisms in place for good governance and oversight.[57]

Considerations for successful implementation

- → Assessments should be evaluated across multiple dimensions, including stakeholder awareness, participation, and progress toward the assessment's overarching aims.
- → Mechanisms should be established to collect data on near misses and major events. This data should be used to build a picture of vulnerability and to learn lessons.
- → Data analysis and modelling should be a collaborative, multi-stakeholder process.
- → Data standards should be adopted to ensure any data captured is of usable quality.
- → Unknowns, assumptions, and limitations of modelling should be clearly communicated.
- → Opportunities to gain further insights from other work on data in emergencies should be explored.[65]

7. Review based on need

Different risks have very different characteristics: many will remain relatively static over time while others may be very sensitive to technological advances and societal changes. For example, the likelihood and impact of flooding changes at a pace slower than a two-year review cycle, where change is related to longer-term trends such as climate change and electrification. In contrast, cyber risks have a much faster pace of change, both in terms of threat and vulnerability – for example, with the accelerated shift to remote working and reliance on online platforms during the pandemic. The timeline for assessing risks should be set based on need rather than on a predetermined, standard interval.

Timescales for decision-making also vary. For example, shorter assessment and planning timescales may disincentivise longer-term mitigation planning and miss new and emerging risks. New and emerging risks can arise due to global technological advancements and increasing interconnectedness. Systematic ways to identify and act upon emerging risks are important. Foresighting and horizon-scanning activities could be used to help define new and emerging risks to illustrate where they are coming from, how they are evolving, and the anticipated pace of change. While this may not be a realistic use of resource in a single organisation, such information is published by professional engineering institutions, industry bodies, HSE and others, which should be embedded into the process. In turn, information on new and emerging risks should inform review timescales and the consideration of interdependencies.

Risks also change in response to the level of mitigations that are put in place. By assessing for preparedness too, residual vulnerabilities can be identified, actions can be prioritised, and the mitigated impact should be seen to decrease over time, meeting the assessment's main purpose.

Focusing on preparedness rather than likelihood is a central tenet of our **alternative approach**, which is explored in Annex I.

Considerations for successful implementation

- → If a near miss or high-magnitude event occurs nationally or internationally, it should trigger a review of any specific and related risk assessments, incorporating any lessons learned.
- → Mechanisms should be established to fill any gaps in evidence between assessment rounds.
- → Risks with high velocity of change should have effective update mechanisms, with consideration of the changes in risk between review cycles.
- → Assessments should present a clear indication of what has and what has not changed between assessment cycles to provide an audit trail.

4. Conclusion

Risk assessment is a vital function for any organisation, and the consequences of overlooking risks, missing interconnections, or having significant gaps in preparedness can be severe. This report has built upon a review, conducted by the Academy, of the methodology behind the NSRA. The review followed a user-centric approach (Annex II), built an understanding of the 2019 NSRA system (Annex III), and explored a range of case studies to understand good practice across the sectors. This review curated a set of specific recommendations for the NSRA methodology, which are detailed in Annex IV.

Seven **principles for good practice** were identified that can be used by organisations to improve their risk assessment and management processes and increase their resilience. This report has brought together multiple sources of evidence and lessons about approaches to risk assessment, and it is intended to function as an important source of information and knowledge.

In adopting any changes to risk assessment methodology, it is important that risk owners define what 'good' looks like and establish clear measures to indicate whether adopted changes have aided the assessment outcome and delivered its purpose. Any changes will take time to implement and will require active change management and engagement: facilitating opportunities for stakeholders to feedback, reflect, and share learnings on the successes and challenges.

We believe these seven principles offer an opportunity for risk owners to reflect on their own practices and represent a step forward in good practice for risk assessment.

We are calling upon leaders across all sectors to reflect upon the extent to which these **principles for good practice** are incorporated in their risk assessments, and to act upon them. All organisations need to consider how their risk management processes meet their users' needs and prepare them for a broad range of outcomes. Risk assessments should be clearly communicated to and challenged by users and diverse stakeholders so that dependencies and vulnerabilities can be identified and planned for, ensuring that resilience is built in.

These principles are considered collectively in Annex I, where we present a radical **alternative approach** to risk assessment, starting from a 'blank page'.

How can these principles be implemented?

In implementing these principles, there are multiple factors that could determine different dimensions of success. Here, we provide a set of questions that can be used as a starting point to check good practice, to think about how the principles can be practically implemented into day-to-day activities, and to evaluate change.
Useful questions to ask may include:

- Is the role of the assessment broadly understood?
- Is the wider organisation aware of the risks identified in the assessment and any interdependencies that may sit within their responsibilities?
- Is information exchange effective in increasing awareness?
- Can greater cross-organisational collaboration be facilitated to better understand risks?
- Is the organisation better prepared for the risks included in the assessment as a result?
- Are the risks decreasing because of improvements in preparedness or reductions in impact? If not, is that acceptable, or is there a need to be better prepared?
- Do the available capabilities meet the scale of the needs?
- Do plans for chronic issues take coincidental acute risks into consideration?
- Have opportunities for the use of data and external input been maximised?
- What are your practical considerations for change and how would this be measured?

© This is Engineering

Annex I
An alternative approach

The principles identified in this report are broad, spanning all aspects of the risk assessment process. Improving how risk assessments are conducted provides an opportunity to implement change efficiently and disrupt the current risk culture to drive more action and enhance resilience. Our **principles for good practice** can be individually implemented to adapt and improve risk assessment methodology. However, the lessons from this report could also be implemented more holistically, starting from a 'blank page'. Incremental change is not always the best approach; often, a radical alternative with fewer constraints allows us to better focus on the overall desired outcome.

This section sets out a preliminary exploration of an **alternative approach** to apply good practice in a more holistic way, with insights as to what might be possible with further development. This approach was presented to government as an alternative, and therefore the examples are geared toward a government audience. However, we believe this way of thinking and approaching risk has wider benefits across sectors and organisations.

The approach was tested using a flooding scenario with a diverse range of stakeholders, including participants from Defra and the Environment Agency, to explore its benefits and limitations.

What the alternative approach aims to deliver

Risk assessments are tools to inform emergency planning and response at a national and at local levels. Their primary users are the risk-owning individuals and departments and the emergency responders on the ground. These are the people who need to be able to draw value from the process so they may develop their response plans to the identified risks.

A holistic approach to implementing the principles would:

- act as a bridge between risk and resilience by spanning prevention, mitigation, response, and recovery
- provide a prioritisation tool driven explicitly by planning requirements, with likelihood a secondary consideration
- clarify ownership of risks and planning across the organisation, community, or nation to minimise unnecessary duplication and build collaborative relationships
- provide a mechanism to evaluate progress in risk reduction and management
- reduce the complexity of the process to facilitate greater engagement and communication.

Underlying principles of the alternative approach

The alternative approach is underpinned by two principles:

1. Likelihood does not have to be the driver for risk assessment and resilience thinking.
2. The approach should deliver on the needs of its users.

This approach proposes shifting the focus to preparedness – how prepared organisations are for risks with a non-zero likelihood, rather than on the likelihood of those risks occurring. Likelihood assessments remain of value for frequent events where historical data is available; however, it would not be the primary focus.

Instead, a least-regrets decision-making framework, as illustrated in Case study 2, helps inform decisions that must ensure balance between likely, lower-impact events and unlikely but high-impact events. Initial action would be prioritised based on the degree of work required to increase preparedness, with progress toward or evolution of preparedness requirements evaluated with each round of assessment.

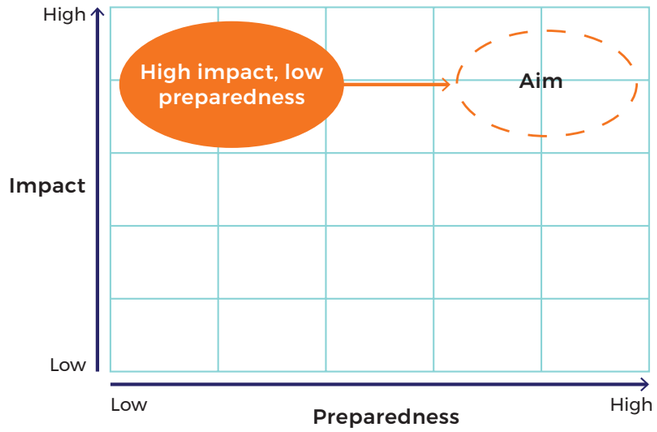


Figure AI.1. | An example of an impact versus preparedness matrix

Ultimately, this alternative approach would aim to evolve to encompass resilience to the unexpected and build in resilience theory, as outlined in Case study 17.

Impact versus preparedness

With this approach, risks are examined against their **impact** and the level of **preparedness** for the consequences:

- **impact** – based on multiple manifestations of a particular risk, the possible **unmitigated** impacts and their magnitude are presented in reference to a set of **common consequences**, in addition to any consequences specific to the individual risk
- **preparedness** – an assessment of how prepared the organisation is to react to the **mitigated** impacts of a risk considering any prevention measures, existing mitigations, general and specific response plans, and recovery requirements: its **residual vulnerability** to the risk. This assessment provides a mechanism to explore what measures are in place or are planned, and these can then be evaluated across future assessment cycles.

The output of the assessment can then be represented as an impact versus preparedness matrix, as illustrated in Figure AI.1.

The alternative approach in detail

Details of the proposed steps of the alternative approach have been illustrated in Figure AI.2 and are outlined below.

Step 0 – Inputs

Before beginning the risk assessment process, the key inputs should be identified. These include:

- **data** – for example, in the case of a flood, this data could come from academia, the Office for National Statistics, the Met Office, the Environment Agency, location data and information on critical national infrastructure, the Flood Forecasting Centre, and the Climate Change Risk Assessment for information on how the hazard might change (see Principle 6 for more information)
- **stakeholders** – other departments, emergency responders, and devolved administrations, agencies, academia, industry, insurance industry, local responders, and citizens
- **risks interdependency map and analysis** – a cross-organisation exercise should be undertaken to map the interdependencies between risks and response plans. This should be available as an evidence-based resource to draw on throughout the process, with feedback loops to return information back into the interdependency map (see Principle 4 for more information).

Step 1 – Build scenarios

For each risk, where appropriate, a range of scenarios should be explored to build an understanding of the breadth of possible impacts it may have (see Principle 5 for more detail). The range of scenarios will drive planning and will feed in across the whole process.

By using a range of scenarios, variability in the impact of each risk can be explored over a set of factors relevant to the risk. For example, the following factors may be appropriate to explore for flooding: geography (urban versus rural), duration (days, weeks, etc), cascades (disruption to power, disruption to transport, risk of landslide, etc), level of flooding, likelihood.

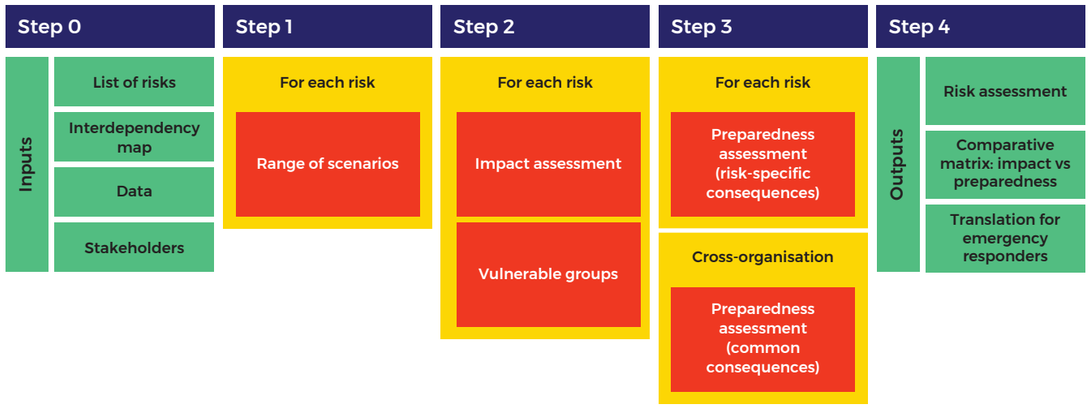


Figure AI.2. | The steps of a risk assessment with suggested inputs, owners, and outputs

Step 2 – Impact assessment

An impact assessment should be conducted for each risk that is evidence based and considers a range of scenarios. Common consequences should be identified across the assessments in addition to any risk-specific consequences.

Common consequences may include fatalities, casualties, displacement of people, public reaction, disruption to services, economic cost (disruption, damage, recovery), disruption to travel and essential services, loss of power and communications, environmental damage (contamination, rubble, and debris), security, legal duties, and international impacts.

Working through the scenarios, drawing on existing evidence and data, the following questions would drive the assessment:

- What common consequences apply to this risk?
- What do those common consequences look like in this context?
- What is the range and maximum level of impact drawn out from the scenarios?
- Are there risk-specific consequences that are not covered by the common consequences?
- Which population groups are disproportionately impacted?
- How can we rapidly identify disproportionately impacted groups, should the risk occur?

This exercise should be conducted with bottom-up input from across the whole organisation, with appropriate external input, challenge, and information sharing.

Step 3 – Preparedness assessment

Following the impact assessments and identification of common and risk-specific consequences across a range of scenarios, this next step is an opportunity to assess the level of preparedness against those impacts. It should encourage cross-organisational discussions on preparedness – particularly for common consequences – and bring together supporting evidence, data, and external expertise.

The preparedness assessment can be divided into two parts:

1. **preparedness for common consequences** – a risk-agnostic assessment should be conducted into the level of preparedness (across mitigation, response, and recovery) for the common consequences at their identified impact levels; this should involve input and evidence from across the organisation
2. **preparedness for risk-specific consequences** – an evidence-based assessment led by the team and/or department that own and are responsible for the mitigation, response, and recovery for a given risk.

It is important that ownership for each aspect of preparedness – mitigation, response, and recovery – is clearly defined, and that there is iterative feedback between the common consequence and the specific consequence preparedness assessments.

This exercise would seek to examine the following questions:

- What mitigation is in place and who owns it?
- What are the response needs – general and specific – and who owns them?
- What are the recovery needs – general and specific – and who owns them?
- What measures are in place for vulnerable groups?

- What are potential interdependency effects?
- What prevention is in place that could help stop the event/consequence happening in the first place?

To aid these assessments, data streams should be established to monitor how preparedness is changing over time; for example, through regular reviews of available skills and personnel capabilities for response. The use of indicators and a scoring index may also assist in assessing the measures that are in place and in the identification of gaps. However, careful consideration of consistency across risks is needed when using common indices. External input can provide a valuable review and challenge function, as well as highlighting additional measures that could be scored against to ensure the robustness of the index.

An example model that could be drawn from is the Global Health Security index,[66] which scores countries based on defined indicators to prevent, detect, and respond to health emergencies, as well as capturing indicators on a country's health system, compliance with international norms, and overall risk environment and country vulnerability.

From a practical point of view, mechanisms, frameworks, and standards will need to be put in place to enable sharing of information on preparedness between teams, departments, authorities, and other relevant organisations.

Step 4 – Impact versus preparedness matrix and other outputs

The outputs of this process can then be reported as an impact versus preparedness matrix (see Figure AI.1), supported with the evidenced assessments of risks and consequences.

This is a significant shift, given that impact versus likelihood is very much the accepted way of assessing and visualising risks within the risk community. As such, clear communication will be important to accompany this shift in practice, ensuring the rationale and benefits of the change are articulated well to create the necessary buy-in.

The usefulness of using likelihood as an indicator for some risks, particularly natural hazards, cannot be overlooked. Furthermore, likelihood will remain relevant for those risks for which response capabilities cannot be rapidly scaled up. An indication of likelihood could be included in the matrix, or as a separate consideration; however, this was not investigated for the present report.

Use of the outputs

The addition of preparedness as a metric would enable a clear picture of an organisation's resilience to different risks and their consequences. This metric alone could facilitate a more holistic approach to resilience by broadening the discussion and identifying areas for action. It would inform and add transparency to the level of risk and preparedness that the organisation is willing to tolerate. The outputs of this process would inform planning and investment decisions. Ownership would be clearly and transparently communicated.

Guidance and good practice should be built into the process to ensure levels of preparedness remain high, and to ensure that well-prepared-for risks, particularly likely ones, are not de-prioritised in funding decisions.

Future assessment cycles and evaluation

With preparedness measured across risks, each assessment cycle would create an opportunity to evaluate progress across prevention, mitigation, response, and recovery and to build assurance into the assessment process, with accountability and responsibility for action. Risks would be expected to move across the matrix over time as preparedness changes, as opposed to the more static picture of an impact versus likelihood matrix.

Piloting the alternative approach

We invite members of the wider community to consider and pilot this alternative approach. This is a different way to think about risk, moving away from risk assessment toward a more holistic, resilience-driven approach. By building a holistic understanding of risks, their consequences, and the level of preparedness, it enables a transparent discussion about how well prepared organisations are. It provides a mutual understanding of risk appetite and helps identify areas for action with clear ownership, accountability, and evaluation.

Considerations for successful implementation

- This should include the development of a preparedness index that includes common consequences broadly applicable to different hazards and threats.
- Frameworks for collaborative assessment processes should be developed.
- Training for skills and capability building will be needed.
- Presentation of multiple scenarios should be considered.
- Consideration should be given to how local and national capabilities could be brought together into the preparedness assessment and the assurance mechanisms this might require.
- The challenge of communicating a new matrix with impact and preparedness should not be underestimated, and expert advice and facilitation should be sought to ensure good communication and effective stakeholder engagement.
- The success of implementation is implicit upon bringing together the right stakeholders from across the process to understand what implications such a change might have.

© This is Engineering

Annex II
Review methodology: a user-centric approach

This annex sets out the methodology the Academy used in reviewing the 2019 NSRA. The NSRA is a complex, multilayered process with a broad range of different stakeholders. The review therefore took a 'systems approach' to help identify different elements and actors and the ways in which they interconnect and interact to build a shared understanding of how different interventions or changes can affect the system as a whole.

We followed the systems approach framework developed by Professor John Clarkson FREng for the Academy's 2017 report *Engineering better care*,[67] to work toward tangible improvements that put user needs and perspectives at the centre, as illustrated in Figure AII.1. Since publishing the *Engineering better care* methodology for health care improvement, we have translated this framework into training for policymakers, providing a pragmatic entry point to implementing a systems approach for policy problems.[68]

A **systems approach** can encourage evidence gathering that draws on the widest, most diverse and critical perspectives leading to a 'bigger-picture' view of the system and its actors. It can help to identify the different elements and actors that contribute to a system, how they interconnect and interact, to help build a shared understanding of how different interventions or changes to the system – for example, new policies – can affect the system.

By exploring the 2019 NSRA through this framework and following an iterative process with expert and user input, we expanded and tested our understanding of the overall risk system and refined a range of solutions in the context of the 2019 NSRA, which were brought together to inform the final actionable recommendations (see Annex IV). Our review consisted of three stages:

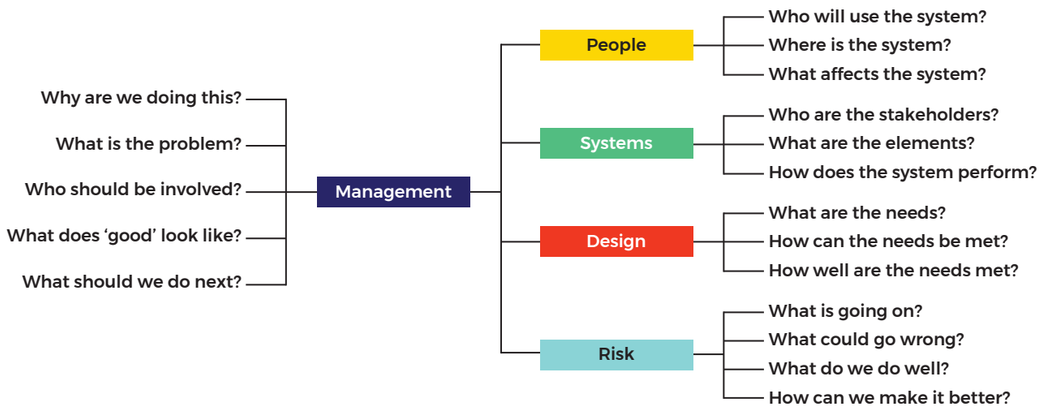


Figure AII.1. | Systems approach framework for thinking. By exploring the questions, an understanding of the overall system and process can be built, a broad range of solutions explored, and these can be brought together to inform proposed improvements. Adapted from *Engineering better care: a systems approach to health and care design and continuous improvement*[69]

1 **Understanding the system, its users, and their needs**. We consulted with more than 130 stakeholders across lead government departments (LGDs), local resilience forums (LRFs), and public sector organisations. We explored how the NSRA is used in central and local government in order to identify the perceived benefits and limitations of the process and methodology. A summary of the findings is presented thematically in the present report's Annex III.

2 **Exploring the solutions**. Evidence from literature, survey responses, and structured interviews were drawn upon to learn lessons and identify possible solutions to the challenges of the 2019 NSRA methodology. Methods for developing scenarios, interdependency analysis, and building resilience thinking are discussed and illustrated by a broad range of case studies in Section 2. The detailed case studies enabled us to explore different organisational practices and to understand the required expertise.

3 **Recommendations for the NSRA**. The key findings and possible solutions were considered in the context of the 2019 NSRA processes and its users' needs. We provided the Civil Contingencies Secretariat with a set of 13 recommendations and practical considerations for their implementation, shown in Annex IV.

Validation and testing

Throughout the review, stakeholder engagement and testing were an integral part of the process, allowing us to iterate and refine our recommendations for the NSRA methodology. The testing phase aimed to:

- re-engage stakeholders and explore their views on the principles
- identify potential tensions, challenges, and opportunities
- ensure the principles were practical and implementable, would meet user needs, and would deliver improvement
- explore how best to communicate and encourage buy-in and support for the principles.

Testing activities, such as exploratory conversations and workshops, were tailored to specific recommendations. In the interests of stakeholders' time, and to examine how various recommendations may interact and impact across the whole NSRA process, where possible, the most challenging recommendations were used as a lens through which to explore the others (see Table AII.1). For example, the workshops either presented participants with 'provocation statements' to react to or walked them through elements of the NSRA process, providing opportunities for verbal and written comments on the implications of any change. Stakeholder engagement for the testing phase was as broad as possible to encourage discussion and debate from multiple and different perspectives of the process. During the workshops, we were open and transparent about our rationale for the recommendations, aiming to identify areas of consensus, diverging opinion, benefits, and concerns.

Table AII.1. | Testing activity summary

Testing aim	Activity	Rationale
Focusing the scope of the NSRA	Workshop – provocation statements	A simple provocation statement to explore pros and cons and discuss the nuances of changes to chronic risks, likelihood, scenarios, and the assessment timescales
Identifying emerging risks	Exploratory conversations	Exploring existing processes and structures to identify how they could be used to support identification of emerging risk
Exploring uncertainty	Workshop – walk through the NSRA process for multiple scenarios	The practicalities and implications of multiple scenarios were explored by walking through the steps of the NSRA process
Implications for the local tier	Workshop – series of questions	The implications for the local tier were probed through a series of questions and discussions
The alternative approach	Workshop – walk through the alternative approach applied to flood risk	Our alternative approach was applied to the risk of flooding to provide context in which potential challenges, benefits, and areas for further exploration could be identified
External engagement	Covered in the other testing activities and the quorum session	Demand and opportunities for external input and data, including examples of good practice

Note: For each activity, a set of recommendations was tested.

Annex III
Understanding the system

To assess the 2019 NSRA methodology, we first needed to understand the system, its users, and their needs. According to the 2019 NSRA, the overarching purpose of the NSRA is assumed to be:

- to present an evidenced oversight of the UK risk landscape and generate risk awareness across government
- to allow comparison, prioritisation, and management of different risks
- to inform proportionate planning at national and local levels and the effective allocation of resources.

With such a broad purpose, there are multiple critical stakeholders involved across Cabinet Office, the Civil Contingencies Secretariat, government departments, and the local tier. To build an understanding of the system, we engaged with stakeholders who were both risk owners and NSRA users, such as LGDs, devolved administrations, LRFs, and other public sector organisations. Stakeholders were asked what they needed from the NSRA and why, giving us insight into how users interacted with the NSRA and the diversity of user needs, alongside the perceived benefits and limitations of the methodology and process. This informed a systems map of the 2019 NSRA process and its owners, an overview of which is shown in Figure AIII.1.

Our understanding of user perspectives enabled engagement with key stakeholders throughout the review process and allowed any implications of changes to the methodology to be quickly identified.

The 2019 NSRA identifies over 130 diverse risks: hazards (non-malicious) or threats (malicious) that could feasibly cause significant harm and disruption to the UK within two years.[iii] Every risk in the NSRA is assigned to a LGD that is responsible for developing a RWCS with input from other organisations as needed. In most cases, under the LGD model, that department is also responsible for leading the planning and response to that risk.[70] The RWCS is intended as a worst plausible manifestation for a particular emergency: an illustration of a high threshold for preparation. It defines the proportionate preparation of capabilities needed for the range of possible emergencies arising from a threat or hazard.[3] Each RWCS is assessed to produce a quantitative scoring on their relative likelihood to occur within the next year and the impact that this occurrence would have. The numerical scores are collated into a risk matrix to allow for a comparison between all risks, with the least likely and least impactful risks in the bottom left and the most likely and most impactful in the top right. An example of such a risk matrix is shown in Figure AIII.2a, with a selection of illustrative risks, reproduced from the NRR.[3] Further information on the risk assessment process can be found in a recent briefing from the Parliamentary Office for Science and Technology.[71]

The matrix is divided into five levels along each axis, allowing RWCSs to be grouped according to their impacts and likelihood on a pseudo-logarithmic scale. The levels of likelihood are detailed on the matrix in Figure AIII.2a, while the levels of impact, evaluated across several categories, are expanded upon in Figure AIII.2b. This grouping aids comparison and, in conjunction with other assessments, the relative scores aid risk-owning bodies such as LGDs and LRFs to undertake proportionate planning and resource allocation. Further information on how the NSRA translates into emergency planning and the roles and responsibilities of risk management across the government can be found in a recent report from the National Audit Office.[72]

iii See Annex V – Glossary for definitions

Process	Method
List of risks	Risks are identified through consultation with a wide range of stakeholders†
	Risks are considered for inclusion in the NRSA on the basis that they could plausibly occur in the next two years and could cause significant harm and disruption in the UK, or to UK interests abroad
Reasonable worst-case scenarios	Departmental risk owners produce plausible but challenging RWCSs for each risk in consultation with stakeholders and using data from a wide range of sources to frame the risk in real-world terms
Likelihood assessment	RWCS are assessed for likelihood of occurring within the next year, using extensive data, modelling, and expert analysis
	Non-malicious risks are assessed by risk-owning departments Malicious risks are assessed based on a balance between intent, capability, and vulnerability
Impact assessment	A likelihood score, expressed as a percentage, places the risk in one of five tiers
	The impact of each risk is assessed across seven broad dimensions: 1. impact on human welfare 2. environmental damage 3. security 4. disruption of essential services 5. economic damage 6. international relations 7. behavioural impacts Each dimension is scored on a 0 to 5 scale, and these scores are combined to give a single overall impact score
Review	Independent expert groups review and challenge the final assessments
NSRA, Risk matrix, *National risk register*, local guidance	The outputs from the NRSA are used: • to inform prioritisation of planning activities • as an evidence base to inform policy • as a communication tool • to produce guidance to support local and devolved implementation

Figure AIII.1. | A schematic overview of the 2019 NRSA process

† Here, 'stakeholders' refers to a broad range of experts, including chief scientific advisers, internal governmental experts, government departments and agencies, the intelligence community, industry and sector stakeholders, as well as external scientific, academic, and policy subject experts.

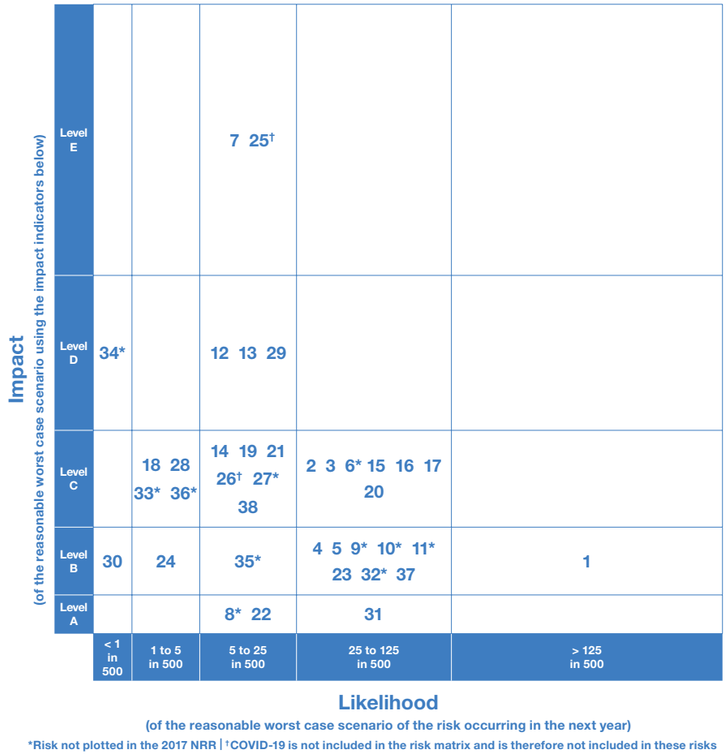


Figure AIII.2. | (a) An impact versus likelihood risk matrix drawn on a pseudo-logarithmic scale, showing the positioning of several illustrative risks. Reproduced from *National risk register* (2020 ed.)[73]

Level	Indicative impact scale indicators	
E	• **Economic impacts:** more than £10 billion. • **Fatalities in the UK:** more than 1000. • **Evacuation and shelter:** 100 thousand people evacuated over 3 days. • **Public perception:** extreme, widespread, prolonged impact owing to significant proportions of the UK population feeling more vulnerable.	• **Environmental damage or contamination:** of city(ies) or region for more than 5 years. • **Essential services:** lack of health and care services affecting 40% of the population for 30 days. • **Electricity supply:** national loss of electricity supply for any period or regional loss of supply for longer than 1 week. • **International relations:** significant damage to UK relationship with key allies.
D	• **Economic impacts**: £1 billion to £10 billion. • **Fatalities in the UK:** circa 201 to 1000. • **Evacuation and shelter:** 20 thousand people evacuated over 3 days. • **Public perception:** high impact owing to millions of UK citizens feeling more vulnerable.	• **Environmental damage or contamination:** of a county OR city(ies) for approximately 1 year. • **Essential services:** lack of health and care services affecting 20% of the population for 7 days. • **Electricity supply**: major disruption to electricity supply to 1 million people for longer than 18 hours. • **International relations:** moderate damage to UK relationship with key allies.
C	• **Economic impacts:** £100 million to £1 billion. • **Fatalities in the UK:** circa 41 to 200. • **Evacuation and shelter:** 5 thousand people evacuated over 3 days. • **Public perception:** moderate impact owing to hundreds of thousands of UK citizens feeling more vulnerable.	• **Environmental damage or contamination:** damage to/contamination of a local area for 1 year. • **Essential services:** lack of health and care services affecting 10% of the population for 12 hours. • **Electricity supply:** major disruption to electricity supply to greater than 300 thousand consumers for longer than 18 hours. • **International relations:** significant damage to UK relationship with international partner country/organisation.
B	• **Economic impacts:** £10 million to £100 million. • **Fatalities in the UK:** circa 9 to 40. • **Evacuation and shelter:** 200 to 1 thousand people evacuated over 3 days. • **Public perception:** minor impact owing to tens of thousands of UK citizens feeling more vulnerable.	• **Environmental damage or contamination:** of the local area for 1 month OR of building for 1 year. • **Essential services:** lack of health and care services affecting 2% of the population for 12 hours. • **Electricity supply:** major disruption to electricity supply to greater than 100 thousand people for longer than 18 hours. • **International relations:** moderate damage to UK relationship with international partner country/organisation.
A	• **Economic impacts:** less than £10 million. • **Fatalities in the UK:** circa 1 to 8. • **Evacuation and shelter:** 50 people evacuated over 3 days. • **Public perception:** limited impact, small numbers of the public (less than tens of thousands) feeling more vulnerable.	• **Environmental damage or contamination:** of a building for up to 1 month. • **Essential services:** lack of health and care services affecting 1% of the population for 6 hours. • **Electricity supply:** major disruption to electricity supply to greater than 10 thousand people for longer than 18 hours. • **International relations:** moderate damage to UK relationship with any other country.

The impact scale indicators above set out the types and severity of impacts the UK might expect to see for the different level risks.
The list above should NOT be read as a set of criteria that needs to be met in order for an assessed risk to be classified at these levels.

Figure AIII.2. | **(b) indicative indicators for scale of impact for assigning a level to each assessed risk. Reproduced from *National risk register* (2020 ed.)[73]**

What are the challenges?

Risk assessment at national level is complex, and any one methodology will face numerous challenges. In the context of the 2019 NSRA methodology, examples of challenges are as follows:

- **confidence in the likelihood assessments varies** – the confidence is greater for risks where there is a long and reliable history of incidence, whereas confidence in the likelihood assessment of malicious risks is limited as the landscape changes very fast
- **scenarios vary in specificity across different categories of risk** – RWCSs can mask cumulative risk as there could be numerous scenario variations with significantly different likelihood and impact scores
- **comparing chronic and acute risks is challenging** – defining an appropriate RWCS and quantifying its impact for risks that do not typically take the form of discrete events is difficult.

Our engagement with NSRA stakeholders alongside current and past chief scientific advisors and risk experts from industry and academia further highlighted some perceived limitations in the 2019 NSRA methodology. We have grouped these insights into several identified themes, which are explored in the rest of this annex.

Scenario design

Scenarios are a useful tool for understanding impact and creating planning mitigations; however, care must be taken not to place too much weight on a single RWCS, as different manifestations of a risk can require different responses or mitigation capabilities. Focusing on a single scenario can also mask cumulative risk. Confidence in a scenario is greater when there is a long and reliable history of incidence or a more static risk landscape. It can also be challenging to design useful scenarios for chronic risks that do not take the form of a discrete event. Development of scenarios should be about the process as much as any numerical outputs, and this process should be communicated to stakeholders.

Impact

Impact can be easier to assess for events that have occurred in recent memory, as the consequences (and potential cascade effects) are better understood. International examples can be helpful in capturing some risks that have not been realised domestically. However, when extrapolating from data-rich historical examples, it is difficult to be confident concerning the impacts when exploring potentially more impactful manifestations of a risk that have not yet occurred. Nonetheless, there remains a need for comparison between impacts for different risks.[74] Any assumed mitigations affecting impact should be explicitly stated; otherwise, they may create a barrier to understanding the impacts of a scenario. Impact is also affected by daily context (eg a bad winter, with high hospital bed occupancy or preventing travel to work) and by mitigations enacted by other stakeholders (eg closed schools reducing staffing levels more than assumed in the scenario).

Likelihood

Likelihood assessment is especially challenging to quantify for events that have never occurred or for malicious threats. While historical data is very effective for quantifying the likelihood of events that happen relatively frequently, such as flooding, understanding the likelihood of infrequent events, such as pandemic influenza, with fewer data points is more challenging. Where likelihood can be derived based on historical precedent, care should be taken to account for changes in the risk landscape over time (eg climate change, which will change the accuracy of historic probabilities).

Assessment timelines

The timeline over which an assessment is made can change the likelihood of risk manifestation (eg a flood has a probability *X* of occurring within a year but a probability *Y* of occurring within five years). Short assessment timelines restrict the use of foresighting techniques and may not allow enough time to establish any strategic mitigation capabilities. For time- or resource-poor stakeholders, such as LRFs, staying up to date with the changes can be a challenge. However, if assessment timelines are too long, the responsibility for action on mitigation, prevention, and preparedness can become unclear.[75]

Concurrent or cascading risks and interdependencies

There is a need to think about the interactions, cascades, and transfers between risks.[iv] Advancing multi-hazard assessment methods can provide techniques to analyse these interdependencies. However, quantifying the interdependencies between elements in the system is very challenging. Consideration of concurrent or cascading risks and interdependencies requires a significant change in mindset, compared to the current focus on individual risks. Consideration needs to be given to how complex interdependencies across risks are presented, so that it has a practical use or application for planning and response.

Data

The role of data varies depending on the risk. Data can be used to inform likelihood assessments, provide early warning of an imminent potential emergency and to monitor an emergency once it happens. Data is critical for some risks where there are local, national, or international examples or modelling that can inform the RWCS. For other risks, data or high-quality models may be less available or accurate, requiring an additional layer of qualitative assessment with expert judgement, such as a high-profile cybercrime incident. Where new data and models are used, the confidence in the data must be assessed. Asking the right questions of the aggregate data will be an important collaborative process. Assessment cycles provide an opportunity to assess what data is available now, what data could become available over the short, medium, and long term, and what could be made available quickly if there was a critical need.

External input and expertise

Where possible, external input and expertise should be used and supported by empirical evidence to ensure the assessment is robust and reduce the risk of groupthink (ie where individuals may overlook potential problems in the pursuit of consensus thinking). Whether the external input is robust is often dependent on who is in the room; sometimes, this can be limited by the fact that threat analysis is disconnected from responders on the ground because of security sensitivity.

Diversity and inclusion

Diversity and inclusion can be limited by restrictions on the sharing of the final risk assessments and through the information used to compile it. There are numerous mechanisms in development to combine different administrative data to help identify who may be at greatest risk. Consideration of disproportional impacts on certain groups is very limited, and which groups count as 'vulnerable' depends on the risk (eg major fire risks identify older men to be disproportionately impacted). It is important to call on the expertise of social scientists, as human behaviours are an important factor in risk assessment despite being inherently difficult to quantify.

iv See Annex V – Glossary for definitions

The process

The 2019 NSRA process was considered by some to be overly complex, with the assessment of different risks likened to "comparing apples and oranges". At the local level, international and security risks in the NSRA can be difficult to meaningfully incorporate into local assessments, and chronic risks can cause confusion. Where national mitigation plans are required, it would be useful for LRFs to understand their role in that context. A lack of feedback between local, devolved, and national risk assessments and the risks they identify can result in a disconnect of priorities and reinforces the perception of a London-centric risk assessment.

The risk assessment process could be communicated better and more regularly to increase buy-in from LGDs. For some risk owners, there is a clear connection between their day-to-day risk management and the NSRA process; for others, there is an opportunity to make it clearer what departments are meant to do with the information.

Assumptions

While reviewing the methodology, the Academy identified several assumptions upon which the 2019 NSRA process appeared to be based. It was not clear to what extent these assumptions were communicated when risk owners were asked to contribute to the 2019 NSRA cycle. These were:

- developing RWCSs provides a mechanism for comparison of risks
- RWCS impact assessments enable the development of planning assumptions for national-level responses
- planning and building generic capabilities to address a RWCS would support effective management of more probable, lower-impact manifestations
- RWCSs and NSRA can be translated from the national to the local level
- the users of the NSRA can use RWCSs for planning and to consider variations around them.

© This is Engineering

Annex IV
Recommendations for the NSRA

Our 2019 NSRA review made 13 practical recommendations based on the limitations of the 2019 methodology, which are presented below. Recommendations 1 to 12 are intended for immediate implementation, while Recommendation 13 is presented as a more radical, alternative 'blank page' approach.

Recommendation 1: The National Resilience Strategy should be used to **implement a systems approach** to risk and resilience across government. The purpose and role of the NSRA must be clearly communicated and how it fits into the wider UK risk and resilience landscape articulated.

Recommendation 2: The NSRA should **primarily focus on acute risks**, and chronic risks should be assessed through a separate but linked process.

Recommendation 3: A collaborative cross-government study is needed to **map the interdependencies** between risks and in response and capability planning.

Recommendation 4: For each risk, **a range of scenarios should be generated to explore uncertainty** and additional planning requirements, improve the output, and deliver maximum value from the overall process. Where appropriate, the range of scenarios should be included in the NSRA.

Recommendation 5: To create a culture of preparedness, likelihood should not be the main driver for prioritisation, as this can be difficult to assess with a high degree of confidence across all risks. **Decision-making should be driven by impact and preparedness** linked to capability across prevention, mitigation, response, and recovery.

Recommendation 6: The NSRA review cycle should be transformed into **a more agile, needs-based approach** that can adapt to risks that evolve at different speeds.

Recommendation 7: The process and purpose of the NSRA must be **clearly communicated** to maximise its value and buy-in across government.

Recommendation 8: The **security classification** of the NSRA and its constituent parts should be reviewed to maximise participation and input from stakeholders and to bring in external expertise that draws upon the widest, most diverse, and critical perspectives.

Recommendation 9: The capacity, capability and structures to **identify and assess emerging risks** should be established and a review of the risks assessed at a local level undertaken to ensure the full breadth of risks are captured and planned for.

Recommendation 10: Opportunities for **external expert participation** should be identified across the whole process to ensure a robust challenge function and minimise groupthink.

Recommendation 11: Government should work with the Office for National Statistics and other public sector agencies and research organisations, such as the Alan Turing Institute, to use the next iteration of the NSRA to identify and establish **new high-quality data for the risk assessment and response**.

Recommendation 12: Any changes made to the NSRA should be formally recorded and evaluated, to better understand the impact of the methodology change on the overall process and to assess **how well it meets its intended purpose**.

Recommendation 13: The **alternative approach** proposed by the Royal Academy of Engineering should be piloted and developed, using a single risk with multiple variations, in the first instance, to trial, test, and build a greater understanding of how the NSRA could be approached more holistically with an **impact against preparedness matrix**.

Annex V
Glossary

Initial definitions are drawn in part from the Royal Academy of Engineering's Safer Complex Systems project,[76] the NRR,[3] the Natural Hazards Partnership and British Geological Survey's *Review of environmental multi-hazards research and risk assessments*,[23] a Parliamentary Office for Science and Technology brief on evaluating natural hazards,[70] and the World Health Organization. Many of these definitions were iterated by the Civil Contingencies Secretariat for inclusion in the national resilience strategy consultation.[77]

Capability: the people, infrastructure, and assets that provide the ability to be resilient

Emergency: an event or situation that threatens serious damage to human welfare or the environment; or war, or terrorism that threatens serious damage to security

Impact: the scale of harm or damage to human welfare, the environment, or the security of the UK

Interdependency: physical, digital, geographic, or organisational links that enable transfer or sharing of risk, failure, or mitigation – interdependency is a precondition for cascading risk

Likelihood: probability of an event occurring within a certain time frame

Multi-hazard event: the specific contexts where hazardous events may occur simultaneously, cascadingly, or cumulatively over time, and taking into account the potential interrelated effects.[22] The type of relationship depends on the effect on the likelihoods and/or impacts of the hazards:[23]

- **triggering relationship** – one hazard triggering other hazards, or a series of triggering relationships forming a cascade or domino event
- **amplification relationship** – one hazard changing the landscape and thereby increasing the likelihood of other hazards occurring

These definitions are focused on hazards; however, they can also be applied to threats, while making note of any potential differences or gaps

Preparedness: actions taken in anticipation of an emergency to facilitate rapid, effective, and appropriate response to the situation

Resilience: the ability to anticipate, assess, prevent, mitigate, respond to, and recover from hazards, threats, disruptive events, and civil emergencies

Risk: an event, person, or object that could cause loss of life or injury, damage to infrastructure, social and economic disruption, or environment degradation. The severity of a risk is assessed as a combination of its potential impact and its likelihood. The government subdivides risks into **hazards** and **threats**:

- **acute risk**: time-bound, discrete events (such as a major fire or a terrorist attack)
- **cascading risk**: the knock-on impacts of a risk that cause further physical, social, or economic disruption; for example, severe weather could cause flooding, which then causes damage to electricity infrastructure, resulting in a power outage that then disrupts communications service providers
- **chronic risk**: continuous challenges that gradually erode our economy, community, way of life, and/or national security (such as money laundering, or antimicrobial resistance)
- **compound risk**: when two or more events coincide in a space and/or time causing impacts greater than the sum of the two individual risks; for example, flooding in an area that is experiencing a disease outbreak
- **concurrent risk**: when two or more events coincide in space and/or time
- **hazard**: a non-malicious risk, such as extreme weather events, accidents, or the natural outbreak of disease, that has the potential to cause harm
- **residual risk**: the risk of harm that remains once risk reduction measures have been implemented
- **risk-agnostic**: the ability of a capability, process, or response to address 'common' impacts of risks (those impacts that occur across multiple scenarios)
- **risk appetite**: the amount of risk an individual, business, organisation, or government is willing to tolerate
- **transferable risk**: transfer of risk from one component in the system to another due to a mitigation
- **triggering risk**: a primary event that causes one or more secondary events; the secondary events might be identical or different from the primary event
- **threat**: a malicious risk such as an act of terrorism, hostile state activity, and cybercrime that has the potential to cause harm.

Vulnerability: the quality or state of being more prone or exposed to the impacts of hazards or threats; vulnerabilities could affect individuals, communities, assets, or a whole system, and may be caused by physical, social, economic, and environmental factors or processes.

Vulnerable groups: populations with physical, psychological, social, or geographic characteristics that limit their ability to anticipate, cope with, resist, and recover from the impacts of disasters, or result in a disproportionate share of the burden associated with emergencies:

- **physical** – includes the chronically ill and physically disabled, and persons living with immunodeficiency; pregnant women
- **psychological** – includes those with chronic and non-chronic mental conditions that may impair judgement in a crisis; those with a history of substance abuse and those who are suicidal or susceptible to homelessness
- **social** – includes those living in abusive families, people who are homeless, immigrants, refugees, and people living in poverty and suffering from its common consequences
- **geographical considerations**, owing to geography creating barriers and exacerbating inequality and creating vulnerable groups (eg isolation and slow response times in the Outer Hebrides; risks will be responded to differently in the Brecon Beacons compared to in the centre of Bristol)
- we should also take into account cases in which vulnerability is created or enhanced by *race*, *ethnicity*, *age*, *sex*, and *income*.

Annex VI
Quorum and staff

Academy project team

Dr Alexandra Smyth
Senior Policy Advisor, Royal Academy of Engineering

Dr Marie Laure Hicks
Senior Policy Advisor, Royal Academy of Engineering

Dr Shabana Haque
Head of Engineering Policy, Royal Academy of Engineering

Dr Natasha McCarthy
Associate Director, Policy, Royal Academy of Engineering

Arizona Rodriguez
Policy Officer, Royal Academy of Engineering

Calum Savage
Policy Officer, Royal Academy of Engineering

Dr John Cully
Policy Officer, Royal Academy of Engineering

Project quorum

A group of Fellows and risk experts formed the project quorum to provide ideas, direction, and constructive challenge to the project, and to ensure that the outcomes are evidence based and implementable.

Chair: Professor Joan Cordiner FREng FRSE, Professor of Process Engineering and External Engagement, University of Sheffield

Professor Robin Bloomfield FREng, Professor of Software and Systems Dependability, City University of London

Professor Phil Blythe FREng, Professor of Intelligent Transport Systems, University of Newcastle

Kathryn Brown, Head of Adaptation, Committee on Climate Change

Dr Corinna Elsenbroich, Senior Lecturer, University of Surrey

Professor Robin Grimes FREng, Ministry of Defence Chief Scientific Adviser (Nuclear)

Professor Jim Hall FREng, Professor of Climate and Environmental Risks, University of Oxford

Professor Nick Jennings FREng, Vice Provost, Imperial College London

Dr Will Lang, Head of Civil Contingencies Services, Met Office

Dr Kristen MacAskill, Assistant Professor, University of Cambridge

Dr Jonathan Rougier, Risk Consultant, Atomic Weapons Agency

Paul Taylor FREng, Non-Executive Director, Morgan Stanley

References

1 *Critical capabilities: strengthening UK resilience*, Royal Academy of Engineering, 2021; *Infrastructure resilience roundtable: ensuring resilient national infrastructure systems*, Royal Academy of Engineering, 2020.

2 *Global Britain in a competitive age: The integrated review of security, defence, development and foreign policy*, [Policy paper], Cabinet Office, 2 July 2021.

3 *National Risk Register*, (2020 ed.), Cabinet Office, 18 December 2020.

4 *Government response to Preparing for Extreme Risks: Building a Resilient Society*, [Policy paper], Cabinet Office, 17 March 2022.

5 *Risk management – risk assessment techniques*, (2nd ed.), BS EN IEC 31010:2019, British Standards Institution, June 2019.

6 *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands*, (rev. ed.), J. van der Horst et al., Ministry of Security and Justice, Autumn 2012.

7 *Reasonable worst-case planning scenario, 30 July 2020*, Scientific Pandemic Influenza Group on Modelling, Operational sub-group (SPI-M-O), Scientific Advisory Group for Emergencies, 5 February 2021.

8 *Scenario development and foresight analysis: Exploring options to inform choices*, K. Wiebe et al., *Annual Review of Environment and Resources*, 43, pp. 545–570, 2018.

9 *Aspirational city futures: A short review of Foresight approaches*, D. V. L. Hunt and C. D. F. Rogers, Foresight Future of Cities Project, 2019.

10 *The futures toolkit: tools for futures thinking and foresight across UK government* (ed. 1.0), Government Office for Science, November 2017.

11 *Shell Scenarios*, Shell Global (accessed 17 September 2021).

12 *Future Energy Scenarios 2022*, National Grid ESO, July 2022.

13 *The risks you can't foresee*, R. S. Kaplan et al., *Harvard Business Review*, November–December 2020.

14 *The optimism bias*, T. Sharot, *Current Biology*, 21, 23, pp. R941– R945, 6 December 2011.

15 *Accelerated Expertise: Training for High Proficiency in a Complex World*, R. R. Hoffman et al., Psychology Press, 2013.

16 *Imagining grim stories to reduce redundant deliberation in critical incident decision-making*, Alison et al., *Public Money & Management*, 1 September 2021.

17 *Red teaming handbook* (3rd ed.), UK Ministry of Defence, June 2021.

18 *Risk management – risk assessment techniques*, (2nd ed.), BS EN IEC 31010:2019, British Standards Institution, June 2019.

19 *Risk assessment techniques*, T. M. Dougherty, in *Handbook of occupational safety and health* (2nd ed.), pp. 127–178, Wiley, 1999.

20 *Critical capabilities: Strengthening UK resilience*, Royal Academy of Engineering, p. 60, 2021. See Annex V – Glossary for risk terminology.

21 *C40 infrastructure interdependencies + climate risks report*, C40 and AECOM, Spring 2017.

22 '*Hazard*', Terminology, United Nations Office for Disaster Risk Reduction, April 2021.

23 *Review of environmental multi-hazards research and risk assessments*, (Engineering Geology & Infrastructure Programme Open Report OR/18/057), R. Ciurean et al., British Geological Survey, 2018.

24 *A review of quantification methodologies for multi-hazard interrelationships*, A. Tilloy et al., *Earth-Science Reviews*, 196, 102881, September 2019.

25 *Risk dependency analysis (RDA) in complex projects*, C. Paolo et al., *Wiley StatsRef: Statistics Reference Online*, 21 August 2018.

26 *Resilience study research for NIC: Systems analysis of interdependent network vulnerabilities*, R. Pant et al., Environmental Change Institute, April 2020.

27 *A review of quantification methodologies for multi-hazard interrelationships*, A. Tilloy et al., *Earth-Science Reviews*, 196, 102881, September 2019.

28 *Construction of regional multi-hazard interaction frameworks, with an application to Guatemala*, J. C. Gill et al., *Natural Hazards and Earth System Sciences*, 20, pp. 149–180, 14 January 2020.

29 *Hazard impact framework:* (1st ed.), O. Gunawan et al., Natural Hazards Partnership, March 2017.

30 *WMO guidelines on multi-hazard impact-based forecast and warning services*, (WMO no. 1150), World Meteorological Organization, 2015.

31 *Hazard impact modelling*, Natural Hazards Partnership (accessed 18 August 2021).

32 *Weather warnings guide*, Met Office (accessed 3 September 2021).

33 *Using Bayesian networks for risk assessment in healthcare system*, B. Zoullouti et al., in *Bayesian networks – advances and novel applications*, Douglas McNair, IntechOpen, 2019.

34 *Bayesian networks in environmental risk assessment: a review*, L. Kaikkonen et al., *Integrated Environment Assessment and Management*, 17, 1, pp. 62–78, 2020.

35 *Bayesian networks*, (technical report no. 5), M. Horny, 18 April 2014.

36 *Experts in uncertainty*, R. M. Cooke, Oxford University Press, 1991.

37 *Multidimensional well-being: a Bayesian networks approach*, (working paper no. 399), L. Ceriani and C. Gigliarano, ECINEQ, Society for the Study of Economic Inequality, 2016.

38 *Coronavirus (COVID-19) risk assessment*, NHS Digital (accessed 9 August 2021).

39 *COVID-19 population risk assessment*, NHS Digital (accessed 9 August 2021)

40 *Living risk prediction algorithm (QCOVID) for risk of hospital admission and mortality from coronavirus 19 in adults: national derivation and validation cohort study*, A. K. Clift et al., BMJ, 371, m3731, 2020.

41 *Multiple hazard uncertainty visualization challenges and paths forward*, L. Padilla et al., *Frontiers in Psychology*, 19 July 2021.

42 *Risk management – vocabulary*, ISO guide 73:2009, International Organization for Standardization, November 2009.

43 *Resilience reimagined: a practical guide for organisations*, National Preparedness Commission, 2021.

References

44 *Resilience in practice: five principles to enable societies to cope with extreme weather events*, K. de Bruijn et al., *Environmental Science and Policy*, 70, pp. 21–30, 2017.

45 *Re/insurance approaches to inform the National Security Risk Assessment methodology review*, T. Thomson and A. Jackman, Royal Geographical Society (with IBG), 2021.

46 *Lines of defence/layers of protection analysis in the COMAH context*, A. Franks, Health and Safety Executive, 1999.

47 *Risk management – risk assessment techniques*, (2nd ed.), BS EN IEC 31010:2019, British Standards Institution, June 2019.

48 *Safety assessment principles for nuclear facilities*, Office for Nuclear Regulation, 2014 (January 2020 rev.)

49 *Guidance on the demonstration of ALARP (as low as reasonably practicable)*, NS-TAST-GD-005 (rev. 11), Office for Nuclear Regulation, November 2020.

50 *Improving shale gas safety with well integrity management*, L. Smith, *Scottish Energy News*, April 2020.

51 *Risk management – risk assessment techniques*, (2nd ed.), BS EN IEC 31010:2019, British Standards Institution, June 2019.

52 *Analyses of Crisis Scenarios 2019*, Norwegian Directorate for Civil Protection (DSB), 2019.

53 Adapted from *Risk management – risk assessment techniques* (2nd ed.), BS EN IEC 31010:2019, British Standards Institution, June 2019.

54 *TE2100 plan*, Thames Estuary 2100, Environment Agency, November 2012.

55 *Resilience engineered*, [Film series], K. MacAskill, The Resilience Shift, 2021.

56 *Fostering resilience-oriented thinking in engineering practice*, K. MacAskill et al., *Engineering Sustainability*, 173, 7, pp. 356–364, 2020.

57 *Towards trusted data sharing: guidance and case studies*, Royal Academy of Engineering, 2018.

58 *UK climate change risk assessment 2022*, [Policy paper], Department for Environment, Food & Rural Affairs, 17 January 2022.

59 *2021 progress report to Parliament*, Climate Change Committee, 24 June 2021.

60 *Living without electricity: one city's experience of coping with loss of power*, Royal Academy of Engineering, May 2016.

61 *Winter is coming: risks for interdependent infrastructure*, [Event note], Royal Academy of Engineering, 2020.

62 *Supply chain challenges, lessons learned and opportunities*, National Engineering Policy Centre, Royal Academy of Engineering, July 2020.

63 *Enhanced Warnings*, National Preparedness Commission, December 2021.

64 *Digital twins for the build environment*, The Institute of Engineering and Technology, 2019.

65 *Data readiness: lessons from an emergency*, DELVE report no. 7, Royal Society, 24 November 2020.

66 The *Global Health Security index* was developed by the Nuclear Threat Initiative, the John Hopkins Center for Health Security, and the Economist Intelligence Unit (accessed 5 August 2021).

67 *Engineering better care: a systems approach to health and care design and continuous improvement*, Royal Academy of Engineering, August 2017.

68 *Policy Fellowships*, Royal Academy of Engineering (accessed 10 November 2022).

69 Adapted from *Engineering better care: a systems approach to health and care design and continuous improvement*, Royal Academy of Engineering, Figure 5, p. 31, August 2017.

70 *Responding to emergencies: the UK central government response*, Cabinet Office, 19 April 2013.

71 *Evaluating UK natural hazards: the national risk assessment*, [Research briefing], Parliamentary Office for Science and Technology, 24 April 2019.

72 *The government's preparedness for the COVID-19 pandemic: lessons for government on risk management*, (HC 735), National Audit Office, 19 November 2021.

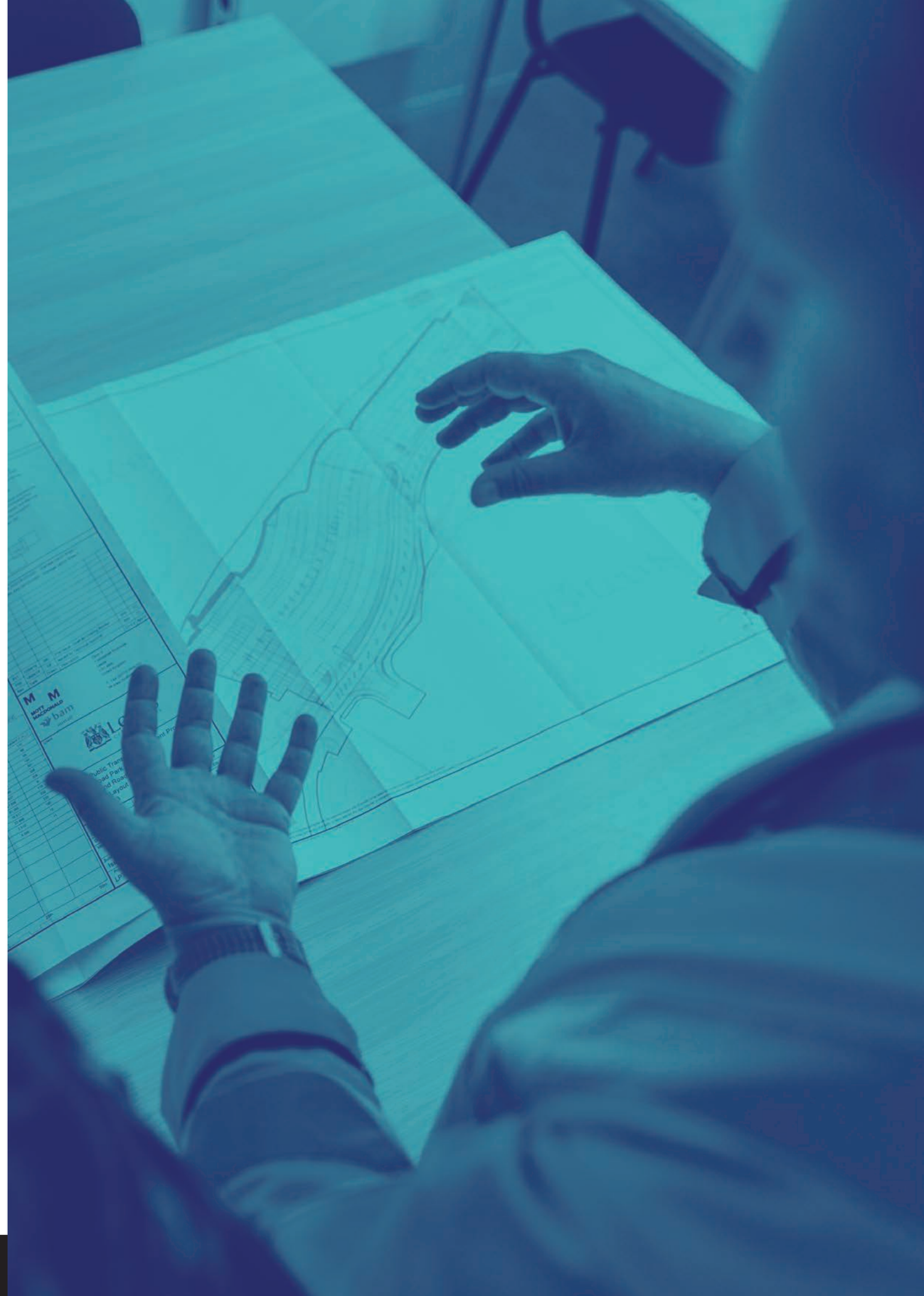
73 Reproduced from *National risk register* (2020 ed.), Cabinet Office, pp. 9–10, 18 December 2020.

74 The ONS has developed mechanisms for collating indicators for their health impacts and crime index that may be transferable; see *Developing the Health Index for England: 2015 to 2018*, Office for National Statistics (accessed 16 August 2021).

75 The *Scottish Risk Assessment* has adopted a five-year timeline, with review every two years, so that the magnitude of the risk is still understood even if the two-year review timelines are proving challenging to meet.

76 *Safer Complex Systems*, Engineering X, Royal Academy of Engineering, 2019.

77 *National resilience strategy: call for evidence*, [Consultation outcome], Cabinet Office, 13 July 2021.



Royal Academy of Engineering

The Royal Academy of Engineering is harnessing the power of engineering to build a sustainable society and an inclusive economy that works for everyone.

In collaboration with our Fellows and partners, we're growing talent and developing skills for the future, driving innovation and building global partnerships, and influencing policy and engaging the public.

Together we're working to tackle the greatest challenges of our age.

What we do

TALENT & DIVERSITY

We're growing talent by training, supporting, mentoring and funding the most talented and creative researchers, innovators and leaders from across the engineering profession.

We're developing skills for the future by identifying the challenges of an ever-changing world and developing the skills and approaches we need to build a resilient and diverse engineering profession.

INNOVATION

We're driving innovation by investing in some of the country's most creative and exciting engineering ideas and businesses.

We're building global partnerships that bring the world's best engineers from industry, entrepreneurship and academia together to collaborate on creative innovations that address the greatest global challenges of our age.

POLICY & ENGAGEMENT

We're influencing policy through the National Engineering Policy Centre – providing independent expert support to policymakers on issues of importance.

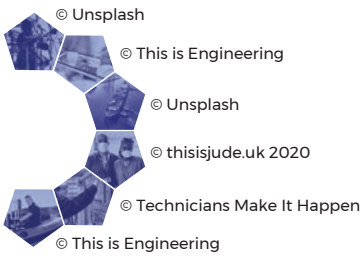
We're engaging the public by opening their eyes to the wonders of engineering and inspiring young people to become the next generation of engineers.

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel 020 7766 0600
www.raeng.org.uk
@RAEngNews

Registered charity number 293074

Front cover images:



© Unsplash
© This is Engineering
© Unsplash
© thisisjude.uk 2020
© Technicians Make It Happen
© This is Engineering