Item 19
For Information

National Risk Register

2023 edition

HM Government

CONTENTS

Foreword 4

Chapter 1: Introduction 5
What is different in this edition? 7
How does the government plan for risk? 8
Who should use the National Risk Register (NRR)? 9

Chapter 2: Risk assessment methodology and matrix 10
How are risks identified and assessed? 10
Assessing likelihood 11
Assessing impact 12
Expert challenge 13
Risk matrix 14
Response capability requirements 14
2023 NRR matrix 15
Chronic risks 17

Chapter 3: Individuals and communities 20
Preparedness advice 21
Supporting communities and volunteering 24
Guidance for responding organisations 24
Community volunteering and resilience building 25
Mental health needs in emergencies and crises 27
Identifying people who could be vulnerable in emergencies and crises 28

Chapter 4: Risk summaries 30
Terrorism 31
International terrorist attack 32
Northern Ireland related terrorism 33
Terrorist attacks in venues and public spaces: explosive devices 34
Terrorist attacks in venues and public spaces: marauding attacks 35
Malicious maritime incident 36
Malicious rail incident 37
Malicious aviation incident 38
Strategic hostage taking 39
Assassination of a high-profile public figure 41
Chemical, Biological, Radiological and Nuclear (CBRN) attacks 43
Malicious attack on chemicals infrastructure 45
Conventional attack: gas infrastructure 46
Cyber attack: gas infrastructure 47
Conventional attack: electricity infrastructure 48
Cyber attack: electricity infrastructure 49
Conventional attack: civil nuclear 50
Cyber attack: civil nuclear 51
Conventional attack: fuel supply infrastructure 52
Cyber attack: fuel supply infrastructure 53
Attack on government 54

Cyber 55
Cyber attack: health and social care system 56
Cyber attack: transport sector 58
Cyber attack: telecommunications systems 59

State threats 61
Malicious attack: UK financial CNI 62
Cyber attack: UK retail bank 63
Total loss of transatlantic telecommunications cables 64

Geographic and diplomatic risks 65
Disruption of Russian gas supplies to Europe 66
Disruption to global oil trade routes 67

Accidents and systems failures 68
Major adult social care provider failure 69
Insolvency of supplier(s) of critical services to the public sector 71
Insolvency affecting fuel supply 73
Rail accident 75
Large passenger vessel accident 77
Major maritime pollution incident 79
Incident (grounding/sinking) of a vessel blocking a major port 81
Accident involving high-consequence dangerous goods 83
Aviation collision 85

Malicious drone incident 87
Disruption of space-based services 89
Loss of Positioning, Navigation and Timing (PNT) services 91
Simultaneous loss of all fixed and mobile forms of communication 93
Failure of the National Electricity Transmission System (NETS) 95
Regional failure of the electricity network 97
Failure of gas supply infrastructure 99
Civil nuclear accident 101
Radiation release from overseas nuclear site 103
Radiation exposure from transported, stolen or lost goods 105
Technological failure at a systemically important retail bank 107
Technological failure at a UK critical financial market infrastructure 109
Accidental fire or explosion at an onshore major hazard (COMAH) site 111
Accidental large toxic chemical release from an onshore major hazard (COMAH) site 113
Accidental fire or explosion on an offshore oil or gas installation 115
Accidental fire or explosion at an onshore fuel pipeline 117
Accidental fire or explosion at an onshore major accident hazard pipeline 119
Accidental work-related (laboratory) release of a hazardous pathogen 121
Reservoir/dam collapse 123
Water infrastructure failure or loss of drinking water 125
Food supply contamination 127
Major fire 129

Natural and environmental hazards 131
Wildfire 132
Volcanic eruption 134
Earthquake 136
Humanitarian crisis overseas: natural hazard event 138
Disaster response in the Overseas Territories 140
Severe space weather 142
Storms 144
High temperatures and heatwaves 146
Low temperatures and snow 148
Coastal flooding 150
Fluvial flooding 152
Surface water flooding 154
Drought 156
Poor air quality 158

Human, animal and plant health 160
Pandemic 161
Outbreak of an emerging infectious disease 163
Animal disease: major outbreak of foot and mouth disease 165
Animal disease: major outbreak of highly pathogenic avian influenza 167
Animal disease: major outbreak of African horse sickness 169
Animal disease: major outbreak of African swine fever 171
Major outbreak of plant pest: *Xylella fastidiosa* 173
Major outbreak of plant pest: *Agrilus planipennis* 175

Societal 177
Public disorder 178
Industrial action 180
Reception and integration of British nationals arriving from overseas 182

Conflict and instability 184
Deliberate disruption of UK space systems and space-based services 185
Attack on a UK ally or partner outside NATO or a mutual security agreement requiring international assistance 187
Attack against a NATO ally or UK-deployed forces, which meets the Article 5 threshold 188
Conventional attack on the UK mainland or overseas territories 189
Nuclear miscalculation not involving the UK 190

Foreword

The UK is facing an ever-changing and growing set of risks. Even in the 3 years since we published our last National Risk Register in 2020, we have seen the barbaric invasion of Ukraine by Russia, the wide-ranging and long-lasting effects of the COVID-19 pandemic, and the increasing impact of climate change on our day-to-day lives. Technologies such as artificial intelligence (AI) are transforming our world – bringing with them opportunities, but also a number of risks.

This country has overcome countless challenges before, but I am determined to build on our national resilience so that we are prepared for whatever the future holds. To do that, we need to be more open than ever about the risks we face. Government cannot tackle these challenges alone; due to our increasingly complex and interconnected world, all of society needs to work together to strengthen our defences and build a more resilient nation.

That is why we are publishing a new and refreshed National Risk Register. This document reflects our more sophisticated understanding of the risk landscape following events such as COVID-19.

Crucially, the Register is more transparent than ever. For the first time, it is based directly on the government's internal, classified National Security Risk Assessment. Information has only been excluded from the document where there is a specific reason to do so, for example for national security reasons or for commercial confidentiality. We are giving businesses and other organisations as much information as possible about the risks they face, so that they can use this knowledge to support their own planning, preparation and response.

By focusing on our collective resilience, we can help the nation be more safe, more secure – and in turn, more prosperous. This National Risk Register plays a vital role in that process, allowing us to build towards an even brighter future.

The Rt Hon Oliver Dowden CBE MP

Deputy Prime Minister, Chancellor of the Duchy of Lancaster and Secretary of State for the Cabinet Office

Chapter 1

Introduction

Introduction

The National Risk Register (NRR) is the external version of the National Security Risk Assessment (NSRA), which is the government's assessment of the most serious risks facing the UK.

The UK faces a broad and diverse range of risks, including threats to lives, health, society, critical infrastructure, economy and sovereignty. Risks may be non-malicious, such as accidents or natural hazards, or they may be malicious threats from malign actors who seek to do us harm.

The risks that meet the threshold for inclusion in the NRR would have a substantial impact on the UK's safety, security and/or critical systems at a national level. The NRR includes information about 89 risks, within 9 risk themes – although several risks could be categorised under more than one theme. These are:

- Terrorism
- Cyber
- State threats
- Geographic and diplomatic
- Accidents and systems failures
- Natural and environmental hazards
- Human, animal and plant health
- Societal
- Conflict and instability

The NRR assesses the likelihood and impact for each risk, following a rigorous and well-tested methodology (see Chapter 2). Risks can manifest in different ways, with different levels of severity. To ensure the UK is prepared for a broad range of scenarios, the NRR sets out a **'reasonable worst-case scenario'** for each risk. These scenarios are not a prediction of what is most likely to happen, instead they represent the worst plausible manifestation of that particular risk (once highly unlikely variations have been discounted). This enables relevant bodies to undertake proportionate planning. The NRR includes information on the capabilities required to respond to and recover from the emergency, should the risk materialise.

These are not the only risks facing the UK. The NRR focuses on 'acute' risks, which are discrete events requiring an emergency response. In addition, the UK faces a range of serious 'chronic' risks, which are long-term challenges that gradually erode our economy, community, way of life, and/or national security. To make the NRR most usable by resilience practitioners, these 'chronic' risks are not included in the NRR. This is a reflection of the need for a separate process for identifying and managing these risks, and the government is also focused on this. As set out in the Integrated Review Refresh, the government is establishing a new process for identifying and assessing these risks.

This edition of the NRR is based directly on the NSRA – an internal, classified risk assessment that is used within government and by local resilience forums and their equivalents in Scotland and Northern Ireland. The NSRA is produced using a rigorous and well-tested methodology, based on international best practice. It draws on input and challenge from hundreds of experts from UK Government departments, devolved administrations, the government scientific community, intelligence and security agencies, and independent experts. The process is evidence led with 25,000 pieces of data used in the latest full assessment, finalised in autumn 2022.

What is different in this edition?

The UK Government Resilience Framework, published in December 2022, set out the core principle that developing a shared understanding of the risks we face is fundamental: it must underpin everything that we do to prepare for and recover from crises. To meet this aim, the government is committed to sharing its assessments externally wherever possible.

For the first time since the NRR was first published in 2008, this edition of the NRR aligns with the structure and content of the classified internal NSRA, and is based on the same methodology. The government has declassified more risk information than ever before, adopting a transparent by default approach to the NRR, so that risk practitioners can see more clearly how the government identifies and assesses risks. Only in a small number of cases has highly sensitive information not been included, for national security or commercial reasons.

The 2023 NRR also reflects changes to the underpinning methodology of the NSRA. Over the past 2 years, the UK Government has led the most substantial review of the NSRA since its inception, including external challenge from the Royal Academy of Engineering. The review was also informed by the House of Lords special inquiry into risk assessment and risk planning. Although the fundamentals of the NSRA remain consistent, we identified a set of significant changes to ensure the NSRA is comprehensive, accurate and usable. Key changes include:

- Focus on acute risks: as above, to make our risk products most usable by resilience practitioners, they are now focused on discrete events that may require an emergency response. Chronic risks are not included; the government continues to address these through ongoing policy and operational work.
- Longer assessment timescales: non-malicious risks are now assessed over 5 years as they can be assessed with confidence over a longer timeframe. Assessment timescales for malicious risks remain at 2 years.
- New and updated impact measures: learning lessons from COVID-19, a new impact indicator was included on the government's ability to deliver services. Other indicators were updated, such as disruption to education and child services.

COVID-19 pandemic

The most significant risk to materialise in the UK in recent years has been the COVID-19 pandemic. This has impacted all aspects of society and will have consequences into the future.

The risk of a pandemic has long been identified as one of the most serious risks facing the UK. The reasonable worst-case scenario used for planning purposes has in previous versions been based on an influenza-like illness pandemic. Any new pathogen transmitted by the respiratory route is likely to share characteristics with influenza in that it can spread rapidly via close proximity, can travel rapidly and there are few easy immediate countermeasures. It has therefore been a planning assumption that a plan for pandemic influenza would have considerable overlap with a plan for other diseases easily transmitted by the respiratory route.

The lessons from COVID-19 have been incorporated into the government's risk assessment methodology. The reasonable worst-case scenario has been reshaped into a more generic pandemic scenario reflecting a broader range of possible manifestations, and additional impacts, measures and data have been incorporated into the assessment.

How does the government plan for risk?

The government has comprehensive plans to build resilience to specific risks, including those set out in the NRR. For example, the government has published the Net Zero Strategy, the National Cyber Strategy, the Government Food Strategy, the British Energy Security Strategy, and the UK Biological Security Strategy.

However, no risk assessment will ever be able to identify and assess every possible risk. The NSRA uses common consequences of risks – such as mass fatalities and casualties, contaminated environments and disruption to a range of critical services. The government develops generic capabilities that can be used to respond to these impacts, regardless of the risk that caused them. This means the government can respond flexibly to the widest range of risks.

Although the UK Government has an important role to play in assessing and planning for risks, the local level is critical to the UK's resilience. The 38 Local Resilience Forums (LRFs) in England, the 4 LRFs in Wales, 3 Regional Resilience Partnerships (RRPs) in Scotland and Emergency Preparedness Groups in Northern Ireland play a critical role in bringing local responders, such as the emergency services, together to plan for risks. Local resilience partners produce Community Risk Registers (CRRs), which focus on the highest priority risks in each local area. The NRR should be read in conjunction with the CRR for the relevant local area.

Who should use the National Risk Register (NRR)?

The NRR is designed for a broad range of risk and resilience practitioners. This includes, but is not limited to:

- Practitioners, including in voluntary and community sector organisations, who may play a central role in planning for and responding to emergencies and crises but who may not have formal contingency planning responsibilities.
- Businesses, including small- and medium-sized enterprises, and those who operate critical national infrastructure (CNI), who have a need to understand the most serious risks that could impact their business continuity.
- Academics and experts from a wide range of disciplines and backgrounds, who play a critical role by providing external challenge.

This edition of the NRR is not targeted at the general public. Instead, government (at both the national and local level) will continue to provide tailored guidance and communications to help people understand the risks that are most likely to affect them, and the specific actions they can take to protect themselves. For example:

- The 'Run, Hide and Tell' campaign helps people stay safe in the event of a marauding terrorist attack.
- The 'WeatherReady' campaign helps individuals, families and communities prepare for and cope with severe weather.
- The 'Cyber Aware' campaign provides advice on how to stay secure online.

In addition, the UK Government has launched the Emergency Alerts service, to get urgent messages quickly to mobile phones when there is a risk to life, and provide clear instructions about how best to respond. While the alert service will initially be used as part of our severe weather and flood warning response capabilities, it could also serve a wider purpose and be used as an emergency response for other scenarios, such as public health emergencies, fires and extreme weather.

Risk assessment methodology and matrix

The 2023 NRR is based directly on the government's internal National Security Risk Assessment completed in 2022.

How are risks identified and assessed?

Risks were identified for inclusion in the NSRA by consulting a wide range of experts from across UK Government departments, the devolved administrations, the government scientific community and outside of government (for example, in partner agencies, academic institutions and industry). Risks are owned by departments or other government organisations, who are responsible for assessing the impact and likelihood of their risks.

Risks in the NSRA and NRR are assessed as 'reasonable worst-case scenarios'. These scenarios represent the worst plausible manifestation of that particular risk (once highly unlikely variations have been discounted) to enable relevant bodies to undertake proportionate planning. The scenarios for each risk were produced in consultation with experts and data was collected from a wide range of sources.

As set out in Chapter 1, the NSRA does not aim to capture every risk that the UK could face. Instead it aims to identify a range of risks that are representative of the risk landscape and can serve as a cause-agnostic basis for planning for the common consequences of risks.

Assessing likelihood

Government departments and agencies responsible for assessing non-malicious risks (for example, severe weather events or accidents) assessed the likelihood of their reasonable worst-case scenario occurring within the assessment period (which is 5 years for non-malicious risks and 2 years for malicious risks) using extensive data, modelling, and expert analysis. The resulting likelihood (expressed as a percentage) is then scored on a scale from 1 to 5, where a score of 1 represents the lowest likelihood and 5 represents the highest likelihood.

The likelihood of malicious risks (for example, terrorist attacks or cyber attacks) is assessed differently, with scores being calculated via the Professional Head of Intelligence Assessment (PHIA) yardstick (see Table 1 to the right). The intent of malicious actors to carry out an attack is balanced against an assessment of their capability to conduct an attack and the vulnerability of their potential targets to an attack. These 3 parameters, informed by data and expert insight, are collated together to form one likelihood score (expressed as a percentage), which is comparable with the likelihood of the non-malicious risks and can be plotted on the same matrix.

Likelihood is presented as the percentage chance of the reasonable worst-case scenario occurring at least once in the assessment timescale and is scored on a 1-5 scale. For both malicious and non-malicious risks, a 1-5 score is evaluated on the following scale:

Score	Percentage chance	PHIA yardstick designation
5	>25%	Almost certain (95-100%) Highly likely (80-90%) Likely or probable (55-75%) Realistic probability (40-50%) Unlikely (25-35%)
4	5-25%	Highly unlikely (5-25%)
3	1-5%	Remote chance (0-5%)
2	0.2-1%	
1	<0.2%	

Table 1: Summary detailing the alignment of the final 1-5 likelihood score for NSRA risks, its corresponding percentage chance and the label using the PHIA yardstick.

We use a scale of 1 to 5 for both malicious and non-malicious risks to allow like-for-like comparison between risks, and as a tool to help effective risk visualisation. The highest score (5) represents a greater than 25% likelihood. The reason that this number is relatively low is that all risks in the NSRA are relatively low likelihood events.

Assessing impact

All risks in the NSRA have a wide range of impacts, whether on individuals, businesses, regions or the whole country. To capture this range, the NSRA assesses impact across 7 broad dimensions:

- The impact on **human welfare**, including fatalities directly attributable to the incident, casualties resulting from the incident (including illness, injury and mental health impacts), and evacuation and shelter requirements.
- **Behavioural impacts**, including changes in individuals' behaviour or levels of public outrage.
- The impact on **essential services**, including disruption to transport, healthcare, education, financial services, food, water, energy, emergency services, telecommunications and government services.
- **Economic damage**, including numbers of working hours lost.
- **Environmental impact**, including damage to the environment.
- The impact on **security**, including on law enforcement agencies, armed forces, border security, and the criminal justice system.
- **International impacts**, including damage to the UK's international relations and ability to project soft power, disruption to international development, violation of international law and norms, and international displacement and migration.

In addition to the impacts listed, qualitative data is collected on the disproportionate impacts of the reasonable worst-case scenarios on vulnerable individuals and groups. In accordance with the Public Sector Equality Duty, risk-owning government departments and agencies are required to pro-actively consider how they can contribute to the advancement of equality and the prevention of discrimination by taking into account the potential effects of their policies, functions, and service delivery on groups with protected characteristics. They are encouraged to go further than the defined list of protected characteristics and to collect data to inform their assessments.

The assessment and scoring of a risk focus primarily on domestic impacts – even where the risk occurs internationally. Each of the dimensions listed left is scored on a scale of 0 to 5 based on the scope, scale and duration of the harm that the reasonable worst-case scenario could foreseeably cause (see Table 2 on page 13 for a selection of example impact scale indicators). These scores are then combined to provide a single overall impact score.

	Impact				
	1	2	3	4	5
Fatalities	1-8	9-40	41-200	201-1,000	>1,000
Casualties	1-18	17-80	81-400	400-2,000	>2,000
Economic cost	Millions of £	Tens of millions £	Hundreds of millions £	Billions of £	Tens of Billions £

Table 2: Example impact scale indicators for fatalities, casualties and economic cost.

Expert challenge

To ensure that the assessment process is robust, risks are reviewed by a network of experts. These include professionals from industry, charities and academia, as well as subject matter experts within government. The role of experts is to provide challenge by:

- Supplementing, clarifying or refining the submitted information;
- Identifying areas of uncertainty;
- Helping to resolve inconsistencies in the scoring of impact;
- Helping to improve communication of impact information; and
- Identifying long-term trends that provide context to the submitted risk.

To facilitate the provision of expert advice, thematic impact review groups were set up to bring together a mix of internal and external expertise. These groups covered individual risk themes (for example, cyber, chemical, biological, radiological or nuclear risks), along with the calculated impacts of different risks (for example, impacts on essential services or the environment) and a group to look specifically at the disproportionate impacts of the risk scenarios on vulnerable individuals and groups.

Risk matrix

The likelihood and impact of risks are plotted onto a matrix, enabling users to compare risks and inform contingency planning. The NRR matrix below presents the impact and likelihood of a plausible worst-case scenario manifestation of each risk. To enable large differences in impact and likelihood to be shown on the same matrix, non-linear scales have been used. This allows the overall risk landscape to be compared.

The vertical axis shows the impact of each risk. A score of 1 corresponds to the lowest impact, and a score of 5 corresponds to the highest impact. The impact scale is logarithmic and is reflected by the matrix boxes increasing in size.

The horizontal axis shows the likelihood of each risk occurring at least once in the assessment period (2 years for malicious risks, 5 years for non-malicious risks).

The likelihood scale is logarithmic and is reflected by the matrix boxes increasing in size, moving from the bottom left of the matrix to the top right. A score of 1 corresponds to the lowest likelihood, and a score of 5 corresponds to the highest likelihood. The likelihood range in each column, moving from left to right, is 5 times greater than the previous column. For example, a score 3 risk is approximately 5 times more likely to occur than a score 2 risk.

Uncertainty is an inherent aspect of risk assessment. Impact and likelihood scores are given a confidence rating that takes account of:

- Quality and reliability of the evidence base;
- Assumptions used in the analysis; and
- External factors that may affect impact and likelihood for example, global events.

Uncertainty in the assessment of the risk is represented on the main summaries for the risks in Chapter 4, by the lines extending from the plotted dot on each page.

Although a majority of individual risks have been plotted onto the matrix, a number of the most sensitive risks have been thematically grouped, bringing together risks that share similar risk exposure and require similar capabilities to prepare, mitigate and respond. This has been done in order to strike the best possible balance between being transparent about risk information while protecting sensitive information, for example relating to national security or commercial considerations. The position of each grouped risk on the matrix below is an average of the impact and likelihood scores of all the different risks that belong to that category.

Additional scenarios are provided for a given risk if they would result in substantially different impacts or require significantly different planning. Risks that are marked with a number and a letter represent multiple scenarios of the same risk. For example, the flooding risks are 51a, b and c (coastal, fluvial and surface water flooding respectively).

Response capability requirements

The response capability requirements listed in the text are non-exhaustive. They are intended to provide a high-level overview of the potential response capability that may be needed.

IMPACT	1 <0.2%	2 0.2-1%	3 1-5%	4 5-25%	5 >25%
Catastrophic 5	28, 29		9, 26a	54	
Significant 4	21	24, 38, 56a	27, 49, 51a, 51b, 51c, 61	10, 47, 50, 55, 63	
Moderate 3	17, 32, 33, 34, 35, 36, 56c	12, 22, 23, 52	25, 26b, 31a, 45, 53, 56b	4, 8, 11, 40, 43, 48, 60	3, 31b, 46, 62
Limited 2	18, 19, 30, 37	5, 16, 41, 42	14, 20, 56d, 58, 59	7, 13, 57b	2, 6
Minor 1	44	39		15	1, 57a

LIKELIHOOD

Terrorism, cyber and state threats

1. International terrorist attack
2. Northern Ireland related terrorism
3. Terrorist attacks in venues and public spaces
4. Terrorist attacks on transport
5. Strategic hostage taking
6. Assassination of a high-profile public figure
7. Smaller-scale CBRN attacks
8. Medium-scale CBRN attacks
9. Larger-scale CBRN attacks
10. Conventional attacks on infrastructure
11. Cyber attacks on infrastructure

Geographic and diplomatic

12. Disruption to global oil trade routes

Accidents and systems failures

13. Major adult social care provider failure
14. Insolvency of supplier(s) of critical services to the public sector
15. Insolvency affecting fuel supply
16. Rail accident
17. Large passenger vessel accident
18. Major maritime pollution incident
19. Incident (grounding/sinking) of a vessel blocking a major port
20. Accident involving high-consequence dangerous goods
21. Aviation collision
22. Malicious drone incident
23. Disruption of space-based services

24. Loss of Positioning, Navigation and Timing (PNT) services
25. Simultaneous loss of all fixed and mobile forms of communication
26a. Failure of the National Electricity Transmission System (NETS)
26b. Regional failure of the electricity network
27. Failure of gas supply infrastructure
28. Civil nuclear accident
29. Radiation release from overseas nuclear site
30. Radiation exposure from transported, stolen or lost goods
31a. Technological failure at a systemically important retail bank
31b. Technological failure at a UK critical financial market infrastructure
32. Accidental fire or explosion at an onshore major hazard (COMAH) site
33. Accidental large toxic chemical release from an onshore major hazard (COMAH) site
34. Accidental fire or explosion on an offshore oil or gas installation
35. Accidental fire or explosion at an onshore fuel pipeline
36. Accidental fire or explosion at an onshore major accident hazard pipeline
37. Accidental work-related (laboratory) release of a hazardous pathogen
38. Reservoir/dam collapse
39. Water infrastructure failure or loss of drinking water
40. Food supply contamination
41. Major fire

Natural and environmental hazards

42. Wildfire
43. Volcanic eruption
44. Earthquake
45. Humanitarian crisis overseas – natural hazard event
46. Disaster response in the Overseas Territories
47. Severe space weather
48. Storms
49. High temperatures and heatwaves
50. Low temperatures and snow
51a. Coastal flooding
51b. Fluvial flooding
51c. Surface water flooding
52. Drought
53. Poor air quality

Human, animal and plant health

54. Pandemic
55. Outbreak of an emerging infectious disease
56a. Animal disease – major outbreak of foot and mouth disease
56b. Animal disease – major outbreak of highly pathogenic avian influenza
56c. Animal disease – major outbreak of African horse sickness
56d. Animal disease – major outbreak of African swine fever
57a. Major outbreak of plant pest – *Xylella fastidiosa*
57b. Major outbreak of plant pest – *Agrilus planipennis*

Societal

58. Public disorder
59. Industrial action
60. Reception and integration of British Nationals arriving from overseas

Conflict and instability

61. Deliberate disruption of UK space systems and space-based services
62. Attack on a UK ally or partner outside NATO or a mutual security agreement requiring international assistance
63. Nuclear miscalculation not involving the UK

Chronic risks

Chronic risks are distinct from acute risks in that they pose continuous challenges that erode our economy, community, way of life, and/or national security. Generally, but not always, these manifest over a longer timeframe. While chronic risks also require robust government-led responses, these tend to be developed through strategic, operational or policy changes to address the challenges rather than emergency civil contingency responses. Acute risks on the other hand are risks that may require an emergency response from government, such as wildfires or biological attacks.

Chronic risks can make acute risks more likely and serious – for example, climate change can lead to an increase in the frequency and severity of weather conditions that cause floods and wildfires. Antimicrobial resistance (AMR) has the potential to exacerbate the risk of infectious diseases, for example a pandemic occurring in an environment of ineffective antibiotics could result in higher deaths from secondary bacterial infections. Another risk being examined by the government is artificial intelligence (AI). Advances in AI systems and their capabilities have a number of implications spanning chronic and acute risks; for example, it could cause an increase in harmful misinformation and disinformation, or if handled improperly, reduce economic competitiveness.

The chronic risks included in the 2020 NRR are no longer included in Chapter 4 of this edition. This is due to chronic risks no longer being included in the 2022 National Security Risk Assessment (NSRA).

The NRR is the external version of the NSRA and therefore has aligned with this change. As outlined in the Integrated Review Refresh, the government is establishing a new process for identifying and assessing a wide range of chronic risks. Listed below are a selection of examples of chronic risks previously found in the NRR.

Climate change

The UK average surface temperature has already warmed by 1.2°C since the pre-industrial period, and is predicted to warm further by mid-century, even under an ambitious decarbonisation scenario. The impact of climate change on the intensity and frequency of some climate and weather extreme events is already being observed globally, and these impacts will worsen in the future. Climate change adaptation is a priority for government, exemplified by the UK being one of the first nations in the world to enshrine climate adaptation into law within the Climate Change Act. Climate change can also contribute to longer-term changes to water availability, as well as permanent and irreversible changes such as sea-level rise and alterations to habitats and growing conditions.

Antimicrobial resistance (AMR)

AMR arises when organisms that cause infection evolve in ways to survive treatment. Although resistance occurs naturally, the use of antimicrobials in humans, animal agriculture, plants and crops, alongside unintentional exposure, including through environmental contamination and food, is rapidly accelerating the pace at which it develops and spreads. Each year AMR is estimated to cause almost 1.3 million deaths globally, and 7,600 deaths in the UK. The impacts of leaving AMR unchecked are wide-ranging and extremely costly in financial terms, but also in terms of global health, our ability to undertake modern medicine, food sustainability and security, environmental wellbeing, and socio-economic development. The UK's 5-year national action plan (NAP) sets out how the government plans to tackle AMR within and beyond our own borders. The NAP focuses on 3 key ways of tackling AMR including: reducing the need for, and unintentional exposure to, antimicrobials; optimising the use of existing antimicrobials; and investing in innovation, supply and access within human, animal and environmental settings.

Serious and organised crime (SOC)

Serious and organised crime, which featured in the 2020 NRR, is now being defined as a chronic risk and therefore removed from this iteration of the NRR. Serious and organised crime is defined as individuals planning, coordinating and committing serious offences whether individually, in groups, and/or as part of transnational networks. Organised criminals threaten the UK's economic security, costing the UK at least £37 billion every year, with nearly all serious and organised crime underpinned by illicit finance. Serious and organised crime persistently erodes the resilience of the UK's economy and communities, impacting on citizens, public services, businesses, institutions, national reputation and infrastructure.

The National Assessment Centre, which is the National Crime Agency's centre for assessed intelligence reporting, publishes an annual National Strategic Assessment that outlines a comprehensive understanding of the serious and organised crime threat to the UK, drawn from all-source intelligence from domestic and international partners.

Artificial intelligence (AI) systems and their capabilities

AI systems and their capabilities present many opportunities, from expediting progress in pharmaceuticals to other applications right across the economy and society, which the Foundation Models Taskforce aims to accelerate. However, alongside the opportunities, there are a range of potential risks and there is uncertainty about its transformative impact. As the government set out in the Integrated Review Refresh, many of our areas of strategic advantage also bring with them some degree of vulnerability, including AI. That is why the UK Government has committed to hosting the first global summit on AI Safety which will bring together key countries, leading tech companies and researchers to agree safety measures to evaluate and monitor risks from AI.

The National AI Strategy, published in 2021, outlines steps for how the UK will begin its transition to an AI-enabled economy, the role of research and development in AI growth and the governance structures that will be required.

The government's white paper on AI, published in 2023, commits to establishing a central risk function that will identify and monitor the risks that come from AI. By addressing these risks effectively, we will be better placed to utilise the advantages of AI.

Chapter 3

Individuals and communities

Individuals and communities

Preparedness advice

The information included here is for organisations that might have a role in communicating preparedness information to members of the public or to employees.

There are a number of actions individuals can take to prepare for and respond to risks. It is important for people to consider these in the context of their own specific circumstances and daily routines, as well as the risks they may face when living or working in certain locations.

1. Understand the risks

Individuals can be better prepared if they are aware of and informed about the risks that are most likely to affect them by:

- Finding out more about the risks in a specific area by reading any local community emergency preparedness information online and by taking a look at their local community risk register, which can be found by searching for the relevant area:
  – Community risk registers in England and Wales
  – Community risk registers in Scotland
- Signing up for flood alerts or weather updates.
- Checking online to see which areas are at immediate risk of flooding or are likely to flood in the future:
  – Flood risk in England
  – Flood risk in Scotland
  – Flood risk in Wales
  – Flood risk in Northern Ireland
- Taking a look at the Ready Scotland website, for information on preparing for and responding to emergencies affecting Scotland.
- Checking the Foreign, Commonwealth and Development Office's travel advice before travelling overseas.
- Reading the latest updates to the UK's Joint Terrorism Analysis Centre and Security Service's (MI5) terrorism threat levels.

More information on what the different levels mean can be found on the MI5 website.

2. Take steps to prepare

There are a number of activities that individuals could undertake to prepare for, prevent, and mitigate the impacts of risks. Many of these activities can be helpful across a range of different risks. It is important to note that not everyone will be able to undertake all of these, for a variety of reasons, including financial.

Some examples of actions that could be suggested to individuals include:

- Signing up for first aid training – courses can provide useful, potentially lifesaving, skills that can be helpful in a variety of emergency situations.
- Teaching children about how and when to call the emergency services.
- Speaking to their child's school to find out their procedures in the event of different emergency scenarios.
- Storing important documents (for example, insurance documents and key contact numbers) and important items (for example, medication and identification) in an easily accessible location in case of emergency or an evacuation at short notice (and not attempting to retrieve these items if it becomes dangerous to do so).
- Keeping some basic supplies at home such as bottled water, a torch and batteries (which is safer than candles), and a wind-up radio to get updates during a power cut.
- Knowing how to turn off gas, water and electricity in the home.
- Checking the right insurance is in place for home or business (for example, flood insurance) or travel insurance when planning a trip.
- Finding out about evacuation procedures in the workplace.
- Reading official advice on what to do in a marauding terrorist attack or how to report suspicious packages or behaviour.
- Reading advice about on how to stay secure online.
- Joining a community group or social club that is active in emergency preparedness.
- Signing up to the local authority or local utilities provider's vulnerable customer schemes and priority services (if eligible).
- Being aware of the UK Government's Emergency Alerts service and being prepared to inform others in their local area who may not have received or seen an emergency alert, in the event one is sent.

Depending on local risk assessments, individual circumstances or current events, more specific activities may be appropriate.

3. Know how to respond

If people know in advance what to do and what to expect from responding agencies during an incident, it could lead to a more effective response and reduce physical harm, stress and anxiety for those involved. In the event of an emergency, the public can play a vital role by alerting the emergency services (dialling 999) and by providing first aid, comfort and support while waiting for the emergency services to arrive.

Depending on the nature of the incident, those affected may be asked to 'go in, stay in and tune in' to local radio stations or check official sources of information online. Unless there is an obvious risk to the building, going inside and seeking further information is often the safest thing to do. People should always be guided by what they can see going on around them – for example, it is never safe to return to a building that is on fire.

In some situations, people may need to evacuate for their own safety. It is important for people not to delay evacuating properties, buildings or general locality if asked to by the responding authorities. Delaying or refusing to evacuate may put individuals' own lives at risk, as well as putting emergency responders in danger if they later have to return to properties to deliver the evacuation request again.

Depending on the incident, those impacted may be alerted to a risk via the new Emergency Alerts public information system. The system was developed to alert citizens to emergencies, both nationwide and in their local area, that represent an immediate threat to life. The technology used allows a message to be broadcast to a defined area, meaning any compatible device in or entering that area will immediately receive the message, detailing the emergency and actions people need to take to ensure their safety. A loud, siren-like sound and vibration will accompany the message to raise awareness of the hazard or threat. Alerts may also include a URL where further information is contained, and/or a helpline. Alerts will always be replicated on gov.uk/alerts, allowing the public to recover information they contain and validate their origin.

4. Help with recovery

Recovery is a complex process, beginning at the earliest opportunity and running in tandem with the emergency response. Recovery from a serious incident can last months, years or even decades. If it is safe to do so, members of affected communities are encouraged to participate in the recovery process and should be involved in determining how recovery is best achieved in their community.

In the recovery phase of an incident, members of the public who wish to help should look out for calls for support from a local authority or national and local charities, to assist with the clean-up or to help others in their community get back on their feet. As well as providing practical assistance with community recovery, members of the public can also provide support to other individuals affected by an incident, for example by listening to those who want to talk about their experiences.

It is important to look out for persistent signs of distress in trauma exposed individuals, and if symptoms do not resolve with informal support, to point the affected individuals towards professional help. See the NHS England website and Scotland's NHS Inform website for more information.

Supporting communities and volunteering

The information included here is for emergency responders to support their engagement and collaboration with non-statutory partners, such as the voluntary sector or wider communities. It can also help public and private organisations to appreciate the challenges that an emergency can bring and to make appropriate preparations.

For communities, a 'whole-of-society' approach to resilience means that where possible, communities recognise their role in, take responsibility and contribute to the UK's resilience.

Successful community resilience approaches are often based on connection and relationships. Deepened partnerships between statutory responders and the communities they serve can provide benefits and positive outcomes during emergencies, such as an increased understanding of needs in the community, public confidence and motivation to act, and better coordination and integration of collective capabilities to prepare for, respond to and recover from emergencies.

Responders should develop a broad understanding of their communities, including the health, social, financial and environmental impacts that could occur from the materialisation of risks, and the capacity and capabilities that exist within the community to support official preparedness, response and recovery activity, where appropriate.

Responders should seek ways to build community resilience so that individuals and groups are better able to deal with emergencies when they occur. This in turn can help to reduce the pressures on emergency services who can then focus their resources on vulnerable groups and those most in need.

Guidance for responding organisations

The UK Government published the Community Resilience Development Framework and guidance on 'planning the coordination of spontaneous volunteers' in 2019.

The Community Resilience Development Framework is a reference tool for the delivery of strategic approaches to community resilience development, at the local level in collaboration with non-statutory partners, such as voluntary, community and faith organisations, and businesses. It provides a framework for the development of community resilience activity that aims to reduce the impact of emergencies by ensuring that:

- Individuals, businesses, community networks and voluntary organisations are empowered to prepare, respond to, and recover from emergencies.
- Emergency responders understand, enable and integrate the capabilities of the public into emergency planning, response and recovery activity.

The framework contains a wide-ranging, but non-exhaustive, list of organisations that could contribute their capabilities to emergency management on a voluntary basis. The Voluntary and Community Sector Emergencies Partnership (a voluntary sector-led partnership) exists to bring together member organisations to deliver a more coordinated response to emergencies.

When emergencies happen, people often feel compelled to help. Professionals and volunteers train for emergencies, but other members of the community can also be involved through acts of good neighbourliness and spontaneous volunteering. Bringing people and organisations together to form effective networks is key to building community resilience, preparing for emergencies, and making the best use of all available resources.

If the worst happens, members of the public can often rally their skills and resources to help their community. No matter who wants to help, what abilities they have, or whether they have volunteered previously, there may be ways for them to help.

Guidance on planning the coordination of spontaneous volunteers is designed for emergency planners and responders to assist in the planning and management of spontaneous offers of support from the public during an emergency.

Additionally, guidance is available from the Scottish Government on the topic of Building Resilient Communities. This guidance recommends that responders consider best practice, in order to maximise the effectiveness of their work with individuals, community groups, private sector businesses and voluntary sector organisations, to help make themselves more resilient. In line with other Preparing Scotland guidance, it is drawn from existing good practice in Scottish communities.

Community volunteering and resilience building

There are numerous opportunities to volunteer across the UK. Individuals can also find out how to get involved with their community before, during and after an emergency by visiting a local volunteer centre or searching online.

Even if people feel motivated and able to help, in many cases it is best not to just turn up at the scene of an emergency and begin working. This could be dangerous and overwhelm the emergency services. Instead, it is best to get involved via the structures that have been established in the local area, so everyone can work safely for the benefit of those who need help. This means looking out for calls for support from a local authority, or national and local charities and, most importantly, performing essential acts of good neighbourliness.

Before an emergency, members of the public, community organisations and local businesses can help to build the resilience of:

- **individuals**, by raising awareness of risks and preparedness actions, for example through social media
- **households**, by advising on property refurbishment such as property flood defence measures
- **communities**, by identifying vulnerable people and helping them access support
- **organisations**, by supporting business continuity planning
- **systems and networks**, by building trusting relationships between different local and community organisations

During an emergency or crisis, the public can help – if it's safe to do so – by checking on neighbours and vulnerable people in the community to see if they need any help or assistance.

After the emergency, the public can also offer their help to clean up, help others to get back on their feet, or help their community to come to terms with the situation. Opportunities to volunteer might be available through one of the thousands of local organisations that already work at the heart of communities. Members of the public can find out how to help their community with an emergency by visiting a local volunteer centre or searching online.

Mental health needs in emergencies and crises

The information included here is for organisations who have a role to play in supporting individuals or communities involved in emergencies and crises, including organisations whose staff may be impacted.

In the immediate aftermath of a major incident or crisis, it is important to consider the mental health needs of those who may have been affected. This includes people who were directly involved, such as those present at the scene of an emergency or those who became ill during an infectious disease outbreak. It also includes emergency responders, volunteers and healthcare staff caring for people involved in the incident. It's also crucial to consider people who were indirectly involved, such as relatives of the injured, sick or deceased and anyone who may feel responsible for the incident or some aspect of the response.

There is good evidence that people who have been exposed to a traumatic event, and who experience other significantly stressful circumstances (such as financial issues or problems related to children) find it more difficult to cope in the aftermath of a traumatic event. The secondary stressors that often follow crises can persist for long periods of time. They do not end when the emergency service response concludes, but can continue well into the recovery phase of an event. However, it is important to recognise that while many people feel upset and distressed in the days and weeks after a traumatic experience, most short-term distress responses resolve without the need for professional help. Most trauma-exposed people benefit from informal support such as sharing feelings with others with similar experiences, speaking with people they trust, having a supportive line manager and colleagues, sticking to a routine and paying attention to healthy living (trying to get enough sleep, exercise and regular meals). A period of 'watchful waiting' – monitoring symptoms to see if they resolve without treatment – may be advised by a GP. All of these approaches may be beneficial to someone's mental health, but if adverse symptoms do persist a person should always seek further help from their GP.

There is good evidence that providing psychologically focused debriefing, or trauma counselling, in the immediate post-incident period is not only ineffective but may cause additional harm. Instead, it is a good idea to actively monitor those who have been directly or indirectly affected for a few months after a traumatic event. If their difficulties do not appear to be resolving, then they should be advised to speak to a healthcare professional who can assess whether or not they need formal mental health treatment.

Below is a list of useful resources to direct people to in the aftermath of a traumatic event if feeling upset or distressed:

- NHS England website
- Scotland's NHS Inform website
- The Royal College of Psychiatrists

More general advice and support related to mental health and wellbeing can be found on the NHS Every Mind Matters website.

Identifying people who could be vulnerable in emergencies and crises

It is important for organisations to be aware of which individuals might require more support in relation to emergencies and crises.

The UK is faced with a wide range of risks that could have a disproportionate impact on specific vulnerable and at-risk groups. Individuals within these groups are likely to experience higher levels of morbidity and mortality in comparison to the general population. They are also more likely to suffer financial hardship either as a direct or indirect consequence of a risk materialising. Individuals can have multiple vulnerabilities in the context of an emergency or crisis, which can have a compounding effect on their ability to respond to and recover from the event.

There are a broad range of social, financial, health and environmental determinants that can impact the ability of an individual, a household or a community, to mitigate risks and respond in emergencies. For example, across the world we have seen previous events place an inequitable burden on individuals such as:

- Those with pre-existing mental or physical health conditions or disabilities (whether living in the community or in long-term care facilities)
- Older adults
- Children
- Pregnant women
- Individuals from certain ethnic backgrounds
- Healthcare and other frontline workers
- Informal or self-employed workers
- Those in lower socio-economic groups or who are financially insecure
- Individuals exposed to abuse or violence
- Tourists
- Migrants
- Those who are socially isolated
- Individuals with less knowledge and experience related to specific risks

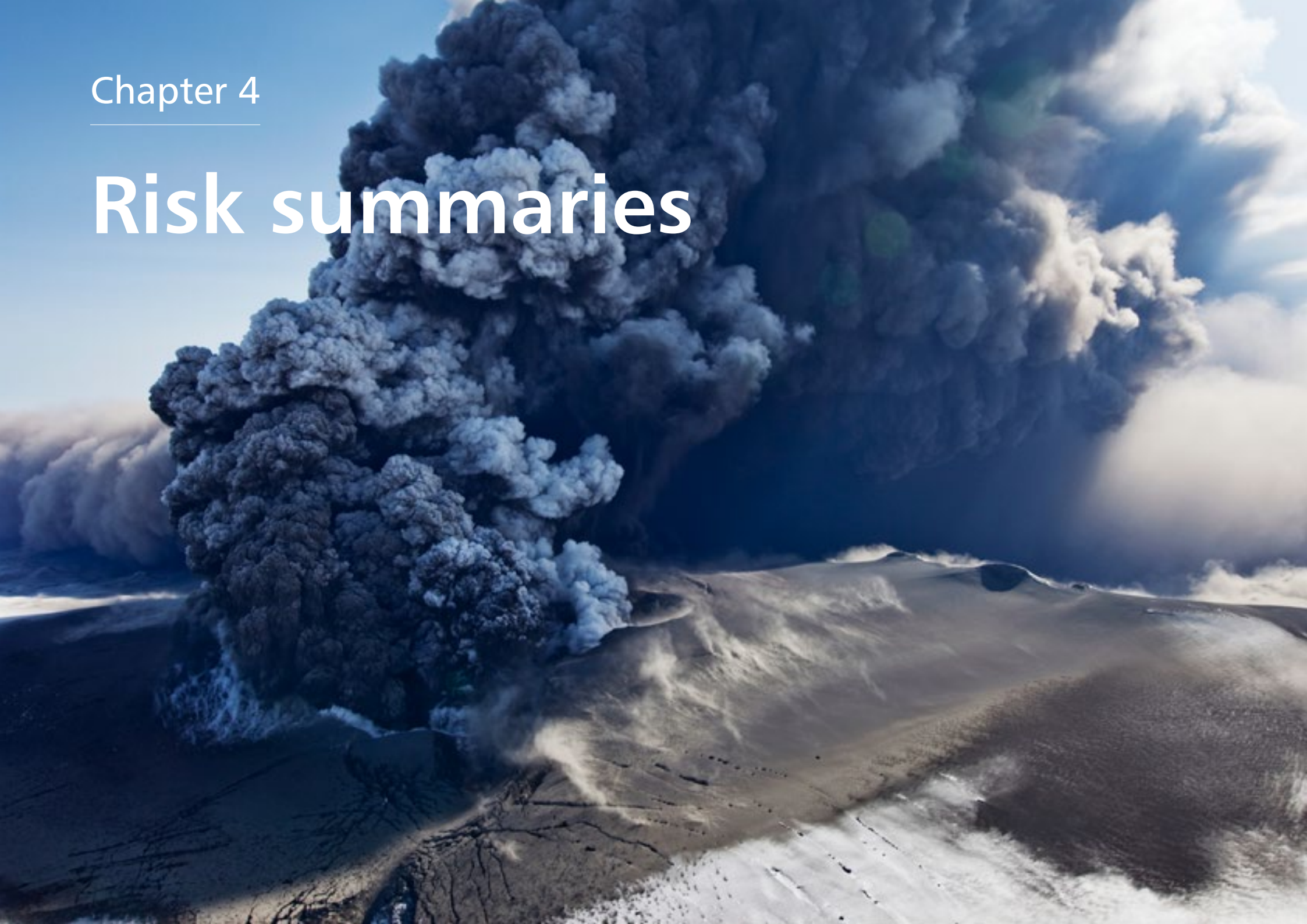
This list is not exhaustive, and different agencies and organisations have different definitions of vulnerability but it illustrates the wide range of individuals who could be considered (or could become) vulnerable in certain emergencies or crises.

Vulnerability is complex and vulnerable groups are non-static. The impacts of an emergency change over time and are influenced by other wider concurrent and contextual factors. Individuals who might be considered vulnerable in the context of one risk might not be for another. For example, older adults might be considered more vulnerable in some virus outbreaks, however could potentially have higher levels of preparedness for a significant power outage, having more experience of these types of events.

The risks discussed in Chapter 4 could result in unequal impacts for individuals, and also for communities. Every scenario is different but when planning for and responding to these risks, planners from national government, local government and community groups all have an important role to play in mitigating the disproportionate impacts on these individuals and communities. Within public bodies, the Public Sector Equality Duty requires a consideration of the potential effects of policies, functions and service delivery on groups with protected characteristics, and the inclusion of reasonable mitigations where negative impacts may be anticipated. For emergency planners, it is important to consider the role that non-statutory partners, such as voluntary, community and faith organisations can play in providing routes to engagement with vulnerable and at-risk groups.

Chapter 4

Risk summaries



Terrorism

International terrorist attack

There have been a number of terrorist attacks occurring overseas that have involved British Nationals. One such event was the incident in Tunisia in 2015, in which 30 of the victims were British.

Scenario

The reasonable worst-case scenario of this risk considers a large-scale terrorist attack occurring overseas, involving a significant number of British Nationals. There would be casualties and fatalities, which would include a diverse range of tourist nationalities.

Key assumptions for this scenario

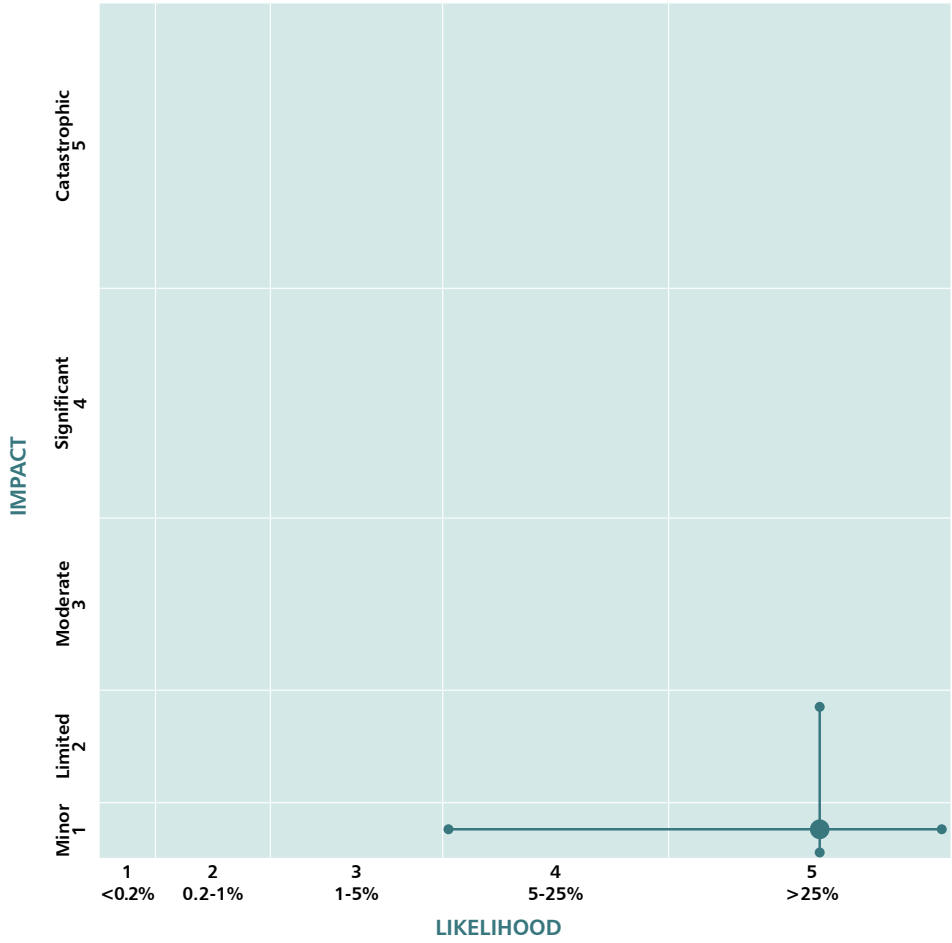
This scenario assumes that a non-state actor, likely a known terrorist group, is behind an attack.

Response capability requirements

Resilient communications systems, humanitarian assistance, victim support and UK sovereign military capability might all be required to deal with an international terrorist attack. Response and recovery would involve counterterrorism programming, security sector development assistance and access to UK support services for affected British nationals.

Recovery

This event is unlikely to directly impact UK infrastructure but there would be an impact on the tourism industry and bilateral relations. Domestic health service support for returning casualties would be required including mental health and medical support for those sustaining long-term injuries.



Northern Ireland related terrorism

The current threat level for Northern Ireland related terrorism in Northern Ireland is severe, meaning an attack is highly likely. Since the signing of the Belfast (Good Friday) Agreement there has been a transformative change in Northern Ireland where peace has brought stability and opportunities, enabling it to develop into the vibrant place it is today. However, there are a small number of people who continue to try to destabilise the political settlement through acts of terrorism and paramilitarism. Their activity causes harm to individuals and communities across Northern Ireland.

Scenario

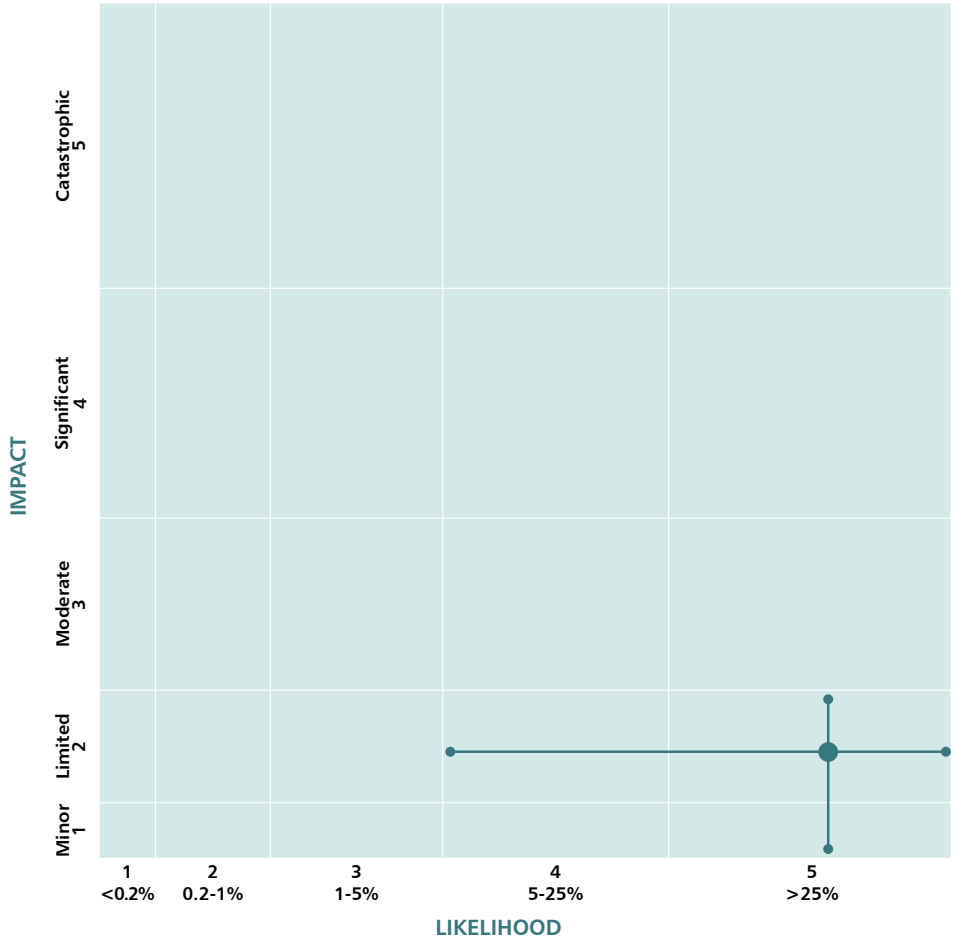
The reasonable worst-case scenario for this risk is a targeted terrorist attack in a public area in Northern Ireland. The intended target would be a site viewed by dissident republicans as symbolic of the British state. The attack could also pose a risk to members of the public depending on where it took place. There could be fatalities and casualties, damage to nearby infrastructure and disruption to transport.

Response capability requirements

Immediate assistance will be required from the Police Service of Northern Ireland and potentially the other emergency services depending on the nature and impact of the attack.

Recovery

Support will be needed for the victim(s) of any attack, those injured and, where necessary, their families. Consideration should also be given to what support the local community will need following the attack. Work may be required to repair any damaged infrastructure.



Terrorist attacks in venues and public spaces: explosive devices

An explosive attack can occur as a result from either a person-borne improvised explosive device, an emplaced improvised explosive device or vehicle-borne improvised explosive device. Examples of explosive attacks that have taken place in the UK include the 2017 Manchester Arena attack where a terrorist killed 22 people and the Liverpool Women's Hospital explosion in 2021. The government continues to reduce the vulnerability of the UK to an explosive attack through restricting access to explosives precursor chemicals, improving detection capabilities including the introduction of National Canine Training and Accreditation Scheme for Private Companies, and maintaining an understanding of the explosive materials and methods that pose a risk in the UK.

Scenario

The reasonable worst-case scenarios included in this category of risk include the detonation of an improvised explosive device (on a person, vehicle or emplaced) at an enclosed or unenclosed location with high crowd densities. These scenarios would result in multiple fatalities and casualties and there may be further fatalities and casualties through structural collapse (enclosed areas), fire/smoke or large numbers of people fleeing a scene to safety. An attack may temporarily impact utility supply, transport services and put pressure on emergency services.

Response capability requirements

The use of the Joint Emergency Services Interoperability Principles provides the basis for a coherent multi-agency response. The response to an explosion may utilise the deployment of both specialist and non-specialist responders. Local Resilience Forums and their Scottish and Northern Irish equivalents would support wider consequence management. Specialist response capabilities would include Explosive Ordnance Disposal and Urban Search and Rescue, which would be required for building collapse or structural damage to buildings. Support from utility providers may also be required if damage from the explosion damages underground cables and pipes. The Forensic Explosives Laboratory provides specialist forensic capabilities, which allows the prosecution of explosives-related crimes, including terrorism.

Recovery

Local, regional and national victim support structures will be required to support all those impacted. The short-term excessive demands on hospitals may lead to delays in the system for several weeks. There would be a potential impact, in the medium term, on the tourism industry and businesses in affected areas. In some incidents the physical damage to structures may be extensive and areas may be out of action for a significant amount of time. Such an attack may also impact temporarily on utility supply to the surrounding areas. Residential properties in the vicinity may also be damaged, meaning that people are displaced for a period of time.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'terrorist attacks in publicly accessible locations' category.

Terrorist attacks in venues and public spaces: marauding attacks

Marauding terrorist attacks (MTAs) involving the deliberate seeking of targets by an attacker can take many forms. A wide range of methodologies, from high sophistication to lower complexity can be used as part of an attack (for example, vehicles, bladed weapons and firearms). Previous examples in the UK include the 2017 London Bridge attack, where terrorists used a vehicle and knives to kill 8 people, and the 2020 Reading attack where a knife was used to kill 3 people. The government reduces the vulnerability to a marauding terrorist attack through a programme of support for venues, public places and specific sectors. This includes free advice, guidance and training through ProtectUK. The government has also published the draft Terrorism (Protection of Premises) Bill known as Martyn's Law, which would, if agreed, require certain premises and events to take forward reasonably practicable mitigations.

Scenario

The reasonable worst-case scenarios for marauding terrorist attacks in the assessment include the use of firearms or low-sophistication methods, such as bladed weapons, with the incidents taking place in a venue or public space. Potential impacts from these scenarios include fatalities and casualties, damage to property and infrastructure, increased demands on the emergency services, disruption to essential services and economic damage. Other impacts include disruption to local and regional transport services, disruption to education and short-term excessive demands on hospitals and the wider health service in both the short and long term.

Response capability requirements

The use of the Joint Emergency Services Interoperability Principles and MTA Joint Operating Principles enable a coherent multi-agency response. The response to an MTA may utilise the deployment of both specialist and non-specialist responders. Specialist responders (such as armed police, Hazardous Area Response Team and Fire and Rescue Service MTA teams) are trained to bring the attack to an end and treat casualties in high-risk environments and can be deployed from key locations across the country. Local Resilience Forums and their Scottish and Northern Irish equivalents would support wider consequence management.

Recovery

Local, regional and national victim support structures will be required to support all those impacted. The short-term excessive demands on hospitals may lead to delays in the system for several weeks. There would be a potential impact in the medium term on the tourism industry and businesses in affected areas.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'terrorist attacks in venues and public spaces' category.

Malicious maritime incident

The risk of a malicious attack targeting the maritime sector in the UK marine area is considered unlikely. An incident such as the scenarios described below has never occurred in or near UK waters, and measures are in place to help mitigate such an incident occurring. However, historically and globally we have seen incidents of terrorists targeting the maritime domain, and the government continues to prepare for a wide range of terrorist attacks. Examples of global incidents of this nature include the bombing of the Superferry 14 in the Philippines in 2004, and the hijacking of the Kartepe in Turkey in 2011. In addition to the protective measures that are in place for maritime, the government aims to ensure we are appropriately prepared to respond to this kind of attack, including working with our international partners.

Scenario

The reasonable worst-case scenarios included in this group of risks involve a terrorist attack on a vessel in or near UK waters. This would lead to casualties and fatalities, structural damage to the vessel and possibly in some scenarios may lead to the vessel sinking, depending on the methods used by the perpetrators. In a sinking scenario, passenger evacuation protocols would be activated. This incident would have significant economic costs due to varying factors including the initial response, salvage of the vessel, potential blockage of navigation channels, medical costs and wider impacts on the maritime sector.

Response capability requirements

Any incident in the maritime domain would require specialist capabilities to respond due to the nature of the operating environment. Military intervention would be required in some scenarios. HM Coastguard Search and Rescue coordination would be needed to support the response to incidents. The triage of casualties by medics and the evacuation/reception of passengers at port would also be needed. The incident would invoke the Victims of Terrorism Unit and Foreign, Commonwealth and Development Office to manage domestic and international victims. Mental health support and recovery victim support services would be needed for impacted individuals.

Recovery

In some incidents a vessel may need to be recovered and removed. Depending on the exclusion zone around the vessel this may cause some disruption. If a forensic investigation is needed, this could take months, causing operational challenges for the receiving port if no alternative location is available for management post incident. An enhanced security posture at ports may be required following such an incident.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'terrorist attacks on transport' category.

Malicious rail incident

The domestic rail network in Great Britain has historically been a target for terrorists. More recently, there have been a number of notable attacks by Islamist terrorists such as the London bombings on the 7th July 2005. Unlike other transport modes such as aviation, there are no security searches when rail users enter the network, which limits the ability of the authorities to detect and prevent attackers. Detection of attacks during the planning stage by the intelligence agencies/police is key, along with deterrent activities, for example encouraging vigilance through the See It Say It Sorted campaign, rail staff undertaking security checks, and British Transport Police patrols. Mitigating the impact of an attack by designing in security and using materials such as laminated glass is also a key priority.

Scenario

The reasonable worst-case scenario of this risk is based on a terrorist attack taking place on the rail network. Different attack methods could be used including high- or low-sophistication weapons. The incident would result in a large number of fatalities and casualties. Although lower-sophistication attacks are currently considered more likely, attacks involving firearms and improvised explosive devices are still considered likely.

Response capability requirements

The immediate response would require a range of capabilities across the emergency services, including specialist teams. There will likely be a requirement for mutual aid for emergency services. In the medium to long term, casualties will require further medical and psychological treatment and support.

Recovery

Recovery depends on a number of factors including the precise location and if there is any damage caused by the attack. The time needed for evidence gathering can range from days to a few weeks. Coordination between investigators and the railway is needed to ensure that key areas are returned first. The length of time and cost of repair and reconstruction would depend on the damage. Where there is serious structural damage, temporary works may be required to make safe and/or weatherproof the area pending a longer-term permanent replacement, which could take years. Following an attack we would likely see a reduction in people using the railway due to loss of confidence.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'terrorist attacks on transport' category.

Malicious aviation incident

While air travel remains one of the safest forms of transport, aviation continues to be an attractive target for terrorists and those who wish to cause harm. In recent decades, there have been several attacks and attempted attacks against aircraft and related infrastructure around the world. The government works closely with the aviation industry on aviation security and continues to develop and implement effective measures to protect UK outbound aviation, including the use of advanced screening equipment at security checkpoints to screen passengers and their baggage. All staff working in restricted areas at airports are subject to screening and enhanced background checks. The aviation industry also works with partners overseas to improve aviation security globally.

Scenario

In summary, the reasonable worst-case scenario involves a terrorist attack against an aircraft with passengers on board, causing it to crash over a populated area. This would cause a significant number of fatalities and casualties, involving a broad spectrum of injuries, with impacts over a widespread area. Long-term rebuilding and regeneration of the affected area would be necessary.

Response capability requirements

The immediate response would require a range of capabilities across the emergency services, including specialist teams. There will likely be a requirement for mutual aid for emergency services. Psychological treatment and support would be needed. There would need to be decontamination expertise to clear any aviation fuel left behind.

Recovery

In the reasonable worst-case scenario, it could take up to 2 weeks for normal air traffic services to resume. However, it would likely take much longer for the local area to recover from any damage caused by the incident. Local residents and businesses might need to be relocated temporarily and some permanently.

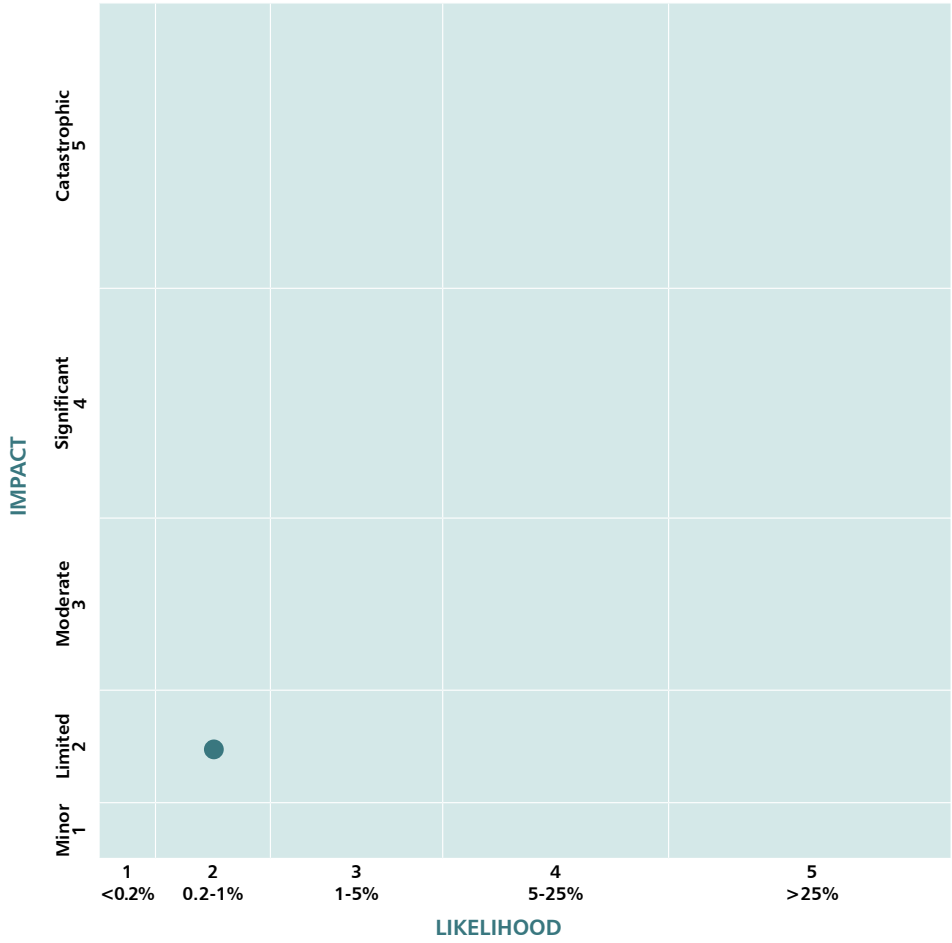
This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the ‘terrorist attacks on transport’ category.

Strategic hostage taking

Strategic hostage taking can be characterised as an incident in which subject(s) are held and/or threatened, in order to fulfil terms and conditions of the attacker(s), who may hold political or ideological motivations. Hostage taking remains a possible method for terrorists, and has been seen internationally, such as in Sydney 2014 where 18 people were held hostage for over 16 hours in a café and Paris November 2015, where 15 people were held hostage in a supermarket following the Charlie Hebdo attacks.

Scenario

The reasonable worst-case scenario of this risk involves a group of people being held hostage as part of a planned siege. Potential impacts of strategic hostage taking include fatalities and casualties, damage to property and infrastructure, increased demands on the emergency services, disruption to essential services and economic damage. Public outrage at the perpetrator(s) would be significant and widespread. Support for hostages' families will be required, along with significant psychological support for the surviving hostages. There is likely to be a large international media presence and coverage of the siege.



Response capability requirements

The use of the Joint Emergency Services Interoperability Principles would enable a coherent multi-agency response. The response to strategic hostage taking may utilise the deployment of both specialist and non-specialist responders. Specialist responders (armed police, Hazardous Area Response Teams, specialist Fire and Rescue Service teams, niche military assets and negotiators) are trained to respond to the threat and treat casualties in high-risk environments, and can be deployed from key locations across the country to attend an incident occurring anywhere in the UK. Local Resilience Forums and their Scottish and Irish equivalents would support wider consequence management.

Recovery

Some individuals will sustain long-lasting physical or psychological injuries. Long-lasting psychological injuries may place long-term pressure on mental health services. Local, regional and national victim support structures will be required to support all those impacted.

Assassination of a high-profile public figure

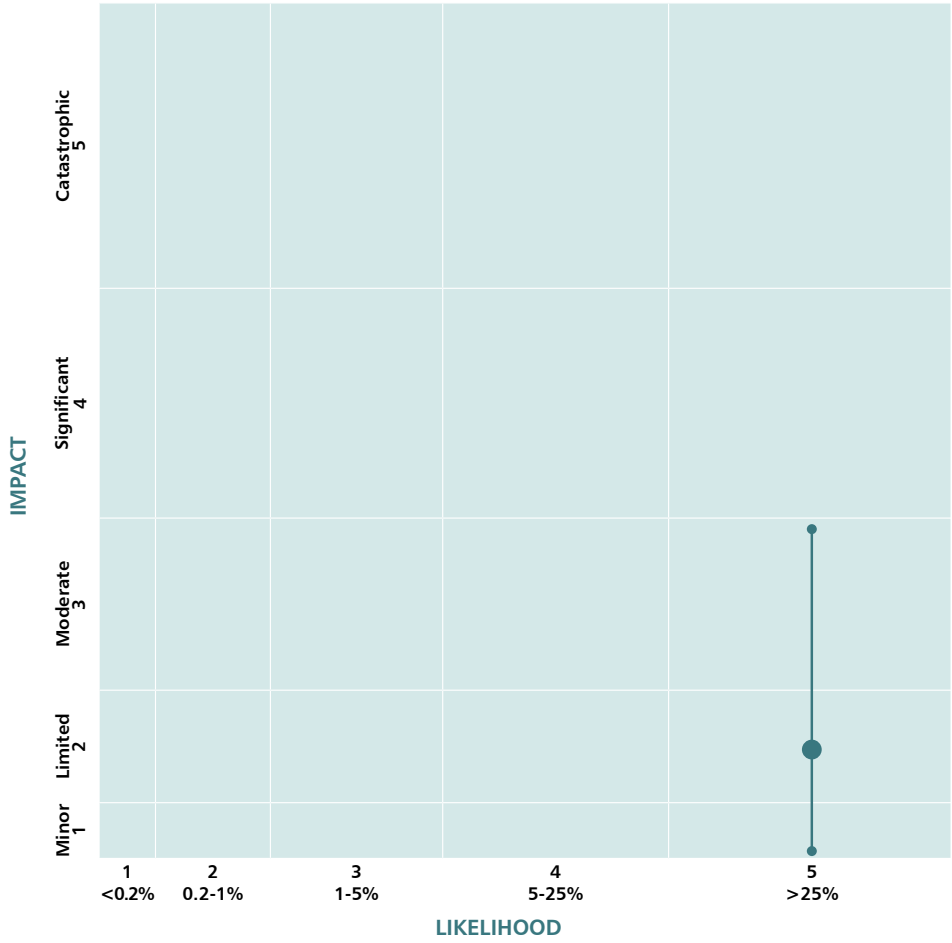
High-profile public figures have historically been targets of assassination attempts. In the UK, the most recent example is that of Sir David Amess MP, who was murdered on the 15th October 2021 at a constituency surgery in Leigh-on-Sea.

Scenario

The reasonable worst-case scenario for this risk concerns the assassination of a high-profile public figure. There is also the potential for a small number of casualties in close proximity to the intended target. This high-profile target would be attacked because of the symbolic value and therefore there would be a large psychological impact. Public outrage would be significant and manifest nationwide (and internationally) as it would be perceived as an attack on our society and way of life.

Key assumptions for this scenario

Outrage may be directed at communities to which perpetrators are believed to be affiliated and any countries/sponsoring group perceived to support them, potentially resulting in heightened community tensions. Although levels of outrage may reduce over time, memory of the event is likely to persist across generations and would be targeted at the perpetrators. Some initial, short-lived anger may be felt about the inability to protect such a high-profile figure.



Assassination of a high-profile public figure

Response capability requirements

A proportionate response will be deployed depending on the specific attack scenario.

Recovery

Depending on the individual who was assassinated, there would be different implications. The running of government and delivery of public services are unlikely to be significantly disrupted by this kind of attack.

Chemical, Biological, Radiological and Nuclear (CBRN) attacks

Malicious actors including terrorists, hostile states or criminals remain interested in CBRN attack methods. In the UK, it is assessed that terrorists are more likely to use knives, vehicles or improvised explosive devices. However, the threat of CBRN attacks cannot be ruled out.

A large-scale CBRN incident has never occurred in the UK, however, small-scale hazardous events are dealt with by the emergency services on a regular basis. Some of these have a criminal element, for example in the case of illegal drugs labs. While a large-scale deliberate CBRN incident has never occurred before in the UK, 2 smaller-scale events challenging our national security have occurred. The first was the former Russian agent Alexander Litvinenko's death on 23 November 2006 in London from poisoning by Polonium-210 (a highly radioactive isotope). The second, in 2018, was the attack on Sergei Skripal, a former Russian military intelligence officer, and his daughter, Yulia Skripal, in Salisbury, which was carried out using Novichok, a chemical warfare agent. This led to the subsequent death of Dawn Sturgess in Amesbury.

The government continues to reduce the vulnerability of the UK to CBRN attacks by improving methods to detect and monitor CBRN materials, including through the UK border, and by limiting access to hazardous materials and their precursors.

Scenario

Chemical

The reasonable worst-case scenarios included in the assessment involve the release of a toxic chemical in an enclosed environment and in an unenclosed environment resulting in potentially large numbers of casualties and fatalities. Other scenarios include incidents which result in contamination of food or water supply, resulting in casualties and fatalities – these events could have an impact on consumer confidence and lead to adaptive purchasing behaviours. With all scenarios there is also the potential for significant economic damage.

Biological

The reasonable worst-case scenarios included in the assessment involve the dissemination of a biological agent in a smaller-scale targeted incident and in a larger-scale widespread event. There is the potential for large numbers of casualties and fatalities, and in the larger-scale event, catastrophic impacts.

Radiological/nuclear

The reasonable worst-case scenarios included in the assessment involve the dissemination of radiological material into an unenclosed environment. The dissemination of radiological material has the potential for large numbers of casualties and fatalities in a relatively localised event. In the case of a nuclear event, the impacts would be catastrophic for the UK. There would be potentially widespread environmental damage and depending on the scale of the event, long-term exclusion of areas contaminated by radioactive material.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together.

Key assumptions for this scenario

For the purposes of the assessment, it is assumed that for certain contamination events, risk mitigation capabilities are in place to reduce the proportion of casualties that become fatalities and to limit the spread/transfer of hazardous materials.

Response capability requirements

The quickest possible response is required to save as many lives as possible. Before specialist response elements can arrive at the scene the Initial Operational Response provides immediate lifesaving actions by the emergency services to minimise preventable deaths and harm for the majority of smaller-scale scenarios. A specialist operational response, supported by CBRN kit and equipment, is then required to manage the scene and the hazard and provide further lifesaving actions.

For example, mass decontamination and specialist medical treatment might be needed. Local authorities are required to support wider consequence management. The use of the Joint Emergency Services Interoperability Principles and CBRN Joint Operating Principles ensure a coherent multi-agency response to emergencies, including those of a CBRN nature. Wider public health responses might be required under some circumstances. Decontamination of land, property and infrastructure may be required depending on the scenario.

Recovery

Recovery from CBRN incidents could be a time-consuming and costly process, depending on the nature of the material dispersed. In some scenarios there could be a long-term environmental hazard that may be difficult to fully decontaminate. As well as the long-term physical effects of these types of events on the built and natural environments, affected individuals and communities may experience significant mental health impacts and a large-scale event would put substantial long-term pressure on health services. For some events the economy could take many years to recover due to widespread cross-sector impacts.

Malicious attack on chemicals infrastructure

The chemicals sector's products underpin UK manufacturing by supplying essential raw materials and intermediate inputs to almost all other manufacturing industries. To date, there has not been a malicious attack on chemicals infrastructure. As with other risk scenarios, terrorist groups may seek to cause harm to advance their political agendas.

Scenario

The reasonable worst-case scenario for this risk is a malicious attack on a major chemicals installation. There is a release of hazardous material as a result, impacting human and animal health. There may be an increased demand on health services and short-term evacuation for affected residents.

Response capability requirements

The on-the-ground response will be led by local responders. Effective local incident management, the availability of site-specific response plans and the integration of site operators into the response may reduce the number of individuals exposed to the release. There may be increased demand on health services.

Recovery

Some individuals may sustain long-lasting physical injuries. Psychological support may be required for those impacted. The contamination from the hazardous materials may be short-lived due to their high volatility. Decontamination may take days to weeks. On-site operations may cease pending the outcome of investigations. The partial restart of operations may take days to weeks. Repairs to affected storage systems may take months to complete.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attack on infrastructure' category.

Conventional attack: gas infrastructure

Gas infrastructure may represent a potential target to terrorist groups with the intent to cause widespread disruption. The Russia-Ukraine war has seen a number of attacks on gas infrastructure (in Ukraine). The UK has a diverse and highly resilient gas network. Industry works to continuously minimise the risk of unplanned disruption while taking the risk of such outages into account in forward planning. Both the government and the Gas System Operator have robust response plans in place in the unlikely event a significant gas supply disruption should occur.

Scenario

The reasonable worst-case scenario is based on a terrorist attack on gas infrastructure which results in a significant loss of gas supply capacity to the UK. Domestic gas customers in the directly impacted region would lose their gas supply. There would be casualties and fatalities from a lack of heating, access to necessary medical treatment, exacerbation of an existing condition or limited ability to use gas-fired cookers safely. However, impacts would depend on the scale of disruption.

Emergency procedures could be required to safely balance and maintain pressure on the gas network by stopping supply to large industrial users, including electricity generating stations. Priority of gas supply would be given to domestic users (as they take longer to reconnect following disconnection for safety reasons). Within this process, some critical sites would be prioritised for supply. Disconnecting gas supply to electricity generating stations could cause a shortfall in electricity supply. In the event of a prolonged electricity supply shortfall, rolling power cuts lasting up to 3 hours may be required to balance supply and demand. Within this process, some critical sites would be protected from disruption, with the remaining disconnections being evenly distributed across Great Britain. Further information on established emergency procedures for a gas or electricity emergency can be found in the National Emergency Plan for Downstream Gas and Electricity on GOV.UK.

Response capability requirements

There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution.

Recovery

Restoration of the affected gas infrastructure could take approximately 3 months, at which point rolling power cuts would no longer be required, as gas supplies to electricity power stations would resume. It would take a further week for industrial gas customers to be fully restored and weeks or months for some sites to return to service. It would take several months to restore domestic gas customers impacted by the initial loss of supply.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the ‘conventional attack on infrastructure’ category.

Cyber attack: gas infrastructure

Gas infrastructure may represent a potential target for cyber attacks. Cyber attacks may involve the encrypting, stealing or destroying of data upon which critical systems depend, or they may result in disruption to operational systems. This could lead to the failure of gas supply infrastructure.

National response plans would be initiated to protect critical services as far as possible.

Scenario

The reasonable worst-case scenario is based on a cyber attack on a system critical to gas transmission, causing a significant loss of gas supply. Domestic gas customers in the directly impacted region would lose their gas supply. There would be casualties and fatalities as a result of a lack of heating, lack of access to necessary medical treatment, exacerbation of an existing condition, or limited ability to safely use gas- fired cookers. However, impacts would depend on the scale of disruption.

Emergency procedures could be required to safely balance and maintain pressure on the gas network by stopping supply to large industrial users, including electricity generating stations. Priority of gas supply would be given to domestic users (as they take longer to reconnect following disconnection for safety reasons). Within this process, some critical sites would be prioritised for supply. Disconnecting gas supply to electricity power stations could cause a shortfall in electricity generation. In the event of a prolonged electricity supply shortfall, rolling power cuts lasting 3 hours at a time may be required to balance supply and demand. Within this process, some critical sites would be protected from disruption, with the remaining disconnections being evenly distributed across Great Britain. Further information on established emergency procedures for a gas or electricity emergency can be found in the National Emergency Plan for Downstream Gas and Electricity.

Response capability requirements

There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution.

Recovery

Restoration of the affected gas infrastructure could take approximately 3 months, at which point rolling power cuts would no longer be required, as gas supplies to electricity power stations would resume. It would take a further week for industrial gas customers to be fully restored and weeks or months for some sites to return to service. It would take several months to restore domestic gas customers impacted by the initial loss of supply. A cyber attack could mean that recovery takes longer than expected, depending on the sophistication of the attack and damage to the system.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Conventional attack: electricity infrastructure

The UK has a highly resilient electricity network. A successful attack on electricity infrastructure has not taken place in Great Britain, though attempts were made to attack electricity infrastructure in the 1990s. Multiple attacks on electricity infrastructure have occurred internationally, in countries such as Iraq and Colombia. Industry works to continuously minimise the risk of unplanned disruption while taking the risk of such outages into account in forward planning. Both the government and the Electricity System Operator have robust response plans in place in the unlikely event that significant electricity supply disruption should occur.

Scenario

The reasonable worst-case scenario is based on a conventional attack against a major electricity infrastructure. This would lead to a loss of electricity output at the site instantly, resulting in an initial regional power cut. The network operator would reconfigure their network to stabilise the grid and reconnect most customers.

Response capability requirements

There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution. Additional support could be provided via mutual aid agreements.

Recovery

Most customers would be reconnected on a staggered basis within 24 hours. However, when damage is widespread, or impacts located on the more remote parts of the network, it could take several weeks to fully restore all customers. This is due to the difficulties of accessing remote locations and the amount of time to repair physical damage. It could take 6-12 months for the affected infrastructure to be fully repaired.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attack on infrastructure' category.

Cyber attack: electricity infrastructure

The National Electricity Transmission System (NETS) transports electricity across Great Britain. A cyber attack may involve encrypting, stealing or destroying data upon which critical systems depend or disruption to operational systems leading to the failure of the NETS. A failure of this system has the potential to severely disrupt all other critical systems, resulting in greater consequences than typical utilities failures. Great Britain has never experienced a nationwide loss of power and the likelihood is low, however similar events have occurred internationally due to natural hazards, rather than cyber attacks. Great Britain has one of the most reliable energy systems in the world and maintaining a secure electricity supply is a key priority for the government.

Scenario

The reasonable worst-case scenario is based on a malicious cyber attack on a critical electricity system, leading to a total failure of the NETS. All consumers without back-up generators would lose their mains electricity supply instantaneously and without warning. A nationwide loss of power would result in secondary impact across critical utilities networks (including mobile and internet telecommunications, water, sewage, fuel and gas). This would cause significant and widespread disruption to public services provisions, businesses and households, as well as loss of life.

Key assumptions for this scenario

For the purposes of the reasonable worst-case scenario it is assumed that the event occurs in winter when there is a high demand for electricity.

Response capability requirements

There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution. It would be vital to ensure that fuel is available to priority users and can be distributed quickly across the country as required. To support the immediate aftermath of the incident, resilient communications systems, humanitarian assistance and victim support should be in place.

Recovery

Within a few hours, small pockets of consumers would be gradually reconnected with intermittent power supply, with a significant proportion of demand being reconnected within a few days to create a stable 'skeletal network'. Full restoration could take up to 7 days. However, depending on the cause of failure and damage, restoration of critical services may take several months. A cyber attack could mean that recovery takes longer than expected, depending on the sophistication of the attack and damage to the system.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Conventional attack: civil nuclear

Civil nuclear power is of strategic importance to the UK's energy resilience and clean energy transition, and a safe mode of generating electricity. Within the UK, and in line with international good practice, an independent regulator holds operators to account. The Office for Nuclear Regulation requires nuclear power sites to demonstrate their ability to defeat very advanced attacks that could lead to the loss of nuclear material or the release of radiation.

Scenario

In line with international good practice, the UK's domestic legislation requires planning for a range of scenarios, including those far beyond a reasonable worst-case. This scenario is extremely unlikely. It is based on a physical attack at a UK civil nuclear installation resulting in radiological contamination off site. The scenario mirrors that of a civil nuclear accident but has the additional component of an active counter-terrorist policing operation.

Key assumptions for this scenario

Scientific modelling has been used to determine the scenario and the countermeasures required.

Variations

Smaller-scale scenarios could occur with a lower percentage of inventory being released. This would decrease the level of impact on people, the environment and the economy. The attack could happen on a range of sites.

Response capability requirements

In addition to the response capabilities set out in the civil nuclear accident scenario there would be a large-scale, multi-agency response including counter-terrorist policing. A detailed communications campaign would be needed to communicate key messages to the public. Protective actions would be promptly implemented to protect people's health and safety.

Recovery

Around affected parts of the UK there would be significant prolonged long-term security, health, environmental and economic impacts requiring sustained recovery.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attack on infrastructure' category.

Cyber attack: civil nuclear

Civil nuclear power is of strategic importance to the UK's energy security and net zero ambitions and in turn, must continue to strengthen its resilience to dynamic and evolving cyber threats. Cyber security in the civil nuclear sector is managed through a combination of nuclear safety and security regulatory requirements, a defence-in-depth approach and sector-wide collaboration under the 2022 Civil Nuclear Cyber Security Strategy. The combination of these approaches drives a holistic and robust risk mitigation on cyber.

Scenario

This scenario assumes a cyber attack that could require a controlled shutdown of a civil nuclear generating site as a protective measure. This could result in a temporary loss of supply to the UK National Grid until its restoration or generating capacity could be increased elsewhere. Impacts from this loss could vary depending on how power redistribution is managed.

Response capability requirements

The National Grid requires the capability to restore grid systems and manage power distribution. Local Resilience Forums are required to manage potential regional-level impact to essential services as part of their arrangements for managing disruptions from loss of power. Functional back-up generators would be required for a range of other critical infrastructure sectors to reduce impact on essential services.

Recovery

The reactor's return to service could be a lengthy process, depending on the nature of the incident, while replacements and repairs take place due to strict regulatory controls designed to ensure nuclear safety and security.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Conventional attack: fuel supply infrastructure

Fuel supply infrastructure is used to produce, import, store and distribute fuels such as gasoline and diesel to consumers. Those with malicious intent could disrupt operations at a fuel infrastructure site causing operations to cease and impacting the production or distribution of fuel in a given region. There is also a risk of serious and fatal injuries to the workforce on site during an incident of this nature.

Scenario

The reasonable worst-case scenario is based on a physical attack on a critical part of the UK's fuel supply infrastructure. This would impact the production, importation and/or regional distribution of fuel as a result of physical damage or loss of operations, and the fuel sector would take time to adapt fully to the temporary or permanent loss of a critical asset.

Response capability requirements

The response would require proactive engagement with relevant public bodies such as the police. Government has established contingency plans in place to manage any impacts on fuel supply, and these are listed in the National Emergency Plan for Fuel. The National Emergency Plan for Fuel sets out the government's approach to maintaining fuel supplies in an emergency. The plan is for use by the government, the downstream oil supply industry and resilience planners for local services. It includes the possibility of prioritising fuel for the emergency services and rationing fuel to retail customers using legislation under the Energy Act.

Recovery

Once operations at the affected site have resumed, fuel stocks would begin to recover quickly. The time taken for the restoration of supplies would depend on the extent of the damage to the infrastructure. The rate at which forecourt stock levels recover would depend on the remaining stock levels across the region, number of sites that have stocked out and demand levels.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attacks on infrastructure' category.

Cyber attack: fuel supply infrastructure

A cyber attack on the UK's fuel supply infrastructure could have implications for UK fuel production or distribution. All UK operators have robust cyber security practices but vulnerabilities in this space are evolving at pace and so it is a risk that government monitors closely.

Scenario

The reasonable worst-case scenario is based on a cyber attack on a system critical to the UK's fuel distribution and supply. This could cause the temporary loss of fuel supply to a region. Replenishment of sites would take several days depending on the location.

Response capability requirements

Government has established contingency plans in place to manage any impacts on fuel supply, and these are listed in the National Emergency Plan for Fuel, including the Reserve Tanker Fleet supported by Operation ESCALIN, a fuel supply contingency measure to make trained military drivers available to support fuel deliveries.

Recovery

Once operations at the given site have resumed and the rest of industry is able to start to readjust supply routes, fuel stocks would begin to recover quickly. However, the rate at which stock levels at forecourts increase would be dependent on the remaining stock levels across the country/region, number of sites that have stocked out and demand levels.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Attack on government

In order for the government to function effectively and provide services to citizens of the UK, it is vital that government assets, including property and information, remain secure from external threats. There is a broad community of organisations and teams across government who work to ensure that – by monitoring, detecting, deterring and responding to any attack attempt.

Scenario

An attack on government assets or democratic processes (through conventional or cyber-enabled means) could lead to: the loss of important government functions; the disruption of critical government services; impacts on local government services; damage to public trust in the government; interference in elections and democratic processes; and the possibility of reputational damage for the UK overseas. It could also lead to loss or compromise of sensitive information held by the government, or in the case of a conventional attack, injury/loss of life.

Response capability requirements

There is a broad community of organisations and teams across government who work to ensure this – by monitoring, detecting, deterring and responding to any attack attempt. The Government Security Group is responsible for security across government, including the implementation of the Government Cyber Security Strategy. The National Technical Authorities, including the National Cyber Security Centre and the National Protective Security Agency provide expert advice. The emergency services and military are equipped to provide a robust response to any conventional attack. The UK also has established structures (including incident response capabilities) in place to safeguard the integrity and security of UK democratic processes from interference, including cyber threats.

Recovery

The complexity, impact and level of response would determine the recovery timeline. There could be an impact across government and local authorities, requiring the enactment of business continuity plans. Government priorities would change to respond to the attack, which could result in a backlog to other work.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the ‘conventional attacks on infrastructure’ category and the ‘cyber attacks on infrastructure category’.

Cyber

Cyber attack: health and social care system

The health and social care system remains a target for cybercriminals. The 2023 Cyber Security Strategy for Health and Adult Social Care sets out a plan to promote cyber resilience across the sector by 2030.

Scenario

The reasonable worst-case scenario would involve significant systemic service disruption due to ransomware moving quickly across the health and care IT estate. Systems would become inaccessible and organisations would move to offline services. Data loss would be widespread across the affected estate, with data also compromised and/or stolen. Some data would be unrecoverable from backups. At least 50% of the estate would be infected with ransomware, but 100% of the estate would be impacted as systems move offline and/or data loss or compromise is experienced. The impacts would be felt immediately, for example cancelled appointments, delays to medical procedures and tests, and A&E diversions. Therefore an outage could potentially have immediate direct clinical care impacts on patients, as well as cause harm. The second-order impacts are likely to manifest themselves increasingly over time, as the delays and cancellations would mean medical conditions worsen or are not diagnosed promptly.

Key assumptions for this scenario

The assessment is based on the WannaCry incident (2017), which was a global attack. This impacted approximately 30% of NHS Trusts and lasted 4 days before the ransomware 'kill switch' was identified, allowing the system to start coming back online.

Variations

A cyber attack specifically targeting NHS systems, which will be more severe if the intent is to create disruption.

We have already seen ransomware targeting healthcare systems around the world, for example the Health Service Executive in Ireland suffered an attack in May 2021. Although the decryption keys were offered free of charge by the attackers, they still requested a ransom be paid to prevent publication of stolen data.

Response capability requirements

Additional staff to handle paper records (during and after the incident), communications team to provide public and responders with clear information, and, possibly, third-party IT support depending on the type and severity of the incident. A Cyber Incident Response Retainer has been established to cover key national systems and address the immediate impacts of incidents.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Recovery

There is likely to be a long recovery time with elective care backlogs lasting months to years. Return to normal service use is characterised by a phased return of priority service functions over several months to years. This is dependent on the type of attack and the different levels of resilience across the cyber system, meaning the most resilient NHS Trusts may come online sooner but will need to handle cases from nearby NHS Trusts that are slower to return to online systems.

Cyber attack: transport sector

Cyber attacks on transport networks or systems have the potential to cause widespread disruption to public transport across the UK and beyond, including but not limited to bus, rail, and aviation services. There are many examples of cyber incidents impacting transport operators both in and outside the UK. In 2021, Northern Rail shut down its new self-service ticket machines following a suspected ransomware cyber attack, and in 2022, Port of London experienced a distributed denial-of-service attack, which temporarily took down its website, but without disrupting transport services.

Scenario

The reasonable worst-case scenario is based on a cyber attack against a critical information network or system in the transport sector. This would result in severe disruption to services delivered by operators. The attack could result in an immediate outage to services and systems, with potential for this outage lasting several hours and requiring multiple days for services to return to normal. The disruption to critical services and systems could result in economic and reputational damage, as well as present an increased threat to passenger safety of the affected operators within or connected to the UK.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Cyber attack: telecommunications systems

Telecommunications is part of the communications critical national infrastructure (CNI) sector, and comprises fixed-line communications, mobile communications and internet infrastructure. Due to the critical services telecoms networks provide to the UK, they represent a valuable target for cybercriminals, therefore building our security and resilience capabilities is paramount. Communication providers are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks. The Department for Science, Innovation and Technology (DSIT), as the lead government department, introduced the Telecommunications (Security) Act 2021 and subsequent secondary legislation, which establishes a new and robust security framework, underpinning requirements to ensure the sector builds and operates secure networks.

Scenario

A disruptive and sophisticated cyber attack against a major UK telecoms network provider would affect millions of customers. This includes customers on other networks that connect or route through the impacted network, as well as impacting services provided by other CNI sectors. Impacts to broadband, landline and mobile would mean that customers are unable to access the internet or make voice calls. All customers without fixed-line and mobile connections are unable to access the Public Emergency Call Service (999/112), among other critical services.

Depending on the nature of the attack, disruption could last for up to 72 hours, but could extend into weeks or months. In extremes, a contingency service could be put in place (potentially within a fortnight).

Key assumptions

The cause and extent of network disruption may not be known immediately and it may be difficult to identify a cyber-telecoms attacker, whether it is a state threat, cybercriminal or hacktivist. Certain state actors have displayed capabilities to attack telecoms networks. Although the UK has not seen an attack at the scale described, it is plausible that under specific circumstances, state actors may demonstrate their intent to disrupt telecoms networks.

Variations

There are numerous variations of this risk in terms of attack vectors, scale, services and sectors impacted, and length of disruptions. The types of cyber threats facing the UK telecoms sector are evolving and diversifying with cyberspace becoming more contested as state and non-state actors seek strategic advantage through advanced technological capabilities. Similar disruptions could also occur from issues other than a cyber attack, such as misconfiguration, accidental disruption and software failures.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Response capability requirements

Telecom operators are required to notify Ofcom of an incident, and consider seeking National Cyber Security Centre (NCSC) and DSIT support to enact a mitigation and response strategy. The overall handling process is underpinned by the Cabinet Office Cyber Incident Management Plan in conjunction with NCSC and DSIT cyber incident processes. The telecoms sector's National Emergency Alert for Telecoms would likely be activated due to impacts on multiple operators. The focus of government and local partners should be to mitigate impacts on the most vulnerable.

Recovery

Full remediation could take months or even years depending on actual or perceived cyber contamination of equipment. Communications recovery timeframes are unknown for other impacted CNI sectors, but again, millions could be affected.

State threats

Malicious attacks: UK financial CNI

Financial market infrastructures (FMIs) are the networks that enable financial transactions to take place. Some FMIs constitute critical national infrastructure (CNI), as they provide services essential to the UK economy/functioning of state. Companies providing the UK's critical national infrastructure, including financial services organisations, are high-profile targets to state and non-state actors that may wish to cause significant disruption. The financial regulators' operational resilience policy requires finance sector organisations to ensure their critical business services are resilient to severe but plausible scenarios, including malicious attacks.

The supervisory framework covers FMIs and Other Systemically Important Institutions, critical to the UK's financial stability, who must also consider their risks in relation to harm their institution may cause to the real economy and financial services sector as a whole.

Scenario

The reasonable worst-case scenario is based on a sophisticated cyber attack against a single FMI carried out by a hostile state or criminal actor. Significant destruction and total disruption to systems cause the unavailability of systems for at least a week, with a partial outage of a few weeks thereafter. The destructive nature of the attack causes hard-drive data to be overwritten and infected with malware. Depending on the FMI impacted, there would likely be significant impacts on the processing of financial transactions. There is a risk that the UK will experience a loss of confidence in the availability and integrity of financial data as well as reduced confidence in the financial system. Secondary consequences include international and domestic legal implications concerning data.

A malicious attack on an FMI that causes its protracted failure could threaten the financial stability of the UK or cause significant disruption to the wider UK economy and to consumers.

Key assumptions

The risk assumes that the fundamental integrity of an FMI has been compromised. It assumes the FMI as well as an available backup have been encrypted, making it inoperable.

Variations

Variations involve different examples of FMIs.

Response capability requirements

Collective incident response capability is managed under the UK's Authorities' Response Framework (ARF). The ARF allows the UK's Financial Authorities (the Bank of England, HM Treasury, and the Financial Conduct Authority) to coordinate a response to attacks that have, or could have, a major impact on financial stability or consumers.

Recovery

Recovery from such an attack could take months with permanent data loss or corruption a strong possibility.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Cyber attack: UK retail bank

Retail banks provide financial services to individuals. The services they provide are vital to the UK's economy. They allow consumers to securely deposit and save their money, and access credit and mortgages. Some retail banks are designated as critical national infrastructure (CNI). UK CNI organisations are high-profile targets for cyber actors, both state and non-state, who may wish to cause disruption or steal information. The financial regulators' operational resilience policy requires finance sector organisations to ensure their critical business services are resilient to severe but plausible scenarios, including malicious attacks.

Scenario

The reasonable worst-case scenario is based on a sophisticated cyber attack against a bank's internal IT systems, carried out by a state or criminal threat actor. Such a malicious attack, in a reasonable worst-case scenario, could take a bank's systems totally offline, with significant destruction and total disruption to systems, causing the unavailability of systems for at least 2 days, with a partial outage for 2 days thereafter. The most significant impact would be felt by vulnerable customers with only a single bank account. The bank will also likely face heightened fraud and operational losses. Consumers could ultimately lose confidence in the retail bank and bank runs could follow. In attempts to patch the vulnerability and mitigate the damage, state or criminal actors will almost certainly take advantage of delays to carry out malicious cyber activity such as further data exfiltration. This would increase the duration of the attack and disrupt recovery attempts.

Key assumptions

The scenario is based on past cyber incidents and the increasing cyber threat. The assumption would be that the bank concerned would not be able to recover its core banking platform within the time described and the network would be rendered inoperative such that customers cannot access their accounts.

Response capability requirements

Since most systems are owned by private entities, the responsibility is ultimately on firms, though government and regulators can support in a crisis. Firms are encouraged to improve their cyber security and resilience, and the regulators' operational resilience policy requires regulated firms to set impact tolerances and remain within these. Collective incident response capability is managed under the UK's Authorities' Response Framework.

Recovery

Recovery plans would comprise a mixture of patching and implementing security controls, remediating and testing data and assuring systems are secure. Patching the vulnerabilities alone would be insufficient if the network has already been compromised, therefore it is almost certain that future mitigation measures will be required.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'cyber attacks on infrastructure' category.

Total loss of transatlantic telecommunications cables

Transatlantic telecommunications cables are an underwater, fibre optic network of cables that run from one end of the Atlantic Ocean to the other. These transmit large volumes of data traffic that facilitate telephone communications and internet access. There is a risk that these cables could become damaged, which would disrupt communications across the UK and beyond. The system is generally resilient meaning there is a low likelihood of total loss of transatlantic telecommunications, but the risk would be impactful should it materialise.

Scenario

The reasonable worst-case scenario assumes that transatlantic subsea fibre optic cables connecting the UK would be damaged over a number of hours, rendering them inoperable. The primary sector impacted would be communications. There would be considerable disruption to the internet, to essential services that rely upon offshore providers of data services (including financial services), and potentially to supply chain management and payment systems.

Key assumptions for this scenario

The internet would begin to recover within hours as networks are reconfigured. Satellite communications would only provide a fraction of the bandwidth, and there would likely be an impact on European data networks.

Variations

A loss of a small number of cables could result from disruption at sea, such as a major underwater landslip across several hundred kilometres. The loss of connectivity would be more likely from damage to land-based infrastructure such as a cyber attack and could see cables connecting the UK being taken out of service, either directly or indirectly.

Response capability requirements

The required response would – at least temporarily – overwhelm the subsea cables' sector and require an agreement with cable operators to prioritise cable repairs according to government or wider sector and social criticality needs. The government would at a minimum support coordination of the operation to restore connectivity through repair and mutual aid and assistance.

Recovery

Repair would take a minimum of several months depending on the cause, location, availability of spare cables and specialist capabilities such as repair ships and specialist crews. The impact on the internet would begin to recover within hours as networks are reconfigured.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attacks on infrastructure' category.

Geographic and diplomatic risks

Disruption of Russian gas supplies to Europe

Dependence on Russia for gas, and other energy sources, varies widely by country. For gas, the UK meets around half its needs from domestic production and in 2022 sourced less than 1 per cent of its gas from Russia, with the last reported import in March 2022. While the UK relies less on Russian energy than many other European countries, it is still exposed to disruption in European energy markets.

Scenario

All transit gas that flows from Russia to European states are cut off for several weeks during winter, potentially leading to demand curtailment across Europe; however, domestic heating will be maintained. Increased gas prices may put certain energy-intensive industries at risk, but household bills are protected by the price cap. A severe gas shortage in mainland Europe for a significant period could also negatively impact continental European gas-fired electricity generation capacity, which could affect the UK's security of energy supply in winter, impacting household electricity consumers.[1]

Key assumptions for this scenario

The scenario assumes that the risk is materialised when storage is low and demand is high due to cold weather, and potential additional outages across the UK and European systems occur that limit trade and imports.

Variations

The severity of the risk will be determined by the weather, how much demand there is for gas and how much storage is available. How much access the UK has to liquified natural gas as an alternative to Russian gas will also impact the severity of the risk.

Response capability requirements

Businesses and households will require additional support in the face of higher gas prices, with a particular focus on vulnerable groups who are disproportionately affected.

Recovery

Sustained high prices at historic levels will impact the UK and global economy but prices are expected to eventually stabilise.

[1] While the key assumptions in the reasonable worst-case scenario were not met, high prices were experienced in 2022 driven by significantly reduced Russian flows and market fundamentals including bottlenecks in infrastructure in North-West Europe.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'conventional attacks on infrastructure' category.

Disruption to global oil trade routes

Oil is a strategic resource and its free flow is critical to world commerce and global economic prosperity. Due to the global nature of the international oil trade, disruptions to oil trade routes can lead to regional and even global economic crises as a result of significant impacts on energy prices, production, and wider trade.

Scenario

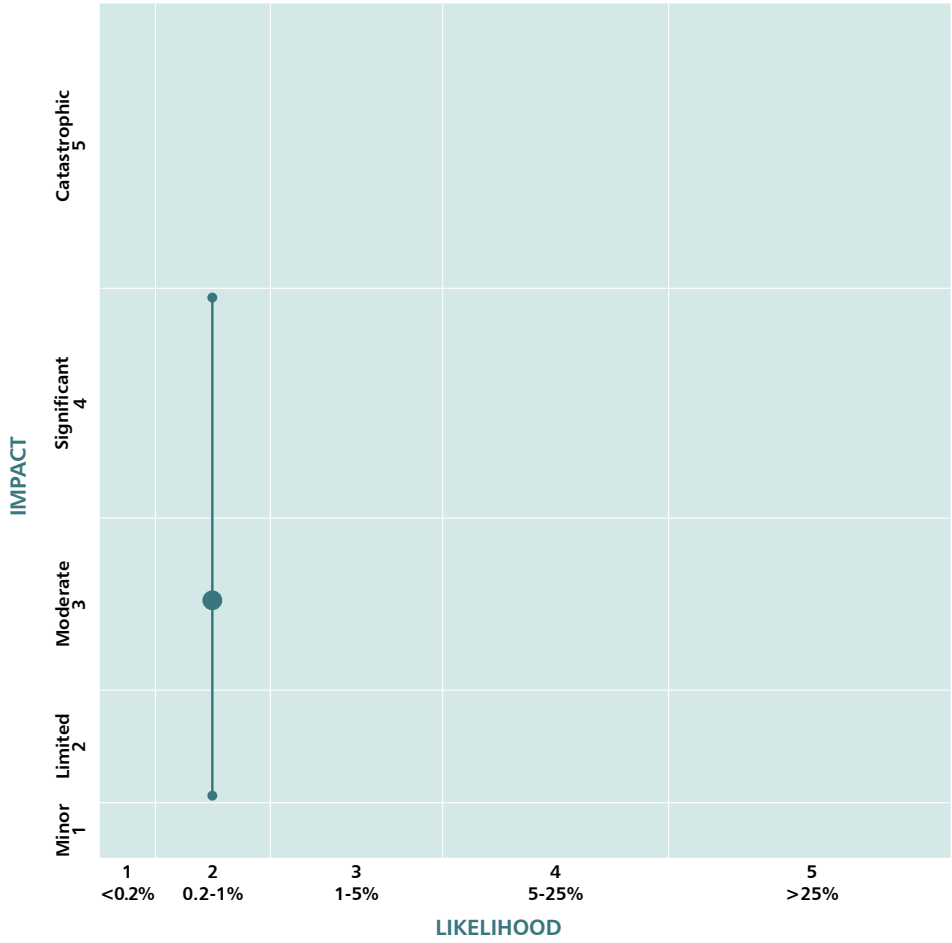
The reasonable worst-case scenario assumes that war, political upheaval or a more benign cause would significantly disrupt global oil supply, resulting in much higher global prices. This has a knock-on effect on the global economy, given its reliance on oil as an energy source (particularly for transport).

Response capability requirements

If a physical disruption to global oil markets did occur, the UK holds emergency oil stocks that can be released to the market as part of a collective action by member countries of the International Energy Agency. If the issue was severe, prolonged and having national impacts, there are emergency powers within the Energy Act 1976 to exert more power over the production and supply of fuels, managing demand during a genuine supply shortage.

Recovery

The UK would likely be able to meet its demand for oil and petroleum products at the market price in a short amount of time, possibly instantly, assuming that markets continue to function or can be re-established.



Accidents and systems failures

Major adult social care provider failure

A complex major provider failure (MPF), characterised by the suddenness of the failure and the number of local authorities and individuals affected, could occur for a number of reasons, such as cost pressures or over-indebtedness. If unmitigated, it could harm continuity of care for people with care and support needs.

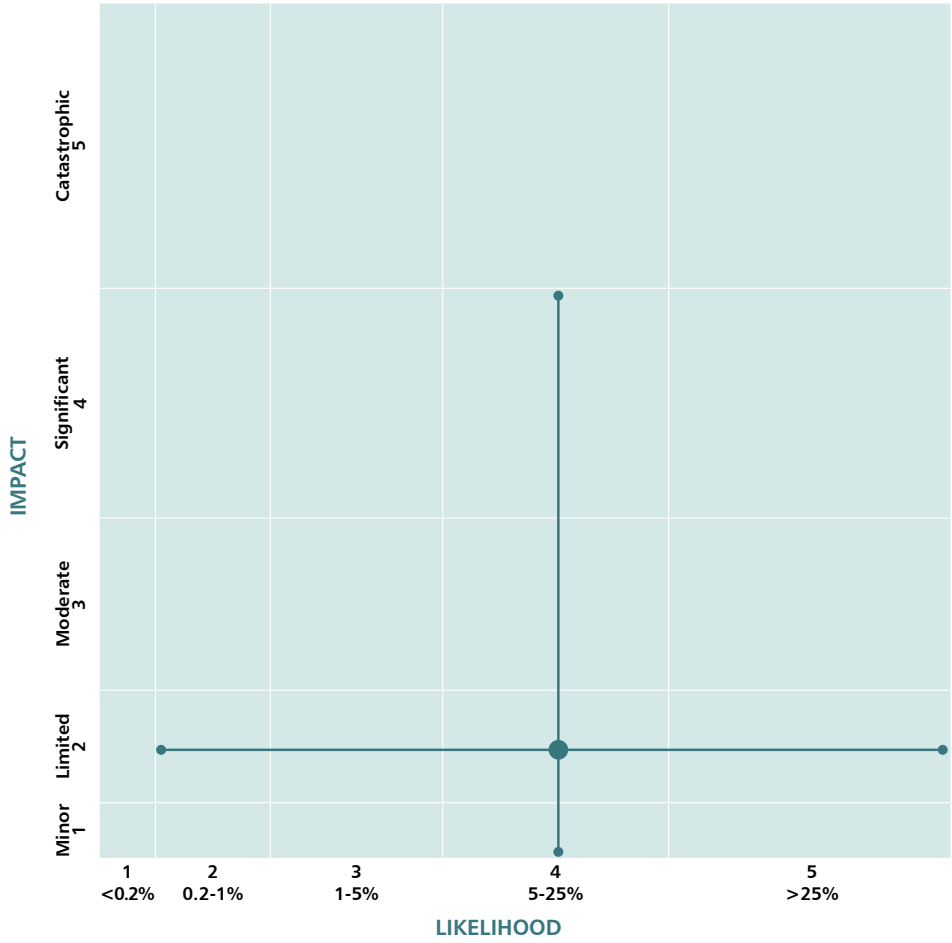
The Care Quality Commission (CQC) Market Oversight Scheme, designed to monitor the financial health of major providers that are difficult to replace, should ensure local authorities are given prior warning that they may need to activate local contingency plans.

In an MPF scenario, the Department of Health and Social Care (DHSC) would also activate robust, sector-wide contingency plans designed to support local authorities (as the commissioners of adult social care) as they work to protect continuity of care.

Scenario

A complex major provider failure occurring with limited prior warning and impacting a significant number of local authorities and people with care and support needs.

In this scenario, due to the scale and complexity of the failure, impacted local authorities might face challenges in discharging their temporary duty to secure continuity of care, putting the welfare of people with care and support needs at risk.



Major adult social care provider failure

Key assumptions for this scenario

The scenario assumes a complex major provider failure that involves a significant number of local authorities and large numbers of people with care and support needs.

The scenario assumes that CQC, through the Market Oversight Scheme, has given local authorities prior notice that the business is likely to fail and services are likely to cease, and local authorities are in the process of rolling out their contingency plans.

Response capability requirements

The scenario reflects the CQC's key role – through the Market Oversight Scheme – in giving prior warning to impacted local authorities, ensuring they have sufficient time to discharge their contingency plans and the impacts are mitigated.

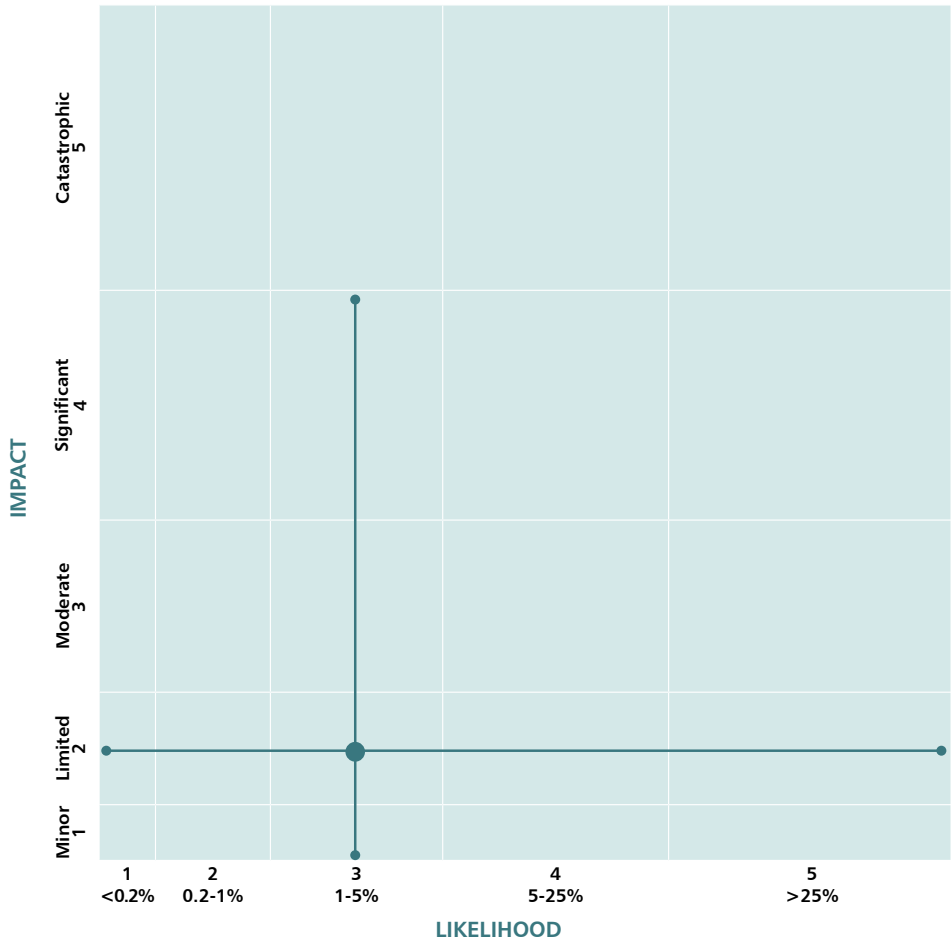
The scenario is likely to put pressure on local authority resources, including social workers and adult social care commissioners. To support local authorities in discharging their temporary duty, DHSC will also activate its own MPF Contingency Plan. This will focus on convening stakeholders across adult social care – including impacted local authorities, other government departments, commercial experts, NHS England, and other sector partners – to ensure a fully coordinated response to secure continuity of care.

Recovery

Recovery time would depend on national and local market conditions.

Insolvency of supplier(s) of critical services to the public sector

There is a risk that a major supplier of critical services to public sectors could suffer insolvency. The types of critical service impacted may vary, and include (but are not limited to) IT services, banking facilities or medical sterilisation services. Any insolvency of a critical supplier could also lead to the disruption of essential public sector services. A number of risk management activities mitigate the risk of insolvency or its impacts, including ongoing commercial capability building across government and the requirement for corporate resolution plans for suppliers of the most critical contracts across government.



Scenario

The reasonable worst-case scenario of this risk is based on the insolvency of a supplier of critical IT services supporting operational systems or back office processes integral to critical national services across the country, such as emergency services communication systems, court services and customs/immigration services and systems. Potential significant impact upon critical service operational delivery, such as lack of ability of emergency services to effectively operate, shutdown or slowdown of immigration systems resulting in reduction of UK border capacity. Ongoing projects likely to incur delays and increased costs. Strategic and political consequences are likely, such as job losses and reputational impacts for the government. Impact dependent on the nature, size and geography of service and supplier.

Key assumptions for this scenario

This scenario assumes that reasonable recovery measures are in place at customers, including government departments, but that these are not sufficient to entirely mitigate the risks associated with loss of service.

Variations of this scenario

Insolvencies may create secondary risks to critical national infrastructure (CNI) targets, such as cyber attacks. These may require more specialised capability and intervention to manage the risk.

Response capability requirements

Continued training on the Sourcing Playbook, the government guidance on making insourcing and outsourcing decisions, and delivering public services in partnership with the private and third sectors. This should be complemented by building commercial, financial and operational capability across government, bolstering effective contract and supplier management. Specialist capability is required to manage distress and contingency plans, such as back-up operations. Central capability in corporate finance (restructuring, insolvency, etc) and in the planning and provision of digital services and data would be required to manage the wide-ranging risks across the government portfolio. Risk mitigations, such as government intervention, should be enabled through controlled and evidenced assessment procedures and relevant legislation.

Recovery

With reasonable recovery plans in place, recovery of systems could be instantaneous or take as long as weeks, depending on the type of services and the supplier's role. Recovery of services could be hampered by backlogs as a result of outages and further work generated by the adoption of short-term manual processes.

Insolvency affecting fuel supply

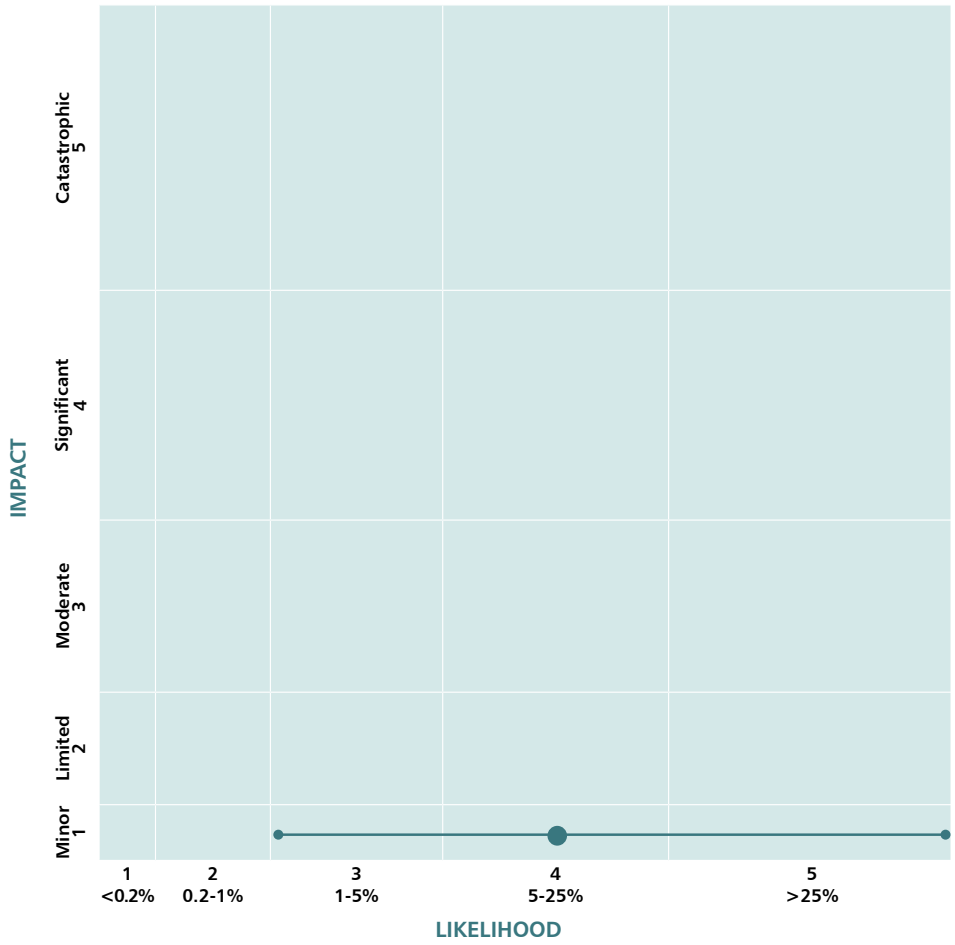
The insolvency of a downstream oil sector operator could have an impact on regional fuel supply and it will be important in this scenario to ensure that there is a managed transition to the closure of the site, enabling the uninterrupted supply of fuel to customers.

Scenario

The reasonable worst-case scenario for this risk concerns an oil refinery, importation, storage or distribution company suddenly becoming insolvent. This could cause major regional disruption to the production and supply of refined fuels, impacting road transport, aviation and domestic heating fuel. The loss of fuel for heating would impact domestic customers, as well as commercial premises and care homes which are required to maintain consistent temperatures for residents. Impacts would be greatest during winter months.

Variations of this scenario

A less severe scenario would see an organised closure and sale process, giving the sector time to reorganise fuel supplies either by use of alternative supply points or through adjusting the business model of the asset to make it more viable within the sector.



Response capability requirements

Government has established contingency plans in place to manage this risk, and these are listed in the National Emergency Plan for Fuel, including Operation ESCALIN, a fuel supply contingency measure to make trained military drivers available to support fuel deliveries. The National Emergency Plan for Fuel sets out the government's approach to maintaining fuel supplies in an emergency. The plan is for use by the government, the downstream oil supply industry, and resilience planners for local services. It includes the possibility of prioritising fuel for the emergency services and rationing fuel to retail customers using legislation under the Energy Act.

Recovery

The government expects that it may take several weeks for industry to readjust supply routes following a sudden closure of a site, but this will begin almost immediately. The government response capability will aim to mitigate the most severe impacts and ensure the readjustment of the sector supply routes happens as quickly as possible.

Rail accident

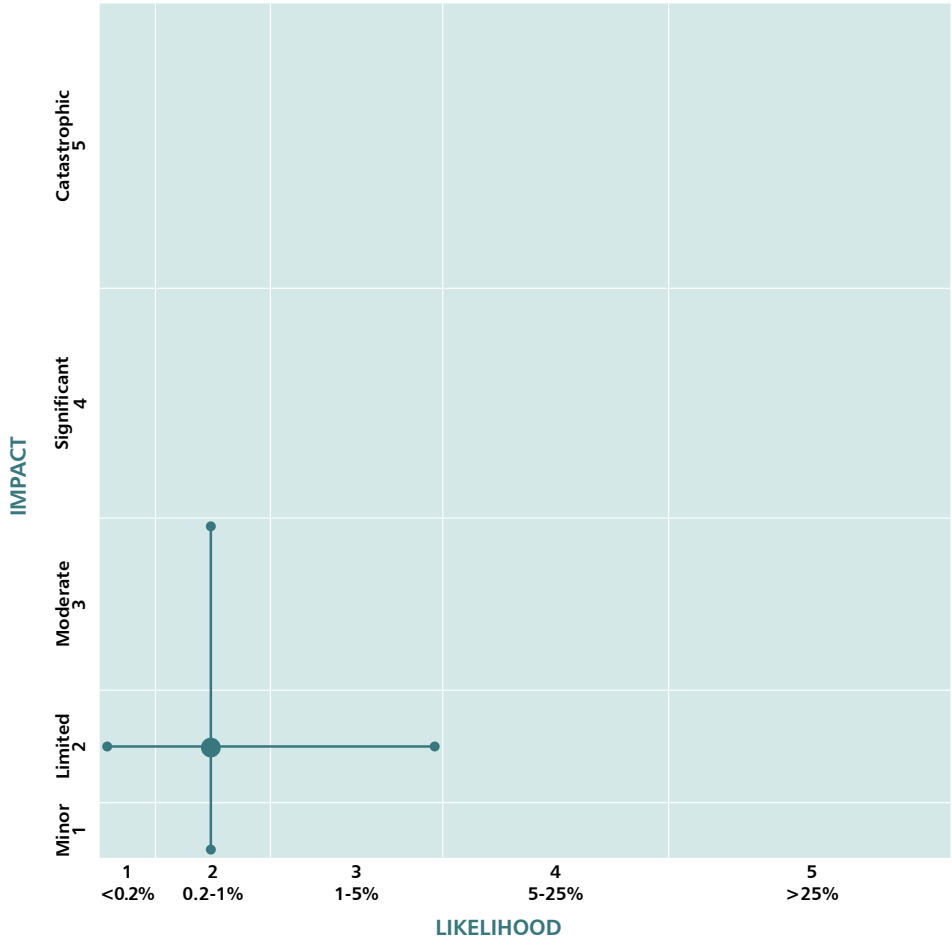
Although UK railways are among the safest in Europe, there is still a risk that a rail accident could occur. Trains operate at high speeds and constitute a significant mass, meaning that any accident has the potential for significant consequences. A recent example of a rail incident is the 2021 Salisbury rail crash, which resulted in the derailment of 2 trains and 14 injured. A robust safety framework, with an active safety regulator and independent accident investigation body, is underpinned by a legislative framework with a clear allocation of responsibilities and duties to all bodies operating on, or around the railway.

Scenario

The reasonable worst-case scenario is based on a serious rail accident that causes multiple casualties or fatalities, or significant environmental or economic damage. There would be damage to property and infrastructure within the affected area, and potential evacuation of those affected. There may also be environmental damage or contamination. Impacts on the railway network would be widespread, with lines being temporarily closed for weeks due to the damage to the infrastructure. This would impact passenger journeys by causing delays, reduce accessibility to specific regions and affect supply chains.

Variations of this scenario

A variety of circumstantial factors may contribute to the risk and impact of an accident. These include weather, human factors, time of day, speed, geography, number of passengers, contents being transported and interaction with infrastructure.



Response capability requirements

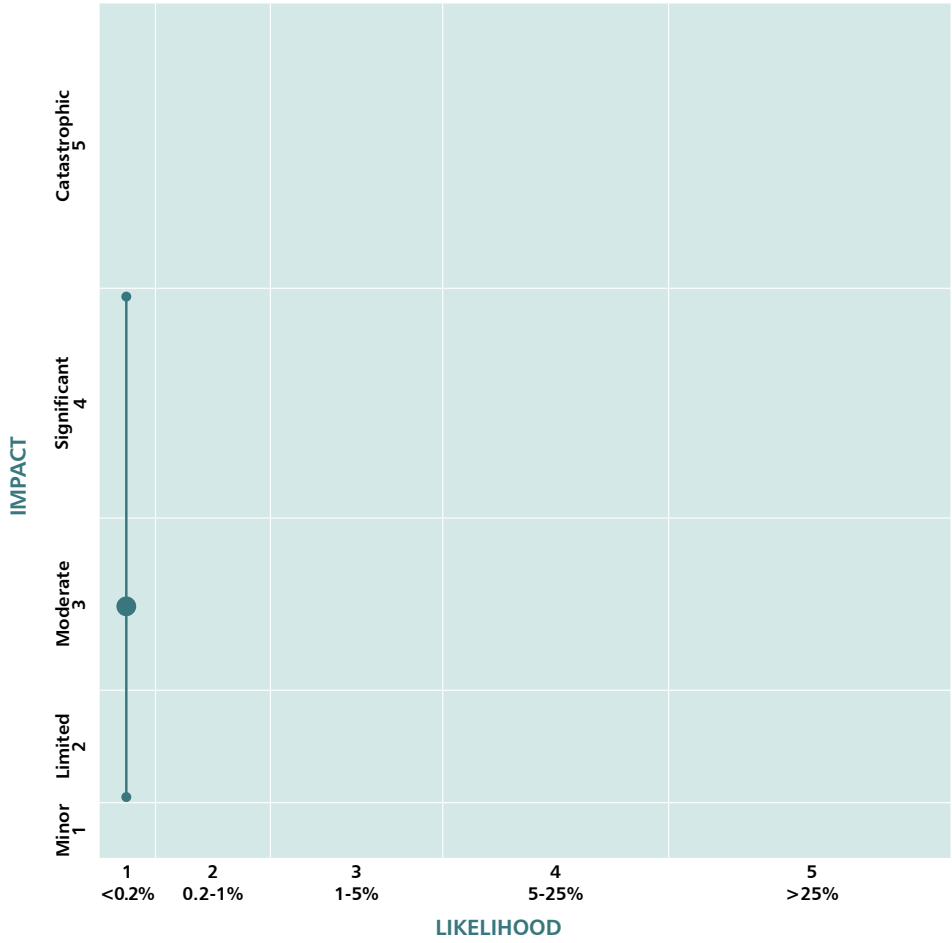
A quick coordinated response between operators, Network Rail, the Office of Rail and Road, the Rail Accident Investigation Branch, local authorities and emergency services (including police and fire and rescue services) would be required to mitigate the impacts of a rail accident and reduce potential for subsequent harm. The industry has experience of managing rail accidents and has procedures and processes in place on how to effectively respond. Where dangerous materials are involved, emergency procedures would need to be rapidly implemented working with the relevant authorities.

Recovery

Some derailments can put a line out of commission for several weeks (or up to one month or more if very severe) due to damage to infrastructure and recovery. Lines are also usually closed temporarily while authorities assess the damage and begin investigations (investigations are not always carried out, but are determined on the basis of harm/economic damage and whether new information or lessons can be learnt). The amount of time this takes will depend on the location of the site, weather, degree of damage or the complexity of factors locally. After testing, the line can be returned to service. Where an accident is caused by asset failure (for example tunnel or bridge collapse) return of service could be several months or years.

Large passenger vessel accident

There is a risk that a large passenger vessel such as a cruise ship could sink in UK waters. This is a low likelihood risk, with the last major accident on a UK-flagged ship at sea having occurred in March 1987 when the Herald of Free Enterprise capsized shortly after leaving Zeebrugge en route to Dover, killing 193 people. International incidents further highlighted the seriousness of this risk should it manifest in the UK. However, the UK deals with many large passenger vessels – not just cruise ships – and has an exemplary safety record.



Scenario

The reasonable worst-case scenario is based on a large passenger vessel (for example cruise ship or ferry) sinking, potentially caused by a collision with another vessel, fire or grounding. Significant numbers of people are aboard, who rapidly abandon the vessel. There would be no-notice fatalities and a substantial number of survivors requiring medical assistance at a shoreside landing point. Older adults with the potential for age-related health and mobility issues, and who would require extra assistance, would be expected on cruise ships. The provision of immediate humanitarian assistance could take several days to complete but would likely be longer in remote parts of the UK. Salvage operations could take several years.

Key assumptions for this scenario

It is assumed for the purposes of the assessment that the incident would take place in the UK search and rescue zone, with passengers and crew being a mix of UK and non-UK nationals. The vessel would sink slowly, allowing search and rescue to take place. The damaged vessel would cause environmental damage.

Variations of this scenario

A variation scenario is a blended incident involving very severe weather, partial abandonment, and one where significant pollution is involved. This would alter the capabilities and subsequent incident management required.

Response capability requirements

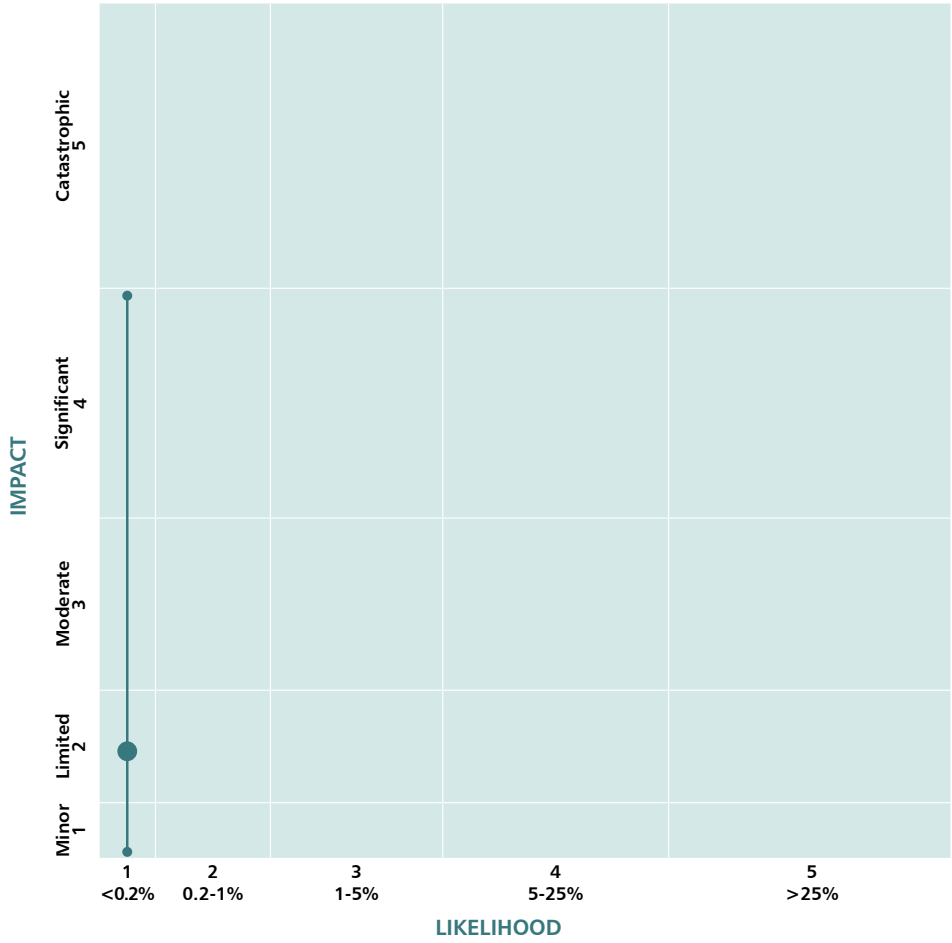
Local level plans are in place to coordinate and respond to the need to provide medical assistance, decontamination, accommodation and repatriation to people landed; however, there are fewer capabilities to do this in more remote locations. Specific requirements include: casualty triage; decontamination; ability to reunite families; language interpretation for foreign nationals; border force; and Foreign, Commonwealth and Development Office input to assist persons without documentation, medication or accommodation. Port security may need consideration and communications capabilities between agencies landside and maritime at the landing point need to be strong. A robust capability to count and track casualties and survivors is required.

Recovery

Recovery in terms of shoreside impacts where casualties are landed would be in the order of days and weeks and managed through existing plans and recovery arrangements in place at the local level. The exception would be remote, small communities who are involved in the response (for example Western Isles) where the incident may leave a lasting impact on the community. Recovery of the vessel and pollution are managed through the National Contingency Plan and commercial salvage routes (see Maritime Pollution Risk). If access to a port is impacted, recovery may take weeks to months.

Major maritime pollution incident

There is a risk of major maritime pollution in UK waters, which could result from the accidental spillage of oil from tankers or leakage from pipelines. These incidents are infrequent but do occur on occasion. For example, hundreds of barrels of oil were recorded to have spilled into the Irish Sea in 2022 following a pipeline leak off the coast of Wales. The UK has plans and procedures in place to deal with pollution at sea in order to quickly respond, limit and reduce impacts on the environment, marine habitats and local coastal communities, working with local authorities, resilience forums and emergency services to communicate and plan for such eventualities.



Scenario

This scenario involves the spillage of 100,000 tonnes of crude oil into UK coastal waters. The cause could be vessel collision, fire or grounding. The spillage results in up to 200km of UK coastline being contaminated with the associated environmental impacts. Depending on the type of oil and extent of the contamination, there could be impacts on land, water, animal welfare, agriculture, waste management and air quality. An extensive clear-up operation on shore may be needed as well as some long-term restrictions on local fishing in the affected area.

Key assumptions for this scenario

The scenario assumes that a fully laden oil tanker leaks in UK coastal waters. The vessel would not sink or prevent access to liquified natural gas terminals or port infrastructure.

Variations of this scenario

A more impactful scenario would be an oil spill near a populated area, disrupting the safe and efficient operation of a major port. This is less likely due to the compulsory use of experienced pilots within port boundaries. A small vessel could run aground and leak a small volume of fuel but containment, clean-up and vessel refloating is straightforward. A less likely, but more impactful, scenario would occur if the ship were to sink or oil ignites and lives are put in danger.

Response capability requirements

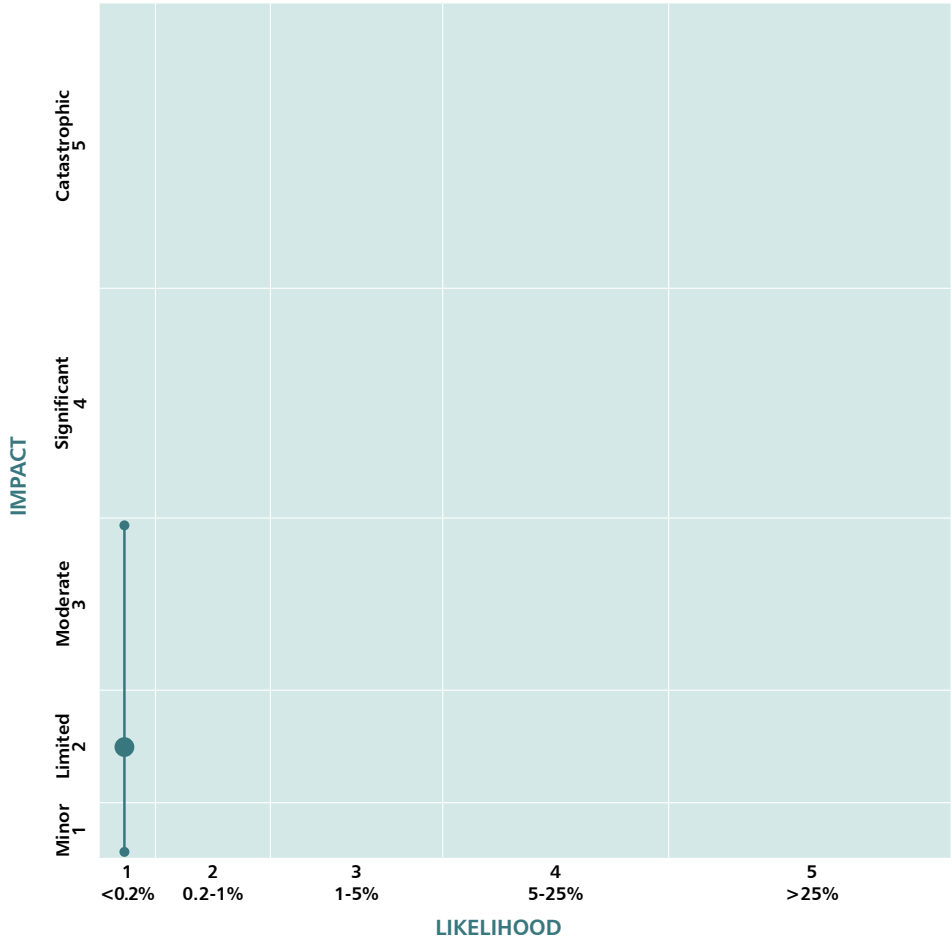
The strain on subcontractors and wildlife conservationists would be significant. There would be a need for recovery vessels to be deployed to remove the excess oil. The Maritime and Coastguard Agency (MCA) would need to work with shipowners, the Secretary of State's Representative, salvors, and ship insurers to organise the removal of the vessel (if safe to do so). Local authorities, the Environmental Agency and environmental groups would need to assess the damage to the coastline, marine life and wildlife. Local fishery restrictions would be applied while a full investigation is undertaken, which could last at least a year.

Recovery

Recovery may take several years. Satellites would be used to assess and monitor oil spread and movement to ensure that oil recovery vessels are deployed appropriately. A significant clean-up operation of up to 1,000 people would be required to return the coastline, beaches and wildlife to a natural environmental state. The Royal Society for the Protection of Birds would need to set up a temporary bird and marine life hospital to treat as many birds and seals as possible. The MCA would be responsible for managing stand-by response vessels. An investigation by maritime accident investigation would be required. Additionally, there would be fishery restructuring required and severe economic impacts locally.

Incident (grounding/sinking) of a vessel blocking a major port

There is a risk that an accident involving a vessel could block a major UK port. The consequences of this risk were observed in the Suez Canal in 2021, which was blocked by one of the largest container ships in the world as a result of it running aground. This resulted in delays to hundreds of vessels waiting to transit through the canal and had significant impacts on trade. The UK has plans and procedures, maintained and executed through the Secretary of State's Representative (SOSREP), to deal with major salvage incidents. The SOSREP will oversee the recovery operations developed by vessel owners and any appointed salvors. Where a counter pollution response component exists within these plans, the Maritime and Coastguard Agency's Counter Pollution and Salvage team will ensure that arrangements are in place to quickly respond, limit and reduce impacts on the environment, marine habitats and local coastal communities.



Scenario

The reasonable worst-case scenario is based on a vessel grounding or sinking, which results in the blockade of a major container port. The port would be unable to commercially operate in any significant capacity for a number of months. Cargo would no longer be able to transit through the port to enter into the UK, potentially impacting critical supply chains. Ships would need to be rerouted, which would be challenging due to their size and the infrastructure required to accommodate them and their critical goods. As a result of the grounded or sunk vessel, boat crew and/or passengers would need to be provided with shelter and treatment for any injuries sustained. There may also be a possible environmental impact from the incident where pollutants are spilt into the sea.

Incident (grounding/sinking) of a vessel blocking a major port

Key assumptions for this scenario

The incident would be the result of extreme weather, or human or technological failure. The port would be able to resume limited activity in the short term by dredging or removal of the wreck.

Variations of this scenario

A vessel grounding is more likely than a vessel sinking. Grounding is easier to resolve through refloating rather than the salvage of a wreck. The business operation of the port would be expected to continue at a reduced capacity. Where critical cargo such as ultra-cold supply chains (for example some vaccines) are impacted due to specialist infrastructure required at ports, vital goods may be lost by not being able to store them correctly.

Response capability requirements

Generic emergency response capabilities such as search and rescue and policing would be required, alongside specialist environmental support and support for victims of the accident. Salvage capability and expertise would need to be imported, which could take months. Dredging can be time consuming and bureaucratic; the government may need to intervene to accelerate the process. If an uninsured vessel is involved, the government may need to provide financial assistance. Direction from the government will be vital in ensuring critical goods are given appropriate priority to meet national needs.

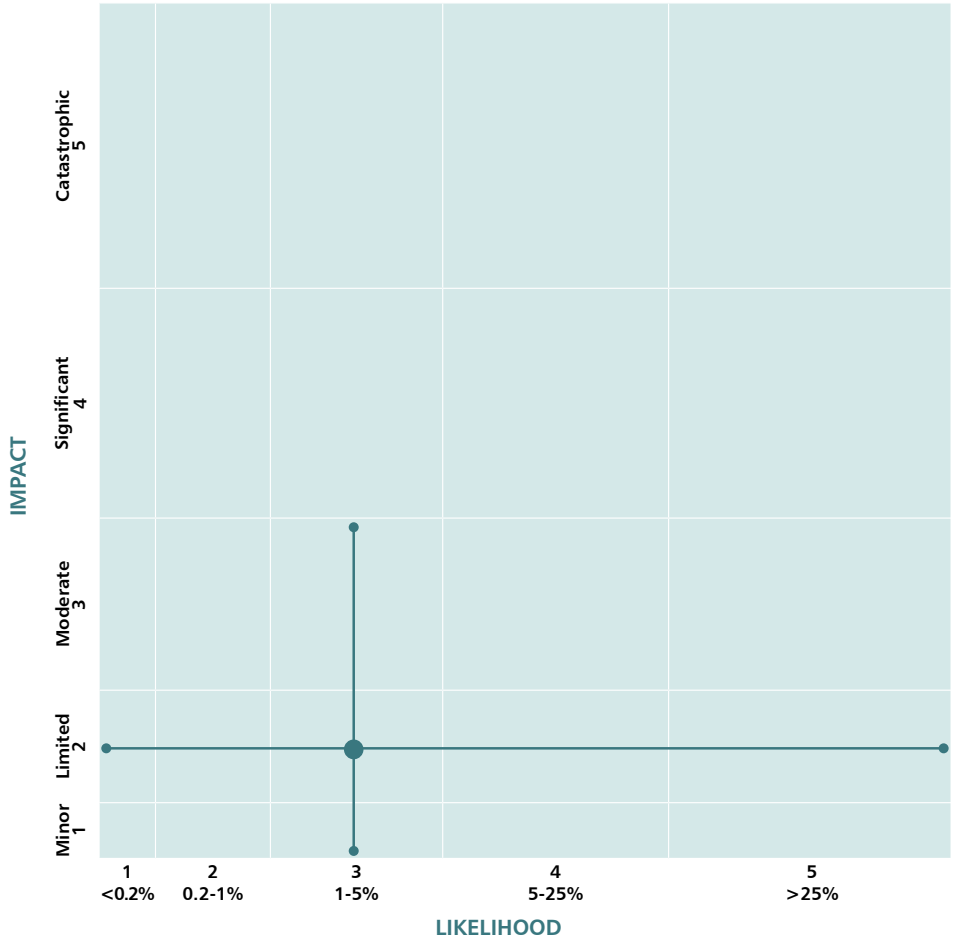
Recovery

Recovery length would depend on the nature of the incident, the location, accessibility to the wreck and availability of specialists to conduct the wreck removal. Partial recovery would be possible by dredging another channel where possible. Insurance would likely protect the facility from financial hardship during this time, but returning to business would be the port's priority.

Accident involving high-consequence dangerous goods

High-consequence dangerous goods may include corrosive, flammable, explosive, oxidising or spontaneously combustible substances. These inherent properties mean that an accident involving high-consequence dangerous goods could have serious impacts, such as mass casualties or destruction to buildings. However, there are regulations in place (the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009) to ensure that these substances are transported safely and securely so that accidents like the reasonable worst-case scenario below are unlikely to happen.

The regulations require, among other things, that drivers of dangerous goods vehicles are trained in the hazards presented by the loads they are carrying and what to do in the event of an accident. Such training is examined and evidenced by an additional driving licence specifically permitting the driver to carry such loads. Additionally, each undertaking involved in the consigning, carriage, or the related packing, loading, filling or unloading of dangerous goods is required to employ the services of a dangerous goods safety adviser. The adviser is responsible for helping to prevent the risks inherent in such activities with regards to persons, property or the environment. Further, it is a requirement that such dangerous goods are identified by appropriate placarding of the vehicles, highlighting the type of dangerous goods carried.



Scenario

The reasonable worst-case scenario assumes that a single road tanker containing high-consequence dangerous goods is involved in an accident, which results in a fire or explosion in an urban area. This would likely lead to road closures of several days, significant local infrastructure damage (road, buildings and bridges), and as a consequence, alternative routing and evacuation of surrounding areas.

Depending on the substance there could also be a risk to the environment, but assuming most of the substance is consumed in the fire, risk of entry into water courses would be minimised. There would also be a small number of casualties and fatalities. The types of substances that could be involved include flammable gases or liquids, substances liable to spontaneous combustion, ammonium nitrate and corrosive substances.

Key assumptions for this scenario

It is assumed that the accident would occur in an urban area on a motorway or dual carriageway and impact housing and other infrastructure nearby. It is also assumed that the vehicle is carrying a full load of dangerous goods meeting the definition of high-consequence dangerous goods.

Variations of this scenario

A less-impactful variation could see an accident in a rural area or with less dangerous goods carried, while a more impactful but significantly less likely variation could see a malicious incident involving more than one high-consequence dangerous goods vehicle.

Response capability requirements

Depending on the substance carried (for example corrosive substances), decontamination may be necessary. There may also be a need for some follow-up communications with the local area regarding possible measures to limit impact from any future accidents.

Recovery

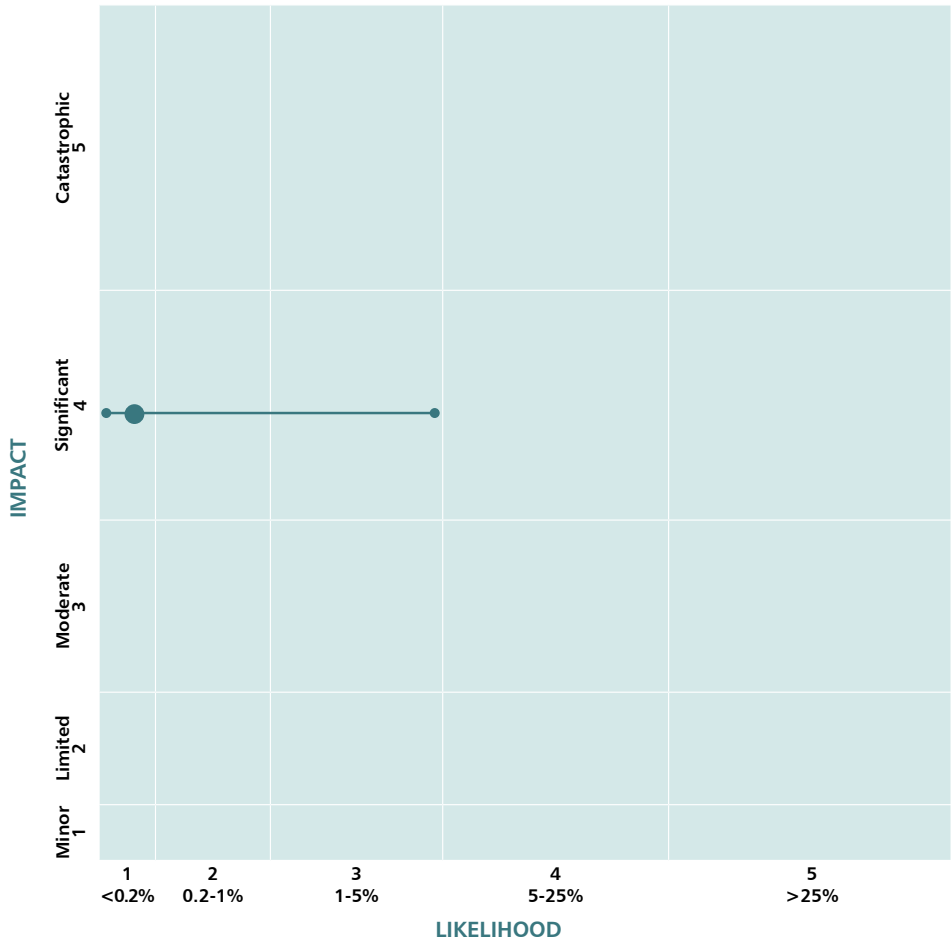
It would take several months to rebuild or repair damage to buildings and infrastructure. If the accident investigation demonstrates that the failure of the tanker was the cause, it could lead to a period of adjustment to vehicle manufacturing requirements and international regime amendments for the transport of dangerous goods.

Aviation collision

UK airspace and UK airlines are among the safest in the world. There has not been a fatality on a commercial passenger airline in the UK since 1989. Even with this success, the government is not complacent and is committed to maintaining and improving the high safety standards in aviation. This is done via a programmatic approach, with the Department for Transport spearheading the State Safety Programme. This involves overseeing risk management across aviation and ensuring effective safety management systems are in place across diverse organisations with a stake in aviation safety oversight to effectively mitigate risk – working closely with the Civil Aviation Authority and other key partners.

Scenario

The reasonable worst-case scenario for the purposes of the assessment is based on an airborne collision involving a commercial airliner and a business jet over a major urban area as the aircraft is approaching the airport. This results in 100% fatalities of passengers and crew on board the aircraft, with further fatalities and casualties on the ground due to falling debris. Debris would also cause damage to buildings and road or rail transport in the affected area. This would require decontamination services to clean up aircraft fuel that is spread over a wide area. There would likely be closures to the airspace over the UK and the airport until the cause of the collision is established.



Key assumptions for this scenario

It is assumed that measures to mitigate risks to aviation safety are broadly as effective as they were in 2018 when the last assessment was carried out. However, this assumption is tested by the Civil Aviation Authority (CAA) iteratively, and any changes to baseline effectiveness will be reflected in future updates.

Variations of this scenario

Other plausible scenarios leading to an aviation crash include Controlled Flight into Terrain, pilot suicide and an uncontrolled lithium battery fire leading to a loss of aircraft. A more impactful but less likely variation could see a mid-air collision of 2 of the largest type of commercial airliners. A less-impactful variation includes the collision of 2 aircraft over a suburban or rural area, resulting in significantly lower numbers of fatalities and casualties.

Response capability requirements

A range of capabilities would be required at the local and regional level in response to the risk occurring, including local authorities and emergency services. There would be a need for decontamination services to clean up aircraft fuel. Structural engineers and builders would be needed to assess the damage from fallen debris and subsequent rebuilding of buildings and infrastructure across a wide area. The Civil Aviation Authority (CAA) and Air Accidents Investigations Branch would assess the cause of the collision and provide assurances that aircraft were safe to fly before UK airspace could be reopened. Victim support would be required for the casualties on the ground and for those in the immediate vicinity of falling debris. It may require engagement with other governments or other services (such as any non-government organisation involved in family assistance for victims of a crash) depending on the nationality of people involved.

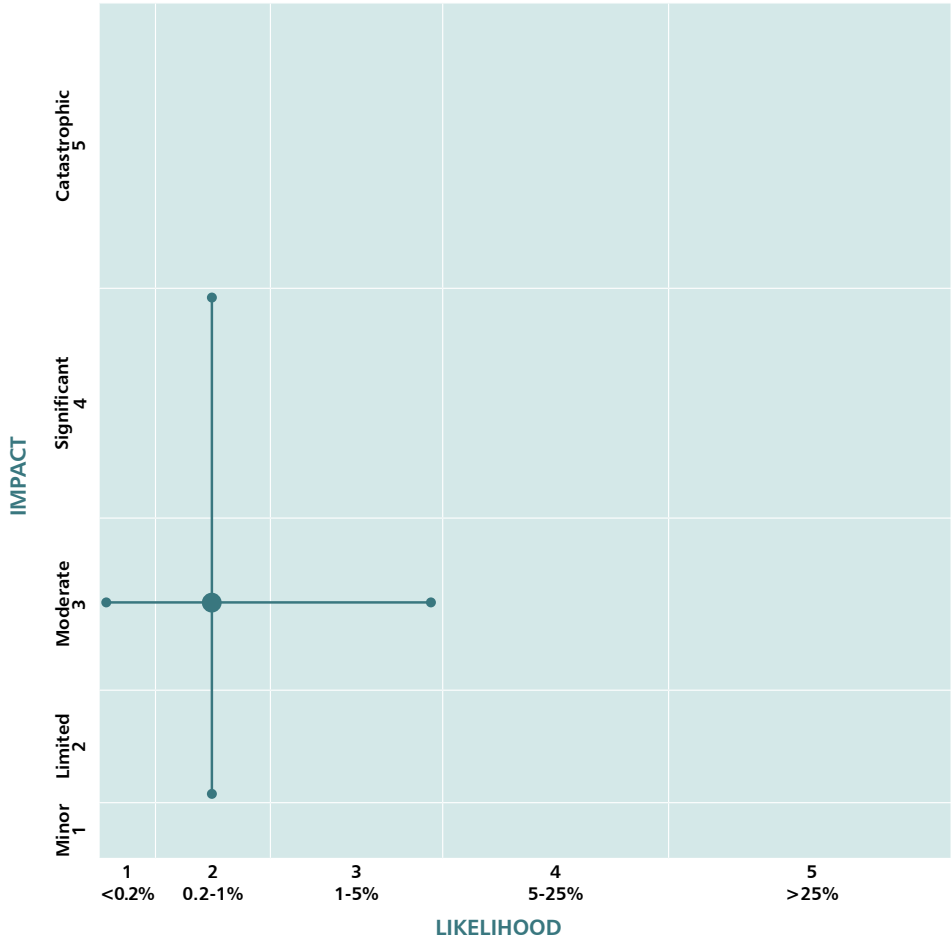
Recovery

It could take several months to clear the debris and rebuild infrastructure, with possible residential and commercial evacuations needed while repairs take place. The recovery and identification of the deceased could take months and would be complex due to the sheer scale of the collision.

Malicious drone incident

The use of drones has increased significantly in recent years, both for business and pleasure purposes. UK law now dictates that registration with the Civil Aviation Authority (CAA) is mandatory for operators of drones over 250 grams and all drones other than toys that are fitted with a camera. It is illegal to fly in an airport's flight restriction zone unless specific permissions have been granted.

There are multiple ways in which a drone could be used maliciously. In 2018 a sighting of a drone at Gatwick airport resulted in significant disruption to flights. Work is ongoing between various government departments, the CAA, industry, and police to maintain risk analysis and continually strengthen mitigations against future malicious drone incidents.



Scenario

One planning scenario is based on the malicious use of a drone at an airport, which could cause disruption and safety concerns. It should be noted that drones are a novel vector to commit crimes and attacks. We actively plan for all types of potential disruption and threat that may result from negligent, criminal, or terrorist use of drones, not just that of airport disruption.

Key assumptions for this scenario

Assumptions vary by scenario, however for the airport disruption scenario described above: It is assumed for the purposes of the assessment that the airport is operating at pre-COVID levels. The risk would not concur at the same time as another major event and the perpetrator is assumed to have malicious intent.

Response capability requirements

Relevant capabilities will vary by scenario. For the airport disruption scenario described above: Specialised police counter-drones capabilities would be required to respond to the incident. Police work, alongside further investigative methods (for example forensic scrutiny of a downed drone), would be used to identify and apprehend malicious users.

Disruption of space-based services

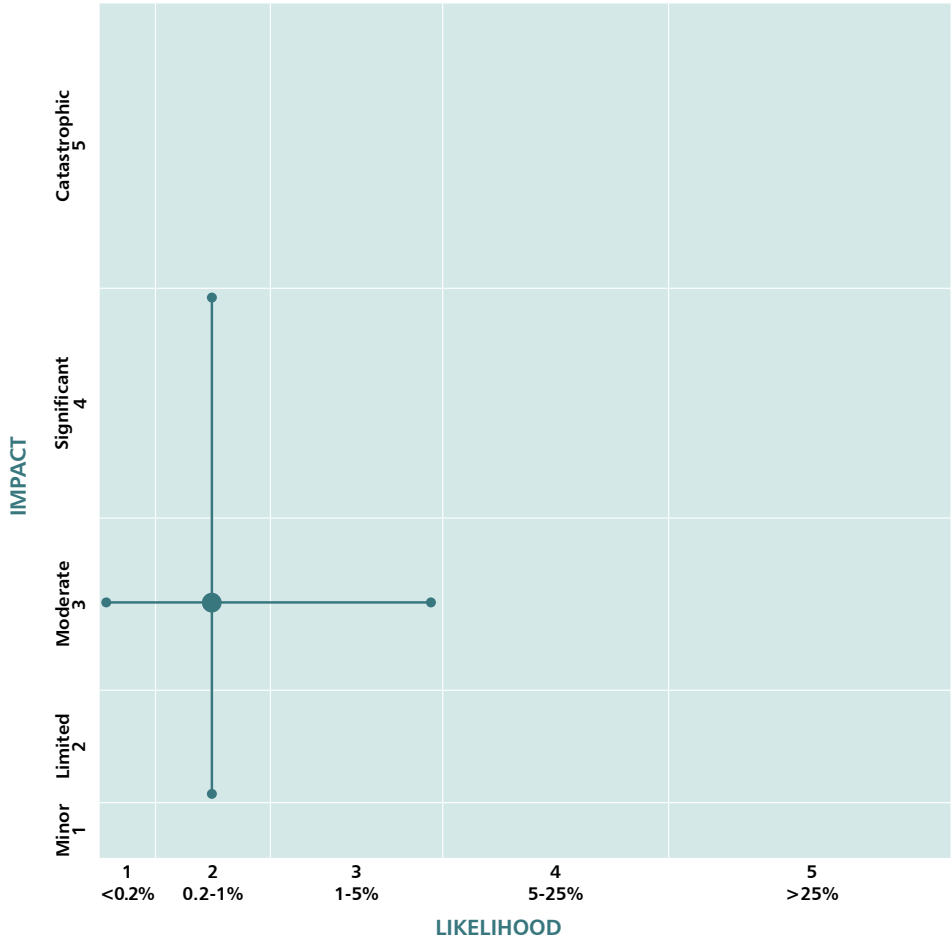
Space-based services such as satellite communication and remote sensing technology are components of the UK's critical national infrastructure (CNI) that enable many essential services to function. Damage to any of these technologies would have a severe effect on multiple sectors, with strategies to help mitigate damage or disruption including the removal of debris from orbit, setting up alternative terrestrial-based services, and developing space situational awareness.

Scenario

The reasonable worst-case scenario assumes that the collision of debris with a satellite produces a debris field that collides with and disrupts other satellites. This would cause a cascade of debris that impacts other satellites and creates further debris. A wide range of space-enabled services would be disrupted or disabled. The disruption to space operations would severely impact the space sector economy. Similarly, essential services such as financial market infrastructure, communications, government services, emergency services and transport infrastructure would be impacted due to their reliance on space sector technologies.

Key assumptions for this scenario

It is assumed that the chance of any debris fragment hitting the UK is extremely unlikely.



Variations of this scenario

Variations include severe space weather disruption to services and a malicious attack on space infrastructure. These variations would generate similar impacts to space-based services on the ground, albeit with differences in scale, depth and duration.

Response capability requirements

Robust resilience and identification of backup systems for CNI that relies on space-based services would be required. There also would need to be strong space situational awareness nationally to task sensors on to specific incidents, and globally to deliver a persistent environmental picture for operators. Coupled with this, an enhanced National Space Operations Centre would be required to provide tracking and monitoring data, warnings and reports, and supporting response and recovery measures to protect government equities in the space domain.

Recovery

Recovery would depend on debris dispersal, with potential impacts on future space operations and associated businesses.

Loss of Positioning, Navigation and Timing (PNT) services

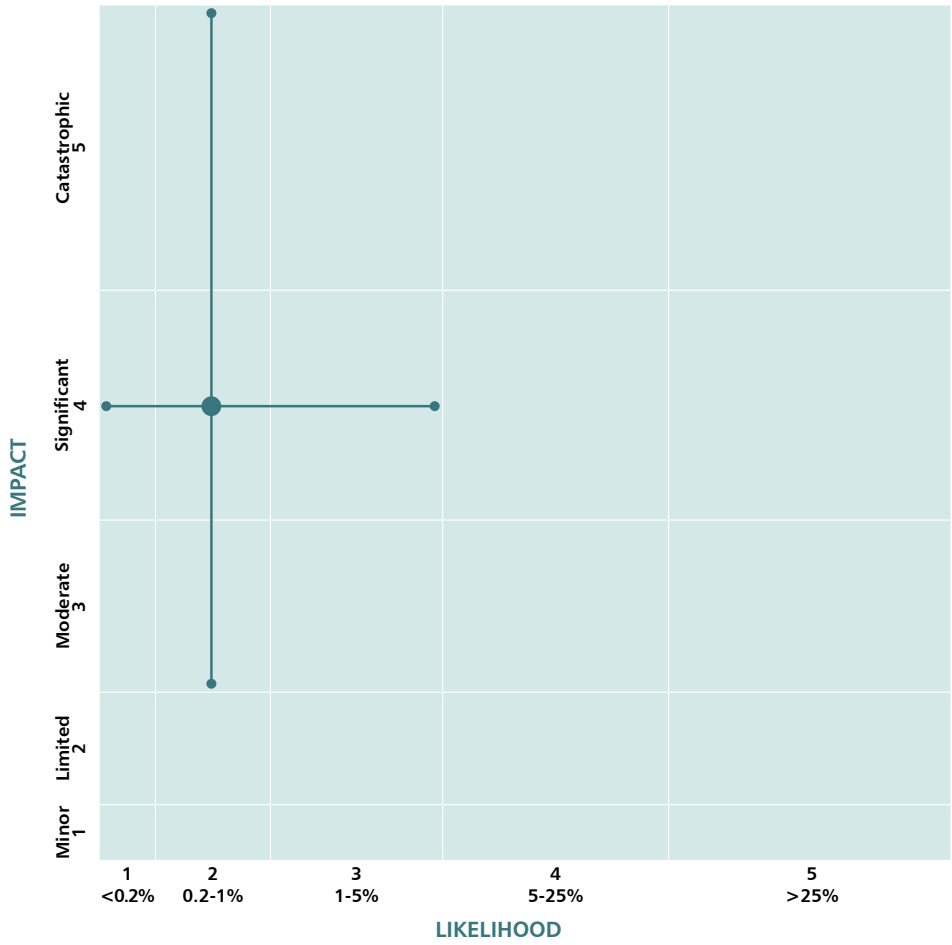
PNT services are a critical component of the UK's infrastructure. They facilitate a diverse range of essential functions across an increasingly interconnected society. For example, PNT is essential for telecommunications, transport navigation and providing precise timings. A loss of PNT services, either due to technological failures or malicious activity, would have catastrophic and cascading effects across the UK and globally.

Scenario

The reasonable worst-case scenario is based on a severe technical failure, due to either hardware failure or human error, in a Global Navigation Satellite System constellation leading to data corruption of that service. This would result in inaccurate position and timing data being delivered to users in space and around the world. The compound series of both technical failure and human error means the service would have no choice but to cease operations. There would be a significant disruption or complete cessation of transport (including aviation and maritime services), communications networks, financial services, energy and emergency services within a few hours of the incident taking place. There is also possible further disruption to other space-based services.

Key assumptions for this scenario

Sectors would revert to older technologies or alternatives to allow for ground services to resume during an extended outage.



Variations of this scenario

Variations include serious and organised crime, jamming and spoofing activities leading to a loss of PNT services, state threat to PNT services, and severe space weather disrupting satellite provision of PNT services. While the impacts are likely to be similar, there would be differences in responses required and the recovery times.

Response capability requirements

Resilient backup systems for critical infrastructure relying on space-based services would be needed, alongside greater space situational awareness nationally and globally.

Recovery

The restoration of full functionality could take up to several weeks, with some ongoing issues with services. Mitigation includes access to other space satellite services and other sources of PNT.

Simultaneous loss of all fixed and mobile forms of communication

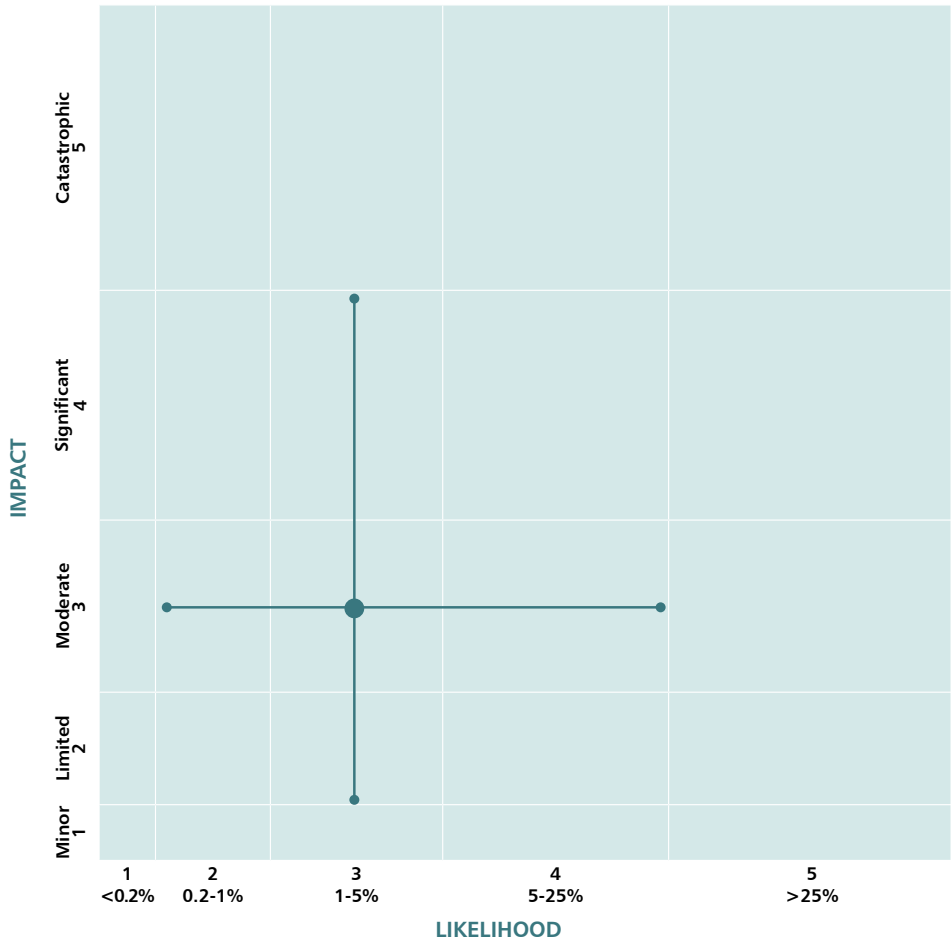
The simultaneous loss of access to all fixed and mobile forms of communication is a form of systems failure that may occur as a result of severe weather. Major storms can cause significant disruption to broadband and mobile infrastructure potentially leading to outages for customers. Ofcom places a regulatory obligation on communications providers to take 'all necessary measures to ensure uninterrupted access to emergency organisations' for their customers, and has issued guidance to protect access to emergency organisations when there is a power cut at the customer's premises.

Scenario

This scenario assumes that all mobile and fixed-line (landline and internet) connections would be lost immediately as a result of a hazard materialising, such as a severe storm or flooding. The incident would affect one region, with most fixed-line connections remaining offline for several days due to a lack of power at the customer premises and damage to overhead cables. All mobile connections in the region would be disabled temporarily until mobile network operators deploy back-up generators to mobile cell sites.

Key assumptions for this scenario

The risk is cause-agnostic and only considers public communication networks (not private networks). It assumes that most domestic premises affected do not have a back-up power supply and the resilient communication systems used by emergency services would not be affected.



Variations of this scenario

Variations include the scale, services impacted, and the length of disruption. Recent severe storms Arwen and Eunice are recent examples of a similar scale event. Storm Arwen (November 2021) was most severe, resulting in millions of customers losing access to mobile and fixed-line connections.

Response capability requirements

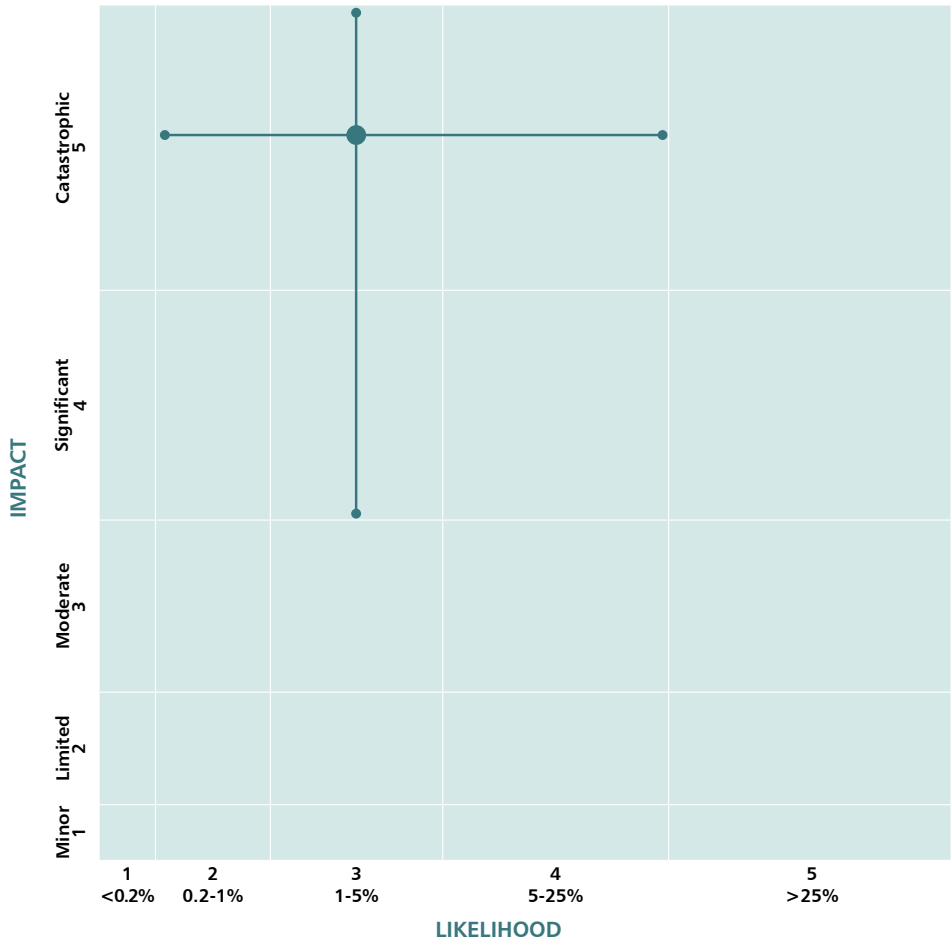
All affected customers would be unable to call 999/112, requiring a full response from Local Resilience Forums and their devolved administration equivalents, government, and local authorities to mitigate against this. Proactive checks for the most vulnerable would be required, especially if they do not have any alternative means to communicate. Resilient communications would need to be established for responders (either via long-range radio or satellite comms); or an alternative power source will be required to power communications equipment.

Recovery

Telecommunication equipment would be very quick to recover, providing the cause of the outage does not persist. Flooding may take longer to recover from as most affected equipment would need to be replaced. Additionally, telecoms equipment is often replaced every 2-5 years and so the sector is well-practised in the quick replacement and repair of equipment, or rerouting of traffic across the network, to minimise disruption to the network. Engineers and recovery assets are also dispersed evenly across the UK, meaning response times would be similar – regardless of what region is affected.

Failure of the National Electricity Transmission System (NETS)

The National Electricity Transmission System (NETS) transports electricity across Great Britain. A failure of this system has the potential to severely disrupt all other critical systems, resulting in greater consequences than typical utilities failures. Great Britain has never experienced a nationwide loss of power and the likelihood is low, however similar events have occurred internationally. In 2019 in South America, millions were left without power following a failure in the electricity system. Great Britain has one of the most reliable energy systems in the world and maintaining a secure electricity supply is a key priority for the government.



Scenario

The reasonable worst-case scenario is based on total failure of the NETS, which would cause a nationwide loss of power. All consumers without backup generators would lose their mains electricity supply instantaneously and without warning. A nationwide loss of power would result in secondary impacts across critical utilities networks (including mobile and internet telecommunications, water, sewage, fuel and gas). This would cause significant and widespread disruption to public services provisions, businesses and households, as well as loss of life. Reasons for failure could include an extreme weather event, a cyber attack and cascading technical failures.

Key assumptions for this scenario

For the purposes of the reasonable worst-case scenario it is assumed that the event occurs in winter when there is a high demand for electricity.

Response capability requirements

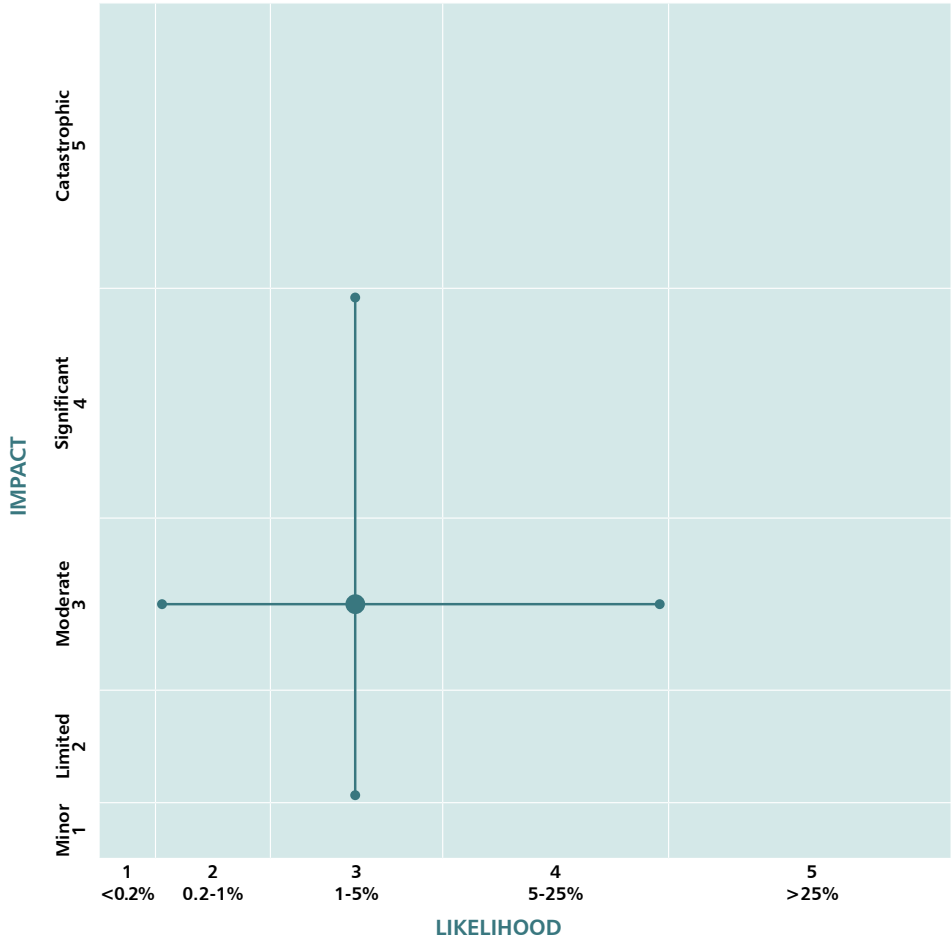
There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution. It would be vital to ensure that fuel is available to priority users and can be distributed quickly across the country as required. To support the immediate aftermath of the incident, resilient communications systems, humanitarian assistance and victim support should be in place.

Recovery

Within a few hours, small pockets of consumers would be gradually reconnected with intermittent power supply, with a significant proportion of demand being reconnected within a few days to create a stable 'skeletal network'. Full restoration could take up to 7 days, however, depending on the cause of failure and damage, restoration of critical services may take several months. As the electricity network is often more complex in urban regions, it is likely that rural areas will receive power more quickly. Due to the geographical distribution of generation across Great Britain, northern regions may receive power more quickly.

Regional failure of the electricity network

A regional failure of Great Britain's electricity network could impact millions and may result from extreme weather causing damage to local infrastructure. Severe winds could bring down overhead cables, or localised flooding might affect a specific power substation. In recent years, Great Britain has experienced smaller-scale regional electricity failures, including those caused by storms Arwen and Eunice in winter 2021/2022 where thousands of homes were left without power. As a result of the government's post-incident review of these storms, industry has taken several steps to improve the electricity sector's physical resilience to future severe weather events, as well as the protections and support available to consumers. These actions will aid in mitigating against larger-scale regional electricity failures.



Scenario

The reasonable worst-case scenario is based on a significant failure of the electricity network across several regions of Great Britain leading to the loss of power across the affected regions. Impacts would vary depending on which regions are affected and the scale of the disruption. This would result in some failures across utilities, causing disruption to public services as well as domestic households and businesses. It is expected that telecommunications systems and transport services (rail, road and aviation) would be disrupted due to the failure of electronic systems.

Key assumptions for this scenario

This scenario is cause agnostic but would likely be the result of extreme weather, with greater impacts in winter. This is a regional scenario which would not cause nationwide disruption.

Response capability requirement

If caused by storms, forecasting would allow government, industry and local authorities to prepare. Specialist equipment and additional workforce would be required, including readying engineers and other workers, cutting down trees near infrastructure, setting up welfare stations for members of the public, and preparing back-up generators to reconnect small numbers of customers quickly. Urban areas would require a different response to rural areas due to higher population densities and infrastructure dependence. Network operators and Strategic Coordinating Groups would coordinate to provide welfare support to customers. Enhanced support, such as alternative accommodation, may be provided to the vulnerable.

Recovery

Most customers (domestic and business) would be reconnected on a staggered basis within hours. However, when damage is widespread, or impacts locations on the more remote parts of the network, it could take several weeks to fully restore all customers. This is due to the difficulties of accessing remote locations and the amount of time needed to repair physical damage.

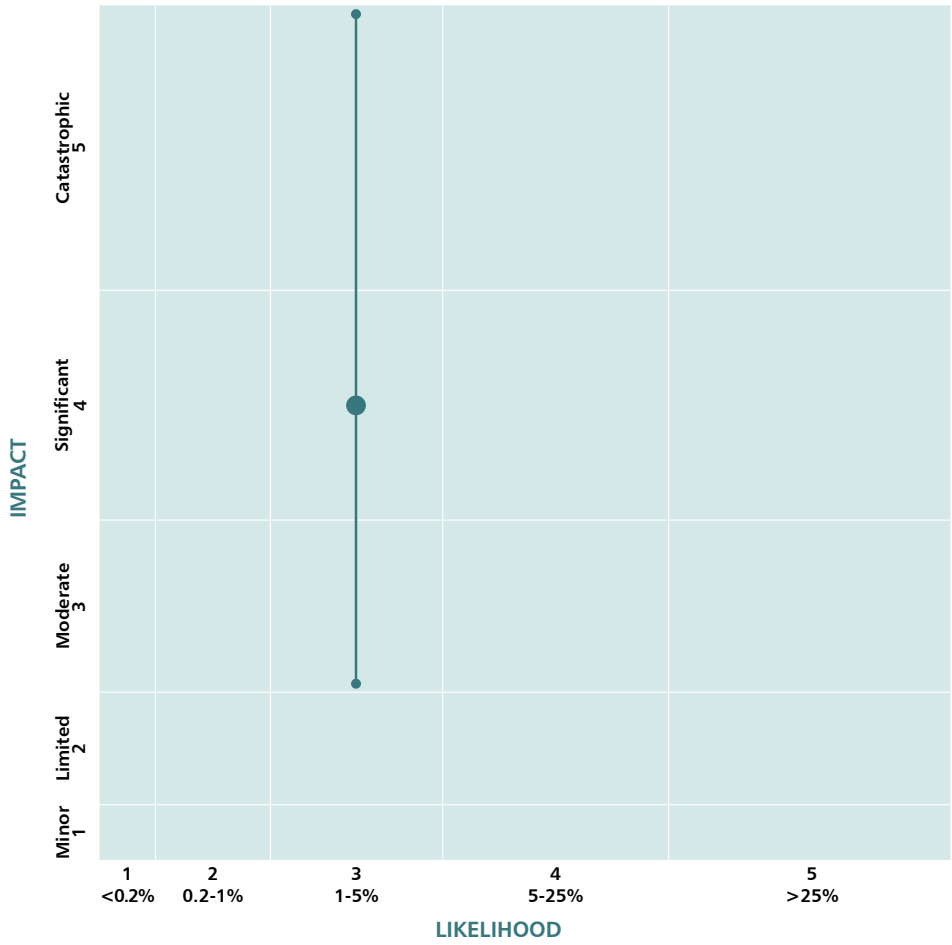
Failure of gas supply infrastructure

The UK has a diverse and highly resilient gas network. Industry works to continuously minimise the risk of unplanned disruption while taking the risk of such outages into account in forward planning. Natural gas is a crucial fuel source that is used to heat homes and businesses, generate electricity or act as a feedstock for industrial processes across the UK. Though unlikely, a failure of gas supply infrastructure may result from a technical issue or accident, with serious impacts on human welfare, essential services and the economy.

Scenario

The reasonable worst-case scenario is based on a technical failure or accident causing a significant loss of UK gas supplies in winter. Domestic gas customers in the region would lose their gas supply. If the loss of supply led to a gas shortfall, emergency procedures could be required to safely balance and maintain pressure on the network by stopping supply to large industrial users, including a proportion of gas-fired power stations (as the largest users). Disconnecting gas supply to electricity generator stations could cause a shortfall in electricity supply.

In the event of a prolonged electricity supply shortfall, rolling power cuts lasting 3 hours a time may be required to balance supply and demand. Within this process, some critical sites would be protected from disruption, with the remaining disconnections being evenly distributed across Great Britain. Further information on established emergency procedures for a gas or electricity emergency can be found in the National Emergency Plan for Downstream Gas and Electricity.



There would be casualties and fatalities from a lack of heating, access to necessary medical treatment, exacerbation of an existing condition, or limited ability to use gas-fired cookers safely. However, impacts would depend on the scale of disruption. Priority of gas supply would be given to domestic users (as they take longer to reconnect following disconnection for safety reasons). Within this process, some critical sites would be prioritised for supply.

Key assumptions for this scenario

The scenario assumes that impacts would be greatest during a severe winter that sees high consumer demand and low supplies from other sources.

Response capability requirements

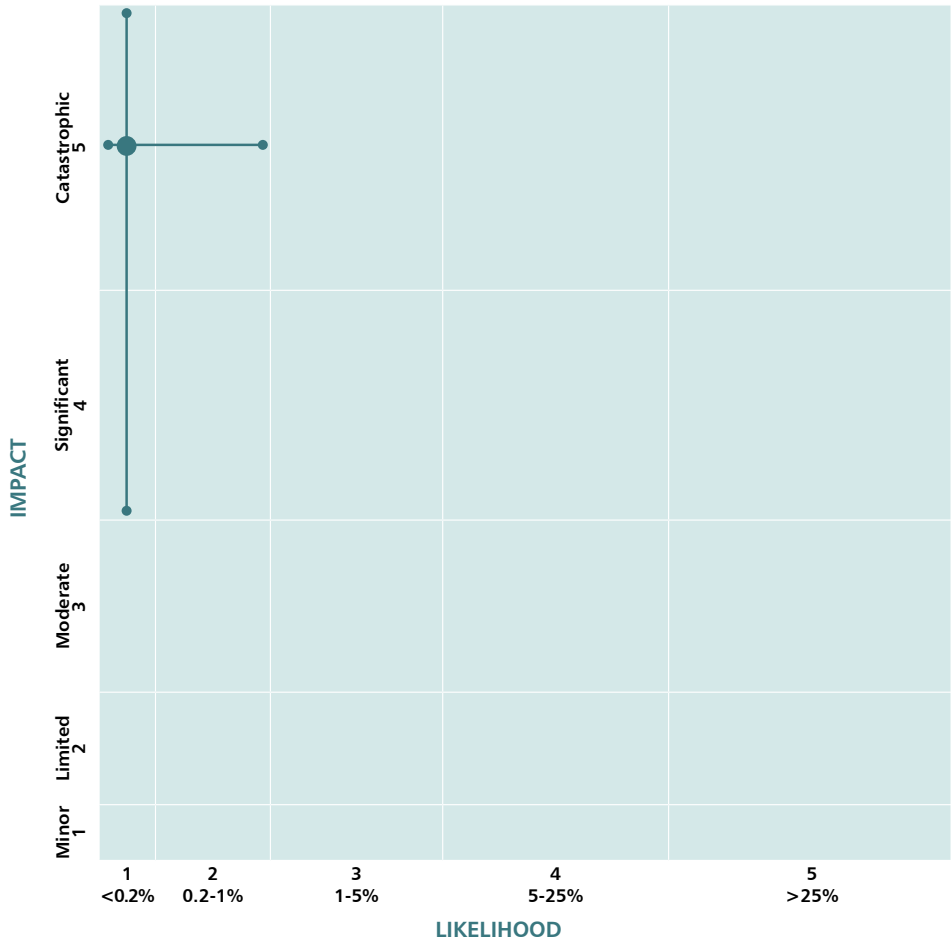
There would need to be preparations in place to support wider recovery and the continued operation of multiple sectors. This includes functioning telecoms, emergency services and fuel distribution. Additional support could be provided via mutual aid agreements.

Recovery

Restoration of the affected gas infrastructure could take approximately 3 months, at which point rolling power cuts would no longer be required, as gas supplies to electricity power stations would resume. It would take a further week for industrial gas customers to be fully restored and weeks or months for some sites to return to service. It would take several months to restore domestic gas customers impacted by the initial loss of supply.

Civil nuclear accident

Civil nuclear power is of strategic importance to the UK's energy resilience and clean energy transition, and is a safe and effective mode of generating electricity. Only a small number of accidents have occurred worldwide since the first commercial nuclear power station came into operation in 1956. As required by UK regulations, there are robust safety procedures in place at all UK nuclear sites meaning an event of this type is of very low likelihood.



Scenario

In line with international good practice, the UK's domestic legislation requires planning for a range of scenarios, including those far beyond a reasonable worst-case. The scenario used for this assessment is therefore extremely unlikely. It is based on an accident occurring at a UK civil nuclear site that results in a release of radiological material that extends beyond the boundary of the site.

Onsite casualties could require decontamination, monitoring and treatment. No immediate fatal health effects would be anticipated offsite but there could be offsite casualties suffering from the effects of radiation. There could also be an increase in the risk of longer-term health impacts, such as cancers.

The resulting contamination could affect the environment and food production, and there could be disruption to domestic and international transport. The overall impacts of a release are highly dependent on weather patterns.

Key assumptions for this scenario

Scientific modelling has been used to determine the scenario and the countermeasures required.

Variations of this scenario

Smaller-scale scenarios could occur, which would decrease the risk to people, the environment and the economy.

Response capability requirements

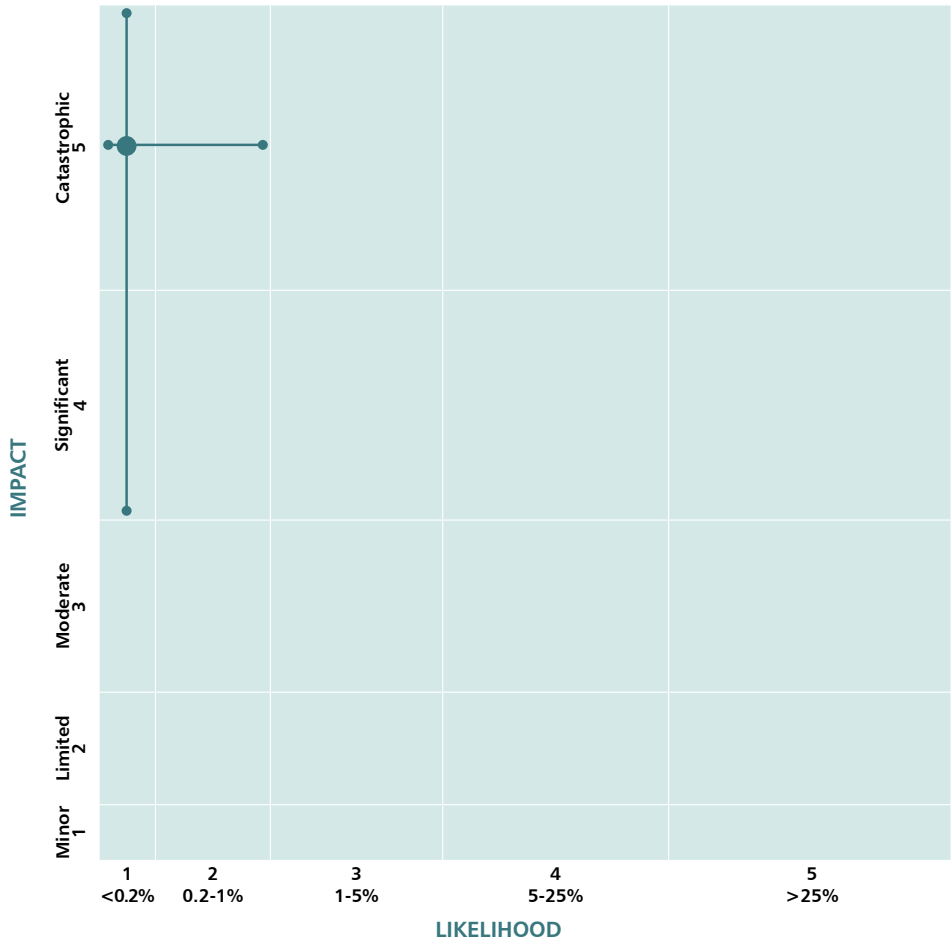
There would be a large-scale, multi-agency response. A communications campaign would be needed to communicate key messages to the public. Protective actions would be promptly implemented to protect people's health, which based on the nature of the accident, could include sheltering, evacuation or the use of stable iodine. A ready stockpile of stable iodine tablets could be required as a medical countermeasure. Immediate capabilities could include radiation monitoring and decontamination services, alongside remediation services to restrict the spread of radioactive material. Humanitarian services would also be required to support those displaced, including but not limited to emergency shelter, food and water.

Recovery

Around affected parts of the UK, there could be significant and prolonged long-term health, environmental and economic impacts requiring sustained recovery.

Radiation release from overseas nuclear site

Another risk that the government is planning for is an accident at an overseas nuclear site that results in the release of radiation. Impacts on the UK homeland would most likely be felt if the accident occurred at a site in a country close to the UK as opposed to a geographically distant location. For example, the 2011 Fukushima disaster in Japan resulted in very low levels of radioactive iodine being detected. Countries near the UK have well-established civil nuclear sectors, with robust safety procedures in place.



Scenario

In line with good practice the UK plans for a range of scenarios, including less likely, more severe scenarios that are beyond reasonable worst-case. This scenario is extremely unlikely. It is based on an accident occurring at an overseas nuclear site, close to the UK. This could affect the UK and its interests overseas, with overall impacts being highly dependent on weather patterns and distance from the UK.

There would likely be no acute radiation-linked immediate health effects for people in the UK although, depending on the weather patterns, there could be an increased risk of cancer over the longer term if the release occurred from an overseas site close to the UK. British nationals in the accident country would likely require consular assistance.

The resulting contamination could affect the environment and food production, and there could be disruption to domestic and international transport into Europe (including Channel shipping lanes). This could impact the import of food from the accident country and surrounding countries. The overall impacts of a release are dependent on weather patterns.

Key assumptions for this scenario

Scientific modelling has been used to determine the scenario and the countermeasures required.

Variations of this scenario

Smaller-scale scenarios could occur, which would decrease the area affected and the risk to people, the environment and the economy.

Response capability requirements

There would be a large-scale, multi-agency response. A communications campaign would be needed to provide key messages to the public. Immediate capabilities would be radiation monitoring and decontamination services, alongside remediation services to restrict the spread of radioactive material.

Recovery

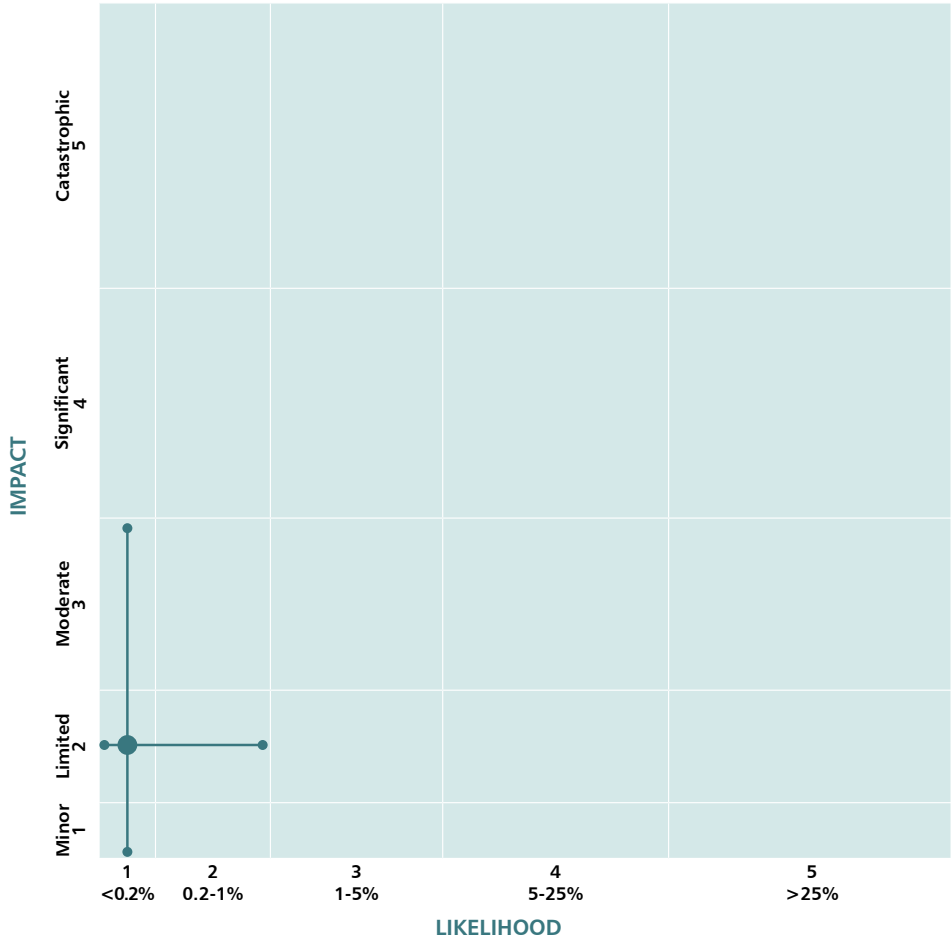
Around affected parts of the UK, there could be prolonged long-term health, environmental and economic impacts requiring sustained recovery.

Radiation exposure from transported, stolen or lost goods

There is a low likelihood risk that radiation could be released from goods being transported within or into the UK. When these goods are handled correctly by trained professionals, the risk of radiation release is extremely low. However, there is a risk as individuals handling transported, stolen or lost goods are unlikely to have the appropriate training. The scenario used in the reasonable worst-case scenario below has never happened in the UK.

Scenario

The reasonable worst-case scenario covers radioactive goods that could be stolen, lost or transported by a legal owner without proper regard to radiation safety regulations. The sources would be mixed with non-contaminated waste in a scrapyard, or subsequently melted in a foundry and used to produce reinforcing bars, table pedestal castings, cast valve bodies or electric motor parts. The packaging used to transport the sources could also be contaminated with radiation. The amount of radioactivity involved would be small and the item disposed of safely. However, the risk would cause moderate economic damage and knock-on impacts beyond the timeframe for decontamination. The process of dismantling the radioactive unit would expose people to radiation and could cause contamination over a wide area, potentially leading to fatalities and casualties.



Key assumptions for this scenario

While radioactive sources could be inadvertently processed in a scrapyard or in another location and mixed with non-contaminated waste and consequently smelted and subsequently used to produce goods contaminated by radiation, this is considered unlikely given the detection systems at each stage of the process. Non-malicious targeted theft of a radioactive source is considered highly unlikely given the robust security requirements in place for radioactive sources in International Atomic Energy Agency Categories 1-4.

Variations of this scenario

Variations include a radiation source becoming breached in an urban environment. Prior to detection, exposure to the radiological component would be spread across multiple locations. Another high-impact variation could involve a radioactive contaminated metal from a scrapyard that is inadvertently melted in a foundry, resulting in radiation exposure. A lower-impact risk involves a radioactive contaminated packaging sold as scrap metal, resulting in hospital admissions. A proportion of these would exhibit clinical signs of acute radiation exposure.

Response capability requirements

Decontamination services and radioactivity scanners would be required immediately. Public communications campaigns would communicate key messages to the public. There would be a requirement for monitoring (sampling and laboratory analysis) and waste management capability would also be impacted.

Recovery

Health impacts among the affected workers (including radiation illnesses) would be expected for a number of years, with a requirement for long-term medical supervision. Decontamination of sites would take several weeks and require extensive resources (cost of clean-up and waste disposal could be substantial).

Technological failure at a systemically important retail bank

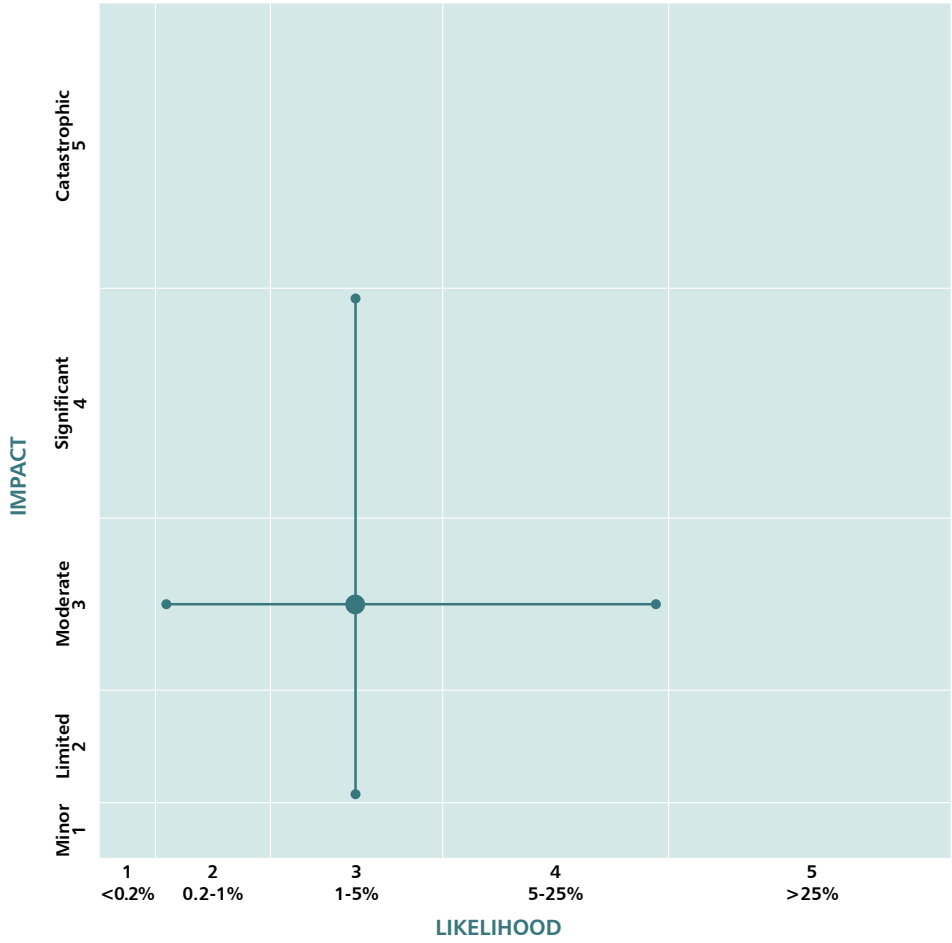
The increasing digitisation of financial services means that a technological failure of IT systems could result in customers being unable to access key account functions and important information, including online banking. The financial regulators' operational resilience policy requires finance sector organisations to ensure their critical business services are resilient to severe but plausible scenarios, including technological failures.

This supervisory framework covers financial market infrastructures (FMIs) and Other Systemically Important Institutions (O-SIIs), critical to the UK's financial stability, who must also consider their risks in relation to harm their institution may cause to the real economy and financial services sector as a whole.

Scenario

The reasonable worst-case scenario is based on a technological systems failure that renders a systemically important retail bank's critical technology inoperable, with a partial outage for 2 days thereafter. Potential immediate impacts would include customers being unable to view account balances, process payments, use online banking or withdraw cash from ATMs. Account data may also be compromised. Online and mobile customers would be locked out of their accounts, with some experiencing disruption in the weeks that follow.

Long-term disruption to consumer-facing banking would impact consumer confidence. The outage would disrupt critical government services for several hours, with longer-term impacts felt for weeks. This would impact people's ability to buy necessary goods, travel to and from work and pay for basic utilities. The most significant impact would be felt by vulnerable customers with only a single bank account. The bank would also likely face heightened fraud and operational losses.



Technological failure at a systemically important retail bank

Key assumptions for this scenario

This scenario assumes that the technical fault directly impacts the IT operations of a UK critical national infrastructure bank, and that the firm's impact tolerances (the maximum tolerable level of disruption) are surpassed. This scenario assumes that the technical fault directly the IT operations of a UK critical national infrastructure bank, and that the firm's impact tolerances (the maximum tolerable level of disruption) are surpassed.

Variations of this scenario

Technological failure of a UK critical financial market infrastructure.

Response capability requirements

Local and national plans to deal with a surge in demand for consumer-facing financial services where online and mobile banking services are offline. Collective incident response capability is managed under the UK's Authorities' Response Framework (ARF).

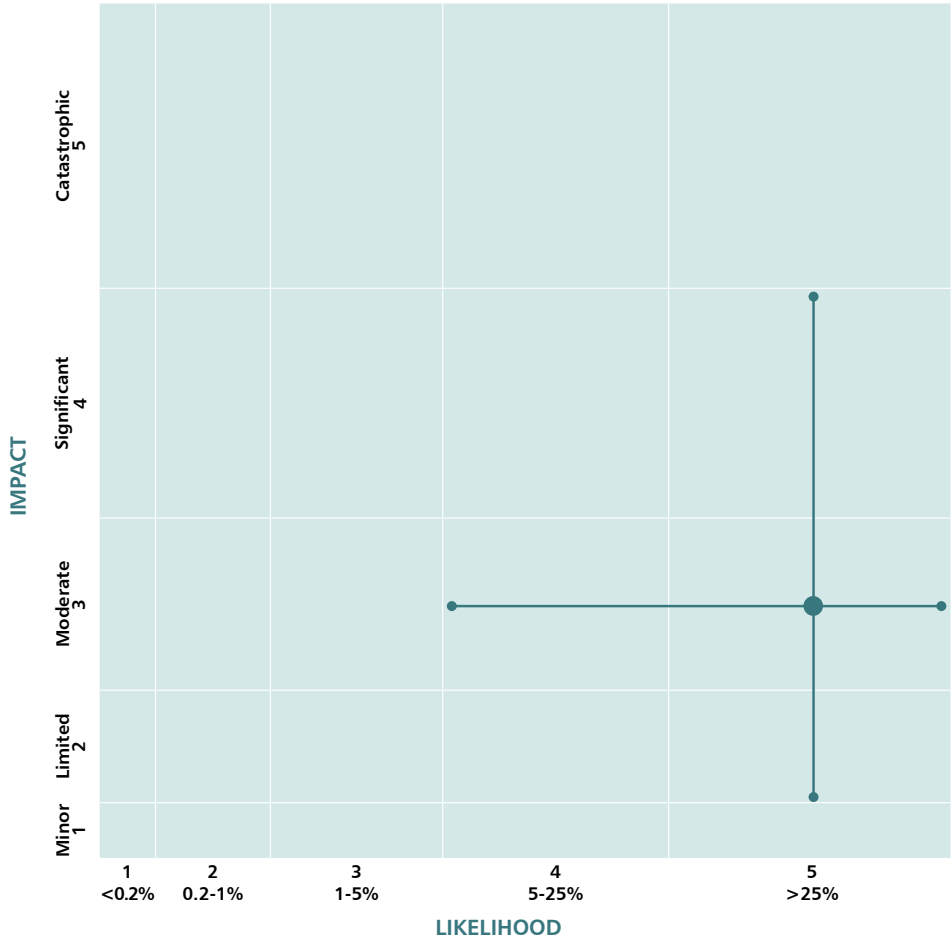
Recovery

Depending on the severity of the technological failure, a full systems recovery could be protracted. Recovery would involve interim actions to provide customer payments and fixing the affected technological systems. Some customers could experience disruption once the technical issue has been fixed as backlogs are cleared.

Technological failure at a UK critical financial market infrastructure

Financial market infrastructures (FMIs) are the networks that enable financial transactions to take place and are a vital part of the UK economy. This means that FMI companies are tightly regulated by the Bank of England to ensure their smooth operation, with technological failures likely to have significant impacts on the UK economy. The financial regulators' operational resilience policy requires finance sector organisations to ensure their critical business services are resilient to severe but plausible scenarios, including technological failures.

This supervisory framework covers FMIs and Other Systemically Important Institutions (O-SIIs), critical to the UK's financial stability, who must also consider their risks in relation to harm their institution may cause to the real economy and financial services sector as a whole.



Scenario

This scenario is based on a technological systems failure causing an outage of a systemically important UK financial market infrastructure (FMI). This would significantly impact the processing of financial transactions. The lack of substitutability of many of these systems and their criticality to the functioning of UK financial systems means a sustained outage could threaten the UK's financial stability. Impacts would be felt across the UK economy. Given the cross-border nature of the financial system and depending on the duration of the outage, there could be significant international implications as a result, with government reputational loss and significant financial loss.

Key assumptions for this scenario

The scenario assumes that the technical fault directly impacts the IT operations of a UK critical national infrastructure FMI. The scenario assumes that the firm's impact tolerances (the maximum tolerable level of disruption) are surpassed.

Variations of this scenario

Variations involve different examples of FMIs. Additional scenarios include the technological failure of a systemically important retail bank.

Response capability requirements

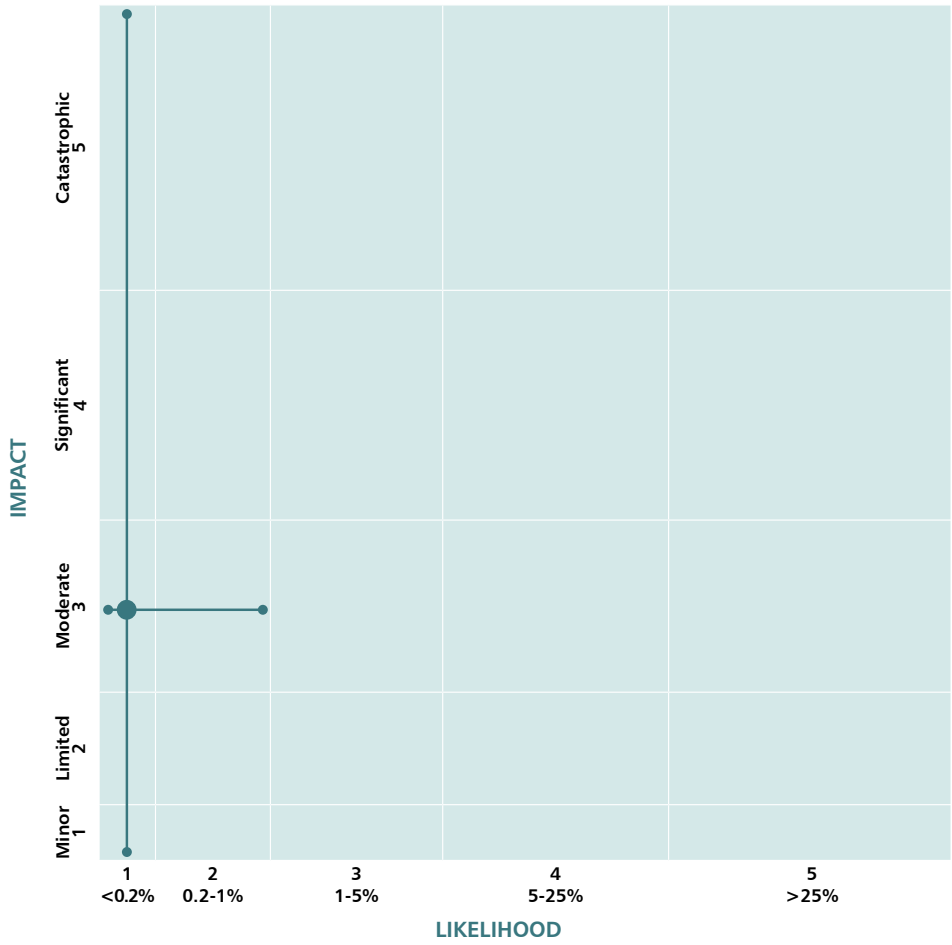
Local and national plans would be needed to deal with a surge in demand for consumer-facing financial services. Collective incident response capability under the UK's Authorities' Response Framework (ARF).

Recovery

Depending on the severity of technological failure, a full systems recovery could be protracted. Recovery capabilities would centre on the particular FMI's response capability requirements. There would be a limited ability to transfer functions or use alternate channels due to the unique profile of each FMI. The recovery would also depend on having a very robust dual site running.

Accidental fire or explosion at an onshore major hazard (COMAH) site

This risk involves a Control of Major Accident Hazards (COMAH) site that produces, stores or uses significant amounts of flammable or explosive substances. There are two types (tiers) of establishment that are subject to COMAH, known as 'Upper Tier' and 'Lower Tier'. Upper Tier establishments hold greater quantities and/or more dangerous substances compared to Lower Tier establishments, meaning that additional requirements are placed on them. Operators of these sites have a legal duty to prevent accidents from occurring and to mitigate their consequences. The Health and Safety Executive develops and enforces legislation, standards, codes of practice and guidance to ensure that operators fulfil these responsibilities effectively.



Scenario

The reasonable worst-case scenario for this risk concerns a major fire and/or explosion occurring at an onshore COMAH site, potentially causing building damage and possible collapse close to the site. The fire would generate a visible plume of smoke that may travel to nearby areas. The accident could result in casualties and fatalities. Other impacts include short-term local transport disruption and economic impacts in the order of hundreds of millions of pounds.

Key assumptions for this scenario

The incident is accidental and occurs at a large industrial complex storing or using flammable substances. The incident produces a cloud of gas or vapour or a spill of flammable liquid, which ignites causing a fire or explosion.

Variations of this scenario

The impacts of the scenario will vary depending on the number of people working on site at the time, how far the nearest population is, the time of day, how long the event lasts, what the site is used for and volume and type of substances involved.

Response capability requirements

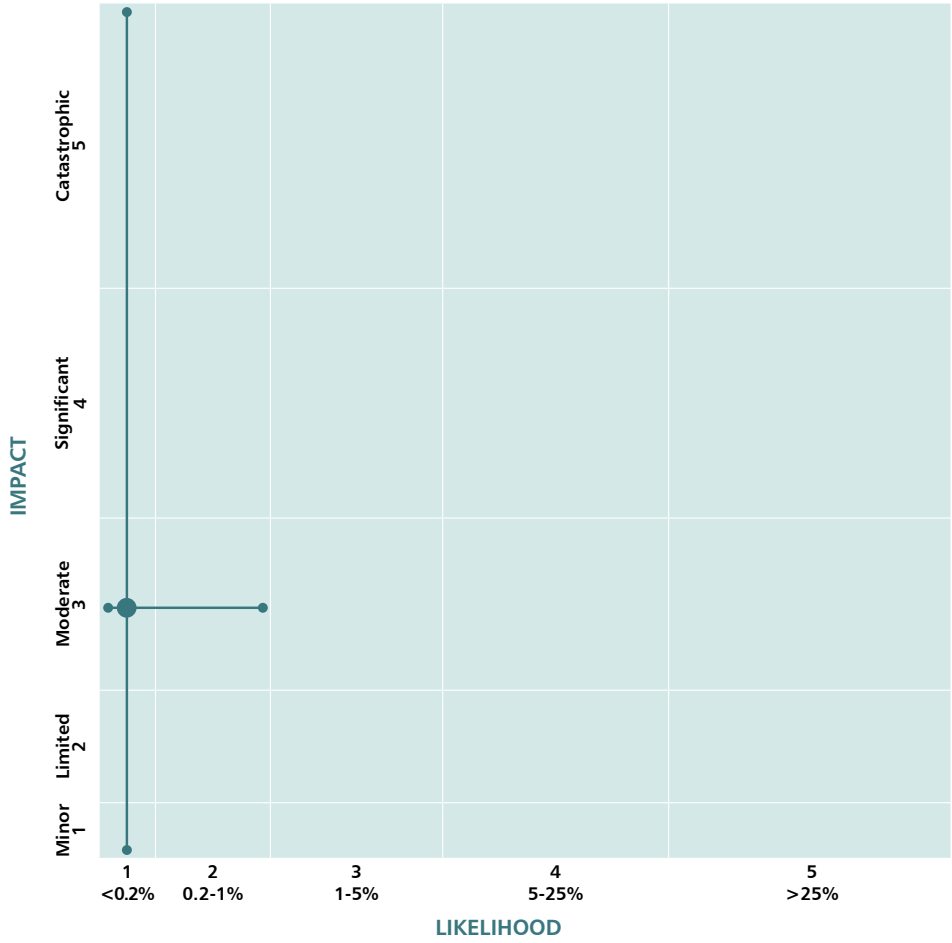
Capability requirements would include temporary evacuation and shelter for displaced people. There would be a need for specialist treatment, surge capacities and appropriate recovery and storage for no-notice mass fatalities and casualties. As a result of rubble and debris, the site would need to be cleaned up and possibly decontaminated and the response would involve search and rescue teams.

Recovery

The health effects arising from exposure to the effects of fire and explosion are likely to be acute but some will continue beyond 5 years. Psychological support may need to be made available to those affected. The duration of environmental contamination could be short (less than one year) or long term (more than 5 years), depending on the site location and inventory.

Accidental large toxic chemical release from an onshore major hazard (COMAH) site

This risk is concerning an incident in which a toxic gas is accidentally released from a Control of Major Accident Hazards (COMAH) site in the UK. There are two types (tiers) of establishment that are subject to COMAH Regulations, known as 'Upper Tier' and 'Lower Tier'. Upper Tier establishments hold greater quantities of dangerous substances compared to Lower Tier establishments, meaning that additional requirements are placed on them. Operators of these sites have a legal duty to prevent accidents from occurring and to mitigate their consequences. The Health and Safety Executive develops and enforces legislation, standards, codes of practice and guidance to ensure operators fulfil their responsibilities effectively.



Scenario

The reasonable worst-case scenario is based on an accidental large release of toxic chemical gas from an onshore COMAH site. The release may involve one of a number of hazardous chemicals and would not necessarily result in a fire or explosion. The site would be located near an urban area and could result in fatalities and casualties. There would also be some long-term health impacts to casualties, with some vulnerable groups disproportionately affected.

Key assumptions for this scenario

This scenario assumes that the incident is accidental and that toxic chemicals would be released as a gas at a large industrial complex or bulk chemical storage site near an urban area.

Variations of this scenario

The impacts of this event would depend on several factors, including the location of the site, the type and volume of gas released, the weather conditions, time of day and individual human responses to exposure. Other variations involve a larger toxic chemical release, which would generate similar impacts but on a larger scale, or a lower scale release of toxic gas with smaller impacts.

Response capability requirements

Site-specific risk assessments are carried out by the site operator, as this is a legal requirement under the COMAH regulations. These assessments inform specific capability requirements locally. Responders will require personal protective equipment (PPE) for recovery of no-notice mass fatalities and to treat no-notice mass casualties. Some temporary evacuation and shelter arrangements may also be required, as well as remediation and potential decontamination of the local environment.

Recovery

The health effects arising from exposure to the toxic gas are likely to be acute, but some will continue beyond 5 years where chemicals pose longer-term hazards to health. Psychological support may need to be made available to those affected.

Accidental fire or explosion on an offshore oil or gas installation

This risk concerns an offshore oil or gas installation. These installations store and process significant volumes of highly flammable hydrocarbon mixtures such as crude oil and natural gas, which could potentially result in a large fire or explosion if released accidently. Operators of these installations have a legal duty to prevent accidents and to mitigate their consequences. The Health and Safety Executive monitors hydrocarbon releases to identify trends and inspects all installations on a regular basis.

Scenario

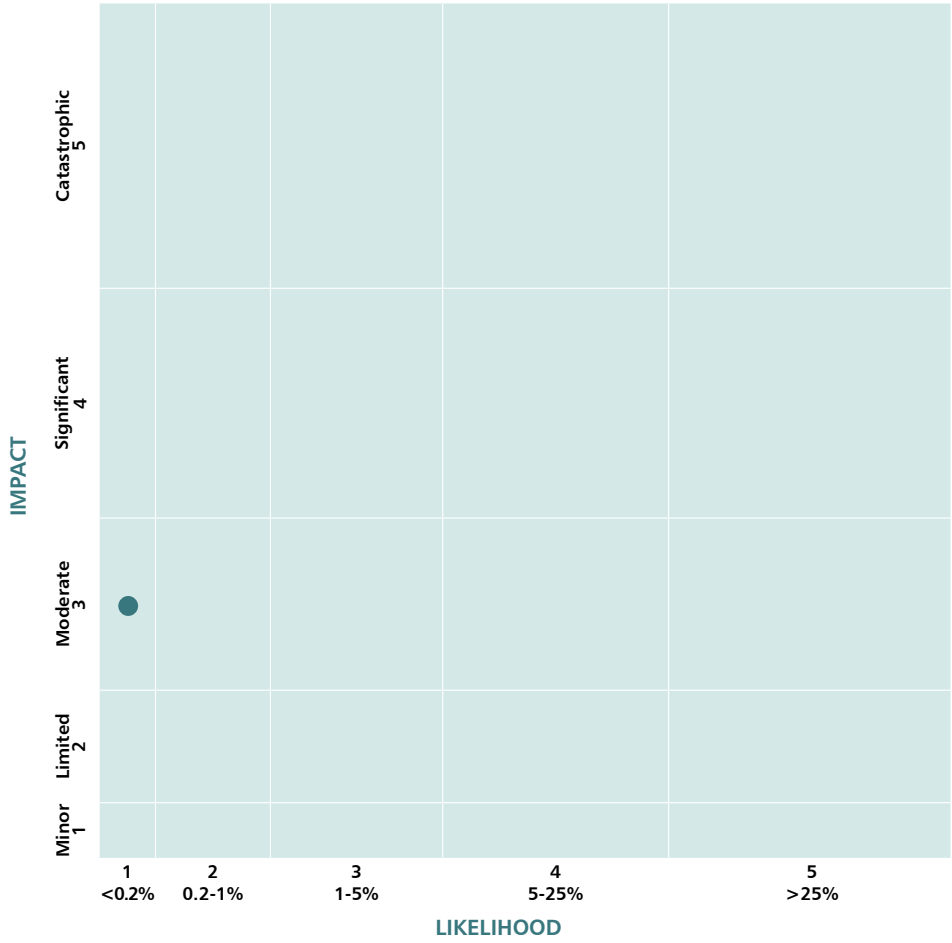
The reasonable worst-case scenario for this risk is a fire or explosion occurring on an offshore oil or gas installation. The incident would be local to the site resulting in casualties and fatalities. There could also be environmental damage. The incident may cause supply issues depending on the type of installation, but it is likely there would be sufficient resilience in the supply chain.

Key assumptions for this scenario

It is assumed that the incident is accidental. The main platform on the installation would be significantly damaged but avoid total collapse. Drilling and key machinery would be closed down quickly, with impacts extending to the people on the platform at the time of the incident.

Variations of this scenario

The impacts of the scenario will vary depending on the size of the fire or explosion, its effect on the integrity of the installation and the size of any resulting substance release. Although the degree of emergency response may differ, the capabilities required of responders are unlikely to change.



Response capability requirements

The capabilities required to manage and respond to an incident would largely be the responsibility of the installation operator. Their onshore command team would need to cooperate with local police, coastguard and the NHS to rescue and evacuate offshore personnel. Firefighting would be carried out by a trained firefighting team with equipment available on the platforms where necessary to assist safe evacuation. Evacuation of the platform and the speed with which this can be accomplished would depend upon weather conditions. The ability to recover, store and identify fatalities and to treat casualties would be required, and operators would need to deliver environmental emergency response plans.

Recovery

There may be some longer-term health impacts for some casualties arising from the incident. Psychological support may need to be made available to those affected. Environmental damage and the associated clean-up operations could be long lasting. Harsh marine weather conditions are more likely to facilitate the break-up of any potential contamination; however, this would also increase the costs of clean-up due to the need to hire suitable equipment and specially trained personnel. Work to decommission, make safe and dismantle a rig damaged beyond repair could take up to 3 years.

Accidental fire or explosion at an onshore fuel pipeline

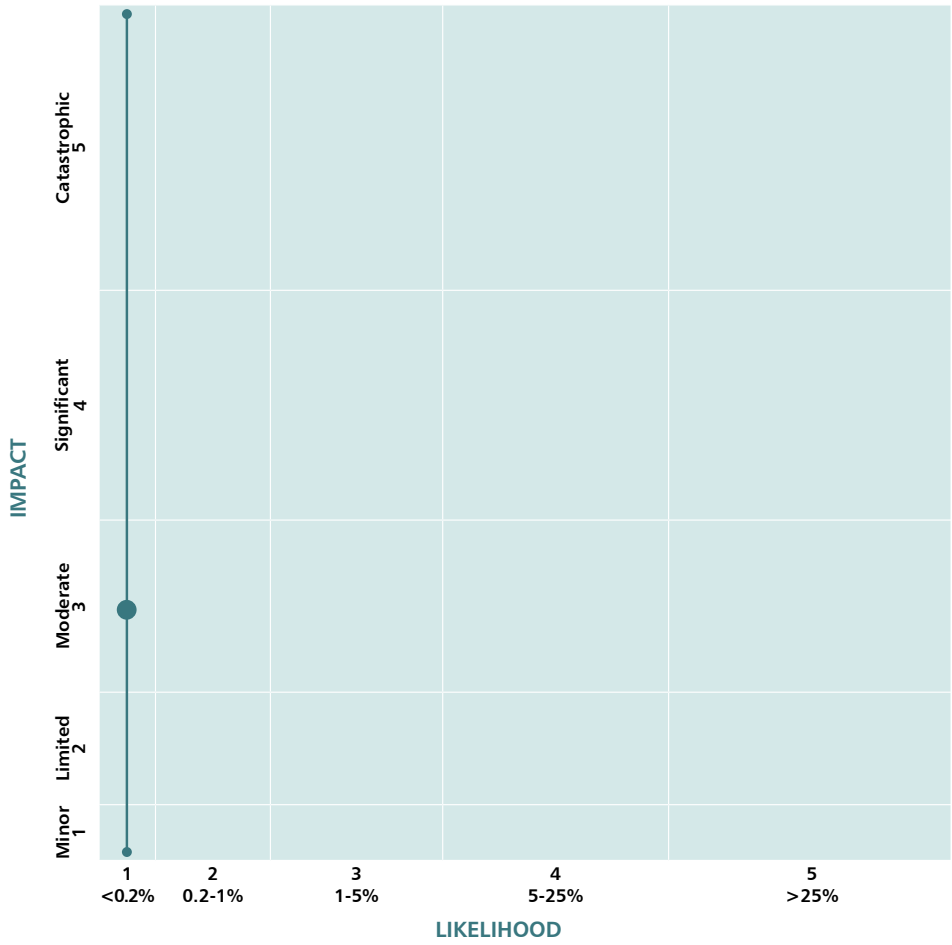
This risk involves an onshore pipeline that transports petroleum and other fuels. Although pipelines are a safe and cost-effective mode of fuel transportation, accidental damage and loss of containment of flammable fuel could potentially lead to fire and explosion. Operators of these pipelines have a legal duty to prevent accidents and to mitigate their consequences. The Health and Safety Executive develops and enforces legislation, standards, codes of practice and guidance to ensure that operators fulfil their responsibilities effectively.

Scenario

The reasonable worst-case scenario for this risk concerns an accidental fire or explosion occurring at an onshore fuel pipeline situated close to a populated area. The ignition of flammable fuel under high pressure would result in a loud explosion, which could cause a crater, destruction of buildings, fatalities and casualties, and evacuation from homes up to 1km around the site. Depending on the fuel involved, there could be long-term environmental contamination. Additionally, up to 1,000 people would require temporary shelter or accommodation, with a number of these potentially requiring longer-term temporary accommodation if their property is seriously damaged.

Key assumptions for this scenario

It is assumed that the incident is accidental and happens close to a populated area. The pipeline can quickly be isolated following the initial fire or explosion, so that demands on emergency responders are substantial but short-lived.



Variations of this scenario

The extent and severity of impacts would depend on a variety of factors including pipeline contents, time of day/night, the time taken to isolate the pipeline, and its location. The release of certain fuels from a pipeline would pose a greater hazard to the human population compared to others, depending on their flammability and combustibility.

Response capability requirements

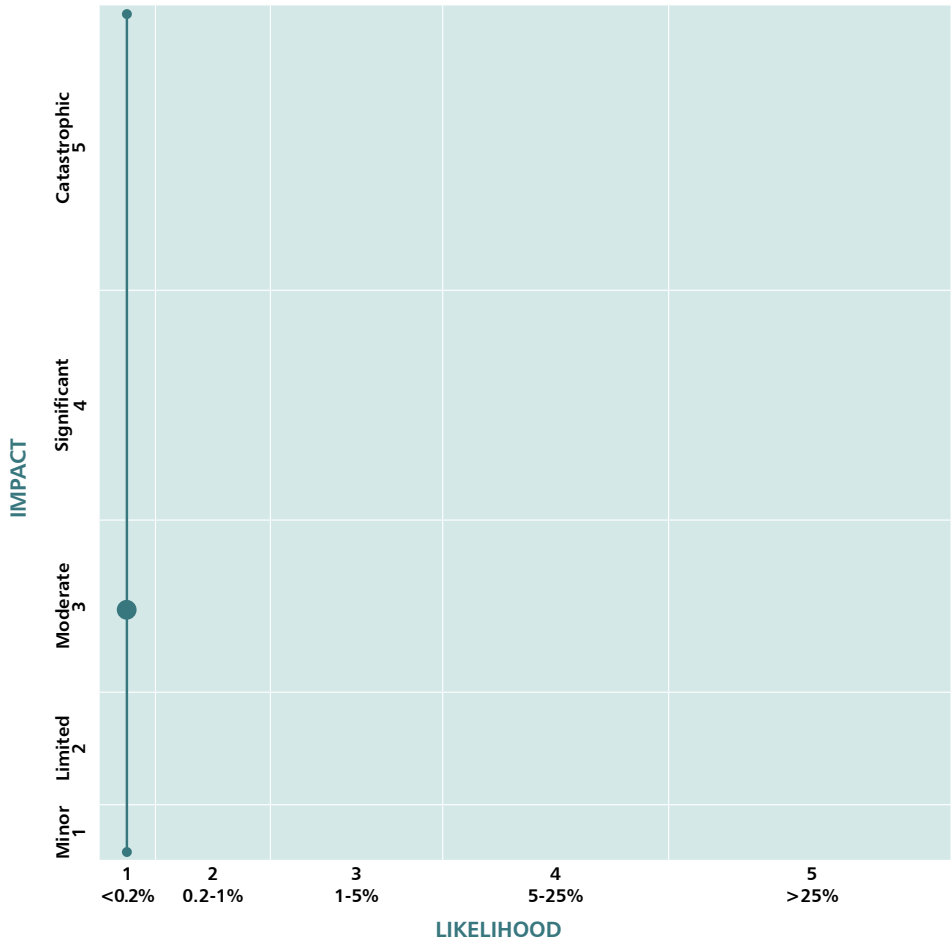
The Pipelines Safety Regulations 1996 do not require local authorities to prepare emergency plans with respect to fuel pipelines, but they are required to plan for emergencies that could happen in their area under other legislation. Pipeline operators are also required to establish emergency procedures for such pipelines. There would be a need for specialist treatment, surge capacities and appropriate recovery and storage for no-notice mass fatalities and casualties. Responders may require personal protective equipment (PPE). Some temporary evacuation and shelter arrangements may be required for displaced people, along with search and rescue teams to locate trapped people. Site clearance plans would be required for the removal of rubble and debris at a local level, and for decontamination of the environment.

Recovery

The health effects arising from exposure to the effects of fire and explosion are likely to be acute but some will continue beyond 5 years. Psychological support may need to be made available to those affected. Making the area safe and treating environmental damage may take up to 5 years.

Accidental fire or explosion at an onshore major accident hazard pipeline

This risk concerns an onshore major accident hazard pipeline (MAHP). These pipelines transport flammable and toxic materials with the potential to cause major accidents if accidently released. Operators of these pipelines have a legal duty to prevent accidents and to mitigate their consequences. The Health and Safety Executive develops and enforces legislation, standards, codes of practice and guidance to ensure that operators fulfil their responsibilities effectively.



Scenario

The reasonable worst-case scenario is based on an accidental fire or explosion occurring at a MAHP situated close to an urban area. The ignition of flammable gas or liquids under high pressure would result in a loud explosion, which could cause a crater, building damage and require evacuation from homes. The fire may continue to burn until the pipeline is isolated. The fire or explosion would result in casualties and fatalities. Some specialist medical services such as intensive care or burns treatment may be required.

Key assumptions for this scenario

It is assumed that the incident is accidental and would involve a loss of containment, producing a cloud of gas or vapour as well as the results of a fire or explosion. This is likely to result in substantial short-term demands on emergency responders, however this should not continue over an extended period of time as pipelines can be isolated.

Variations of this scenario

The range and severity of anticipated impacts could be affected by the location of a pipeline, its contents, design, pressure and construction, the weather and the time of day/night.

Response capability requirements

The Pipelines Safety Regulations 1996 require both a local authority and the pipeline operator to prepare emergency plans for MAHP. There would be a need for specialist treatment, surge capacities and appropriate recovery and storage for no-notice mass fatalities and casualties. Temporary evacuation and shelter for displaced people, site clearance plans and infrastructure repair may be required.

Recovery

The main health effects of exposure will be experienced in the initial incident. There may be long lasting effects for people with continued respiratory issues, but long-latency ill health effects are unlikely. Psychological support may need to be made available to those affected. If the incident involves a high-pressure gas pipeline, there may be some local disruption to supply while repairs take place.

Accidental work-related (laboratory) release of a hazardous pathogen

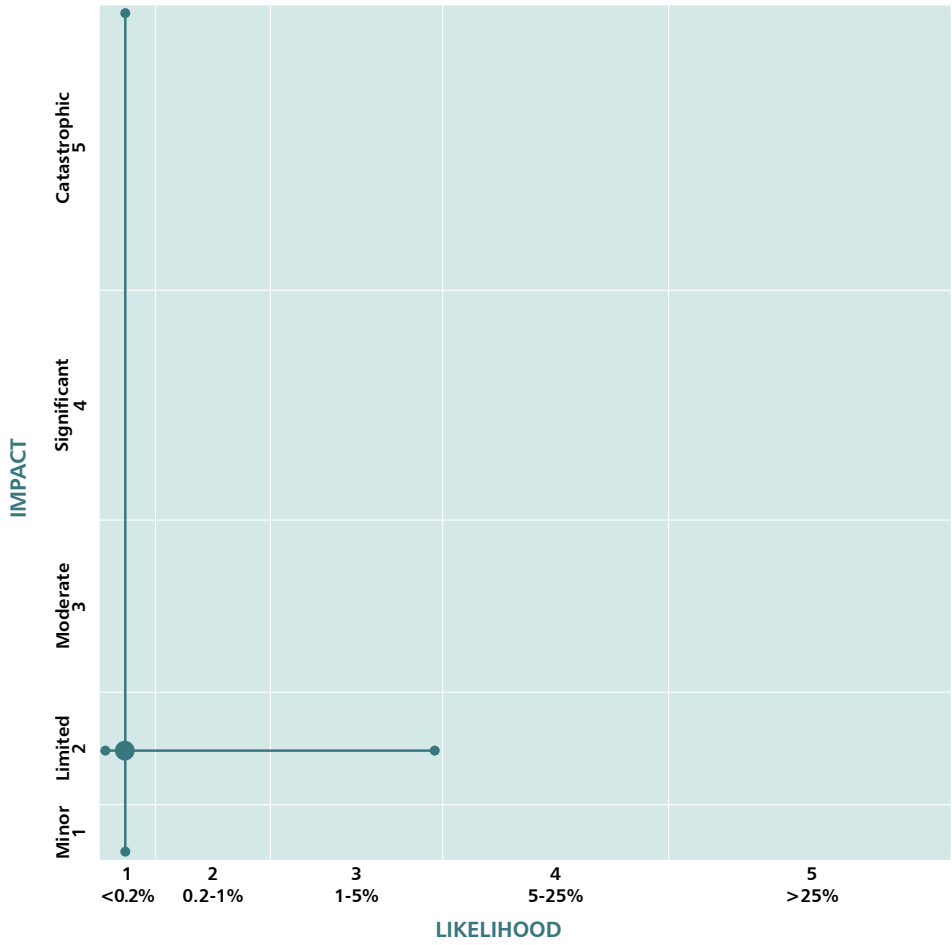
This risk involves the accidental release of a hazardous pathogen from a laboratory in the UK. Operators of these sites must meet strict containment and safety requirements to work with these types of pathogens and develop emergency procedures to mitigate this risk. The UK has a well-established regulatory system to ensure that operators fulfil these responsibilities effectively.

Scenario

The reasonable worst-case scenario is based on the accidental release of an infectious influenza-type pathogen from a UK laboratory. It is assumed that the pathogen would cause an infection that takes several days to emerge and spreads via close contact. This could result in fatalities and casualties requiring hospital treatment, along with cases that can be resolved without the need for hospital admission. The incident could last for several weeks until all contacts are traced and treated.

Key assumptions for this scenario

It is assumed that the outbreak would be identified and contained quickly, without spreading geographically. This would result in a predominantly local outbreak, rather than progressing into an epidemic. The pathogen would be quickly identifiable due to strict regulatory requirements on working with pathogens of this nature. Antiviral drugs would be effective against the virus and made available immediately to restrict further transmission. Human welfare impacts are, however, difficult to estimate with confidence.



Variations of this scenario

The speed of spread within the community will depend very much upon the transmissibility of the virus, the speed with which the outbreak is identified and appropriate mitigation measures enacted, including the efficacy and availability of antivirals. There are also unquantifiable variabilities in terms of individual human immune response. A more likely scenario is that a laboratory worker who is accidentally exposed to a virus during work activity would report this, enabling immediate introduction of containment measures. The worker would be referred for medical treatment and make a full recovery without the onward spread of the virus.

Response capability requirements

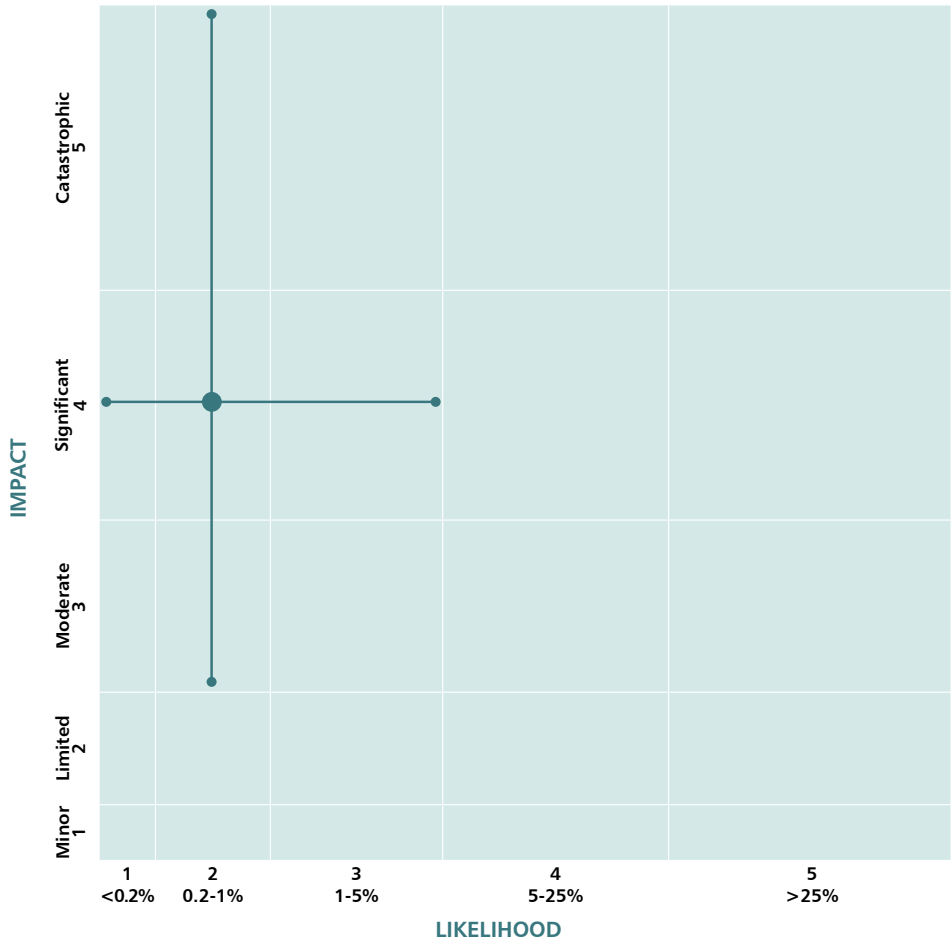
There could be increased demand and disruption to local hospitals. Contact tracing would be required so that all persons in contact with the virus could be identified and treated. The laboratory facilities may require full decontamination and homes of confirmed cases may also need to be deep cleaned.

Recovery

Recovery will take as long as the process to identify, isolate and provide treatment for infected individuals. Longer-term complications include the risk of developing pneumonia (viral or bacterial) some time after the initial illness with some vulnerable groups being at increased risk.

Reservoir/dam collapse

The collapse or breach of a reservoir or dam can be sudden and result in the uncontrolled release of fast-flowing water into a populated area. Potential causes of this may include climate-related land instability, internal erosion or an earthquake. There have been no catastrophic failures of dams in the UK since 1925. However, the incident at the Toddbrook Reservoir in 2019 highlights the significance of this risk and the need to integrate effective preventative measures. This has led to better flood mapping and flood management plans to improve preparation by local resilience forums.



Scenario

The reasonable worst-case scenario is based on a sudden collapse of a reservoir without warning. This would result in flooding, with a substantial quantity of water moving at high speed. There would be casualties, fatalities and significant mental health impacts. Utilities (water, energy, communications) to nearby homes and businesses would be lost, with significant economic impacts resulting from property damage. Recovery operations would be hazardous among collapsed infrastructure and debris.

Key assumptions for this scenario

That the dam collapse occurs with little or no warning and with no time to evacuate local properties. It is assumed that the impact on essential services and communities would be significant and require long recovery times.

Variations of this scenario

Variations to the risk include the amount of warning time prior to the dam collapse, the size and location of the reservoir and a deliberate incident.

Response capability requirements

Since 2020, Department for Environment, Food and Rural Affairs has made it a legal requirement for all owners of large raised reservoirs to have on-site emergency flood plans. Reservoir owners, local authorities and local resilience forums (LRFs) have emergency plans and produce locally specific off-site flood plans from reservoir flood maps. The Environment Agency leads operational preparedness and response to flood impacts and during local-level operation responses and would work as part of a multi-agency team, coordinated through the LRF drawing on resources including the National Flood Asset Register, which has over 100 specialist flood rescue teams on standby to be deployed across the country. The joint Department for Environment, Food and Rural Affairs/ Cabinet Office National Flood Response Centre would coordinate the national UK response.

Recovery

There would be major economic, environmental, infrastructure and humanitarian implications. Key aspects of immediate recovery would involve searching for missing people buried by rubble, debris and sediment, evacuation and shelter of populations, temporary accommodation and clean-up of contaminated urban and agricultural land and environmental damage. There would also need to be long-term repairs to damaged infrastructure (motorways and energy infrastructure) and buildings.

Water infrastructure failure or loss of drinking water

The failure of one or more water treatment works in one region would result in the loss of key public water supply and wastewater services. The water sector has established contingency plans to mitigate a range of water supply incidents. This includes mutual aid capability across the water companies and the provision of alternative water supply, which would prioritise the most vulnerable communities.

Scenario

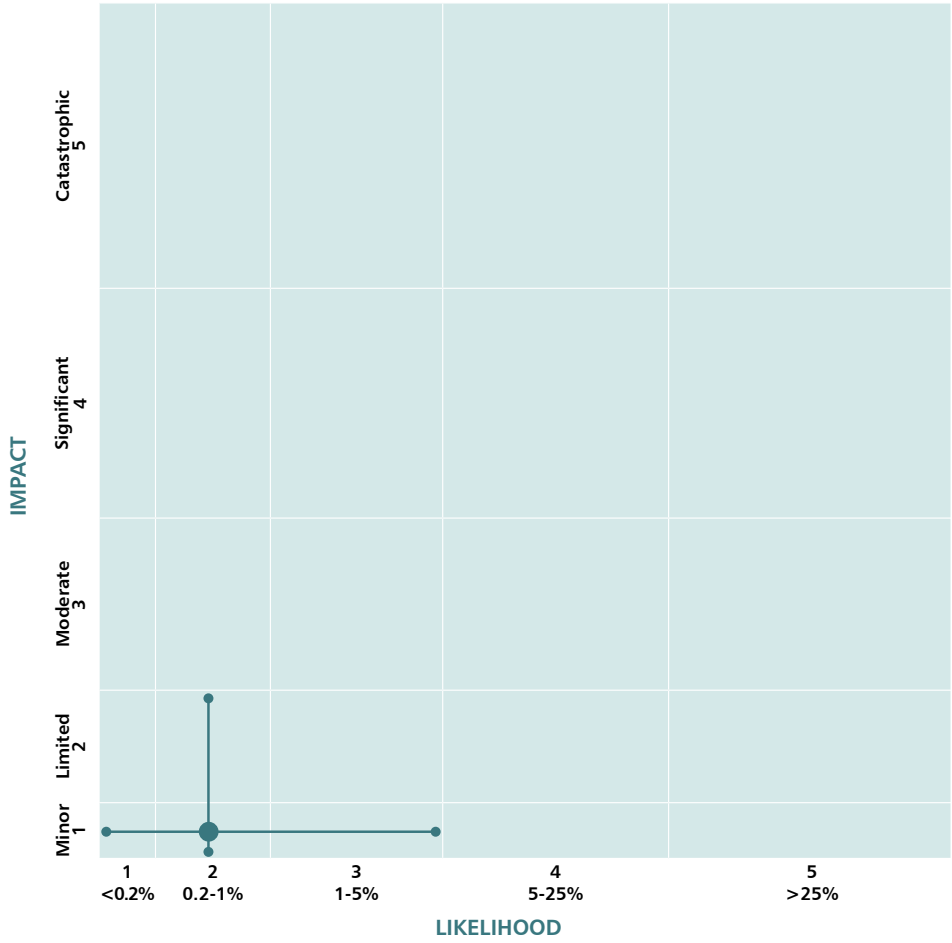
The reasonable worst-case scenario would involve the sudden loss of piped water supply, or the degradation of the piped supply such that it was unfit for human consumption even after boiling. The loss of water would have knock-on consequences to the functioning of essential services such as schools, hospitals and prisons until alternative water supplies are provided or supply is restored.

Key assumptions for this scenario

It is assumed this would be a regional event with loss of drinking water output from one or more water treatment works and there would be limited capability in the water network to reroute supplies from other treatment works.

Variations of this scenario

There are different scenarios that could result in the loss of water supply, including burst water pipes or extreme weather incidents, however the capabilities required to minimise the impacts would remain broadly the same.



Response capability requirements

Water companies in England are required to plan for disruptive scenarios and would seek to use a number of mitigations including rezoning of their network, tankering water from alternative treatment sites, the use of mutual aid from other water companies and the provision of an alternative water supply to affected consumers as soon as possible, but within 24 hours. Alternative water would be prioritised to vulnerable consumers and sites with larger numbers of vulnerable individuals (such as prisons and care homes). Water is a devolved matter and Wales, Northern Ireland and Scotland have equivalent requirements in place.

Water companies would support the local response, which would be coordinated by the local resilience forum and the Department for Environment, Food and Rural Affairs should a national response be required.

Recovery

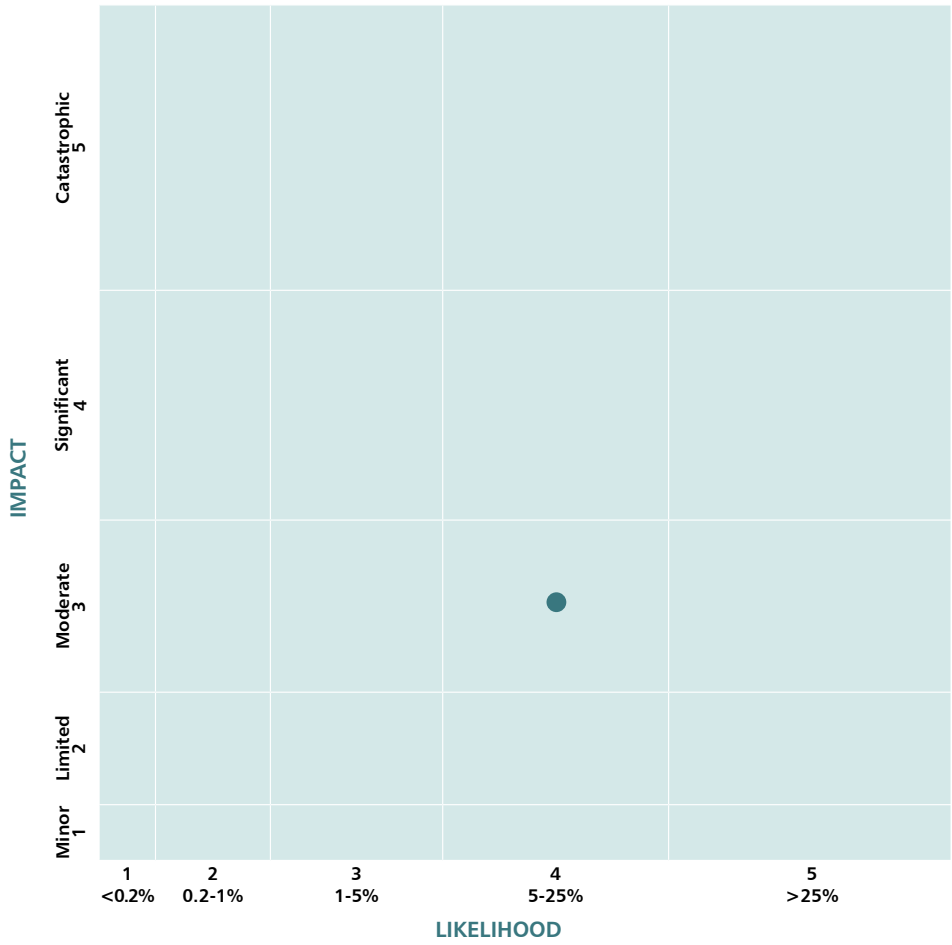
Piped supply would be restored as soon as possible but would be dependent on the extent of the infrastructure damage. Consumers are likely to be gradually brought back on to supply in stages as their area is reconnected. Throughout this time, alternative supplies via bowsers and bottled water stations would be maintained.

Food supply contamination

The contamination of food products with pathogens such as Norovirus, Salmonella, Listeria or Escherichia Coli (E.coli) represents a significant threat to public health. Contamination may result from cross-contamination, poor hygiene, inappropriate storage or contamination with animal waste. The Food Standards Agency (FSA) estimates that food borne pathogens are responsible for 2.4 million cases of disease in the UK each year, at a cost of £9.1 billion. The FSA prioritises keeping the level of foodborne disease low through inspecting, auditing, and assuring businesses in England, Wales and Northern Ireland producing meat, wine and dairy, and through surveillance and preventative programmes.

Scenario

The reasonable worst-case scenario is based on an incident involving a pathogen in the food chain resulting in illness, hospitalisation and possible fatalities in a moderate to large number of people. There could be direct consumer health effects, however the public health impact of food incidents can vary widely. Additionally, the impacts of infection could be more severe in vulnerable groups such as young children, older adults and the immunocompromised. There could be food production/marketing implications, depending on the scale and sector affected (for example major shellfisheries, dairy, livestock production areas). Consumer confidence might also be affected, leading to lost markets and, where staple products are affected, adaptive purchasing behaviours.



Key assumptions for this scenario

It is assumed for the purposes of this reasonable worst-case scenario that the type and source of contamination would not be identified immediately, and the traceability of the contaminated product would be complex and time consuming. The type of food in this scenario is a widely consumed product or an ingredient in a range of different products.

Variations of this scenario

This type of pathogen could be present in other products at different severities. A different pathogen may also be present in similar products.

Response capability requirements

Response capabilities to effectively manage such a scenario would include close liaison between the FSA and public health agencies, possible decontamination services to clear up the site of the incident and mitigation of the risk of widespread loss of consumer confidence in food.

Recovery

Events such as these can potentially cause chronic health effects and demands on health care for a prolonged period following the incident. Psychological support will need to be made available to affected individuals.

Major fire

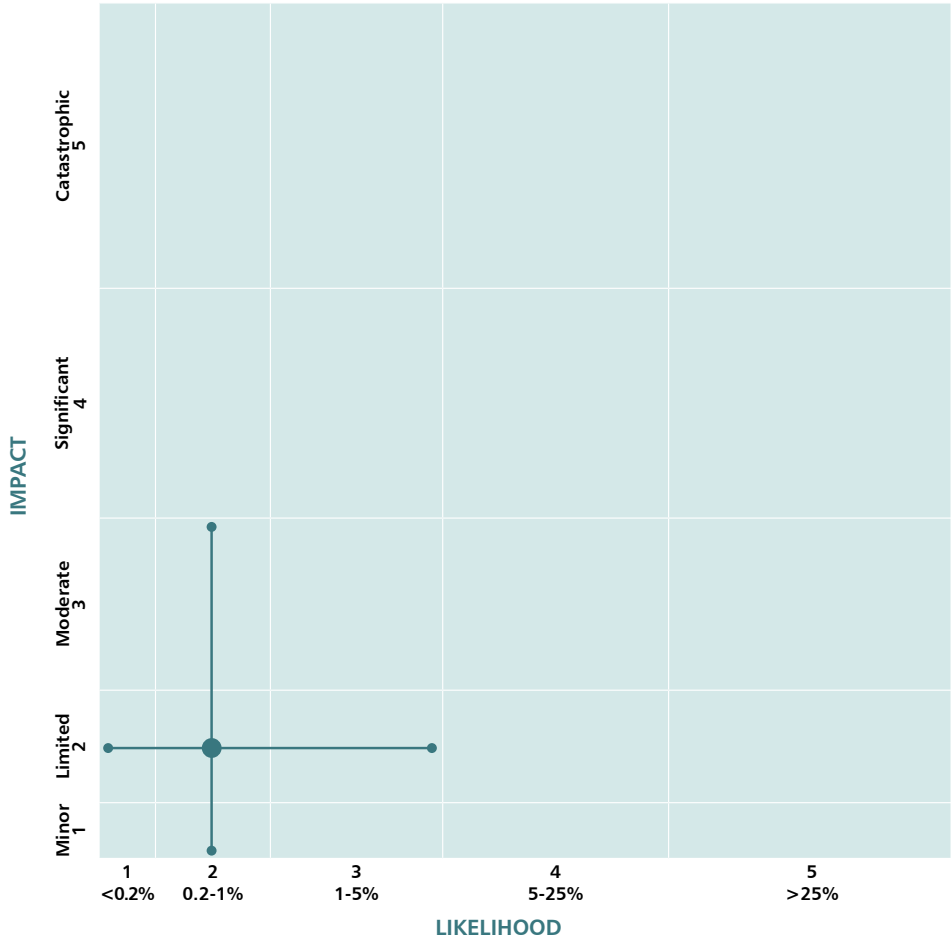
This risk concerns a major fire occurring in the UK. Major fires can start for a variety of reasons, including accidents (for example electrical faults), human activity that combines ignition sources and fuel, malicious activity (for example arson), infrastructure incidents (for example sparks from electricity lines or rail transport) and natural phenomena (for example lightning).

Scenario

The reasonable worst-case scenario is based on major fire, for example in a high-rise residential building, care home, assisted living complex or a hospital, that results in a significant loss of life or injury. There would be significant damage to the building/premises structure, with disruption to local transport services for up to a week. Disruption to essential services would also be expected, with significant pressure on local housing and accommodation due to rehousing requirements of residents.

Variations

A fire could occur in a setting where more vulnerable people live. Within this type of accommodation, there may be residents who cannot respond to an alarm and/or may be less able to self-evacuate, meaning that the impact of the fire could be more severe.



Response capability requirement

Fire and rescue services would lead on the response, including putting out the fire as well as the emergency evacuation and rescue residents. This would include utilisation of national capabilities, for example high-volume pumps and urban search and rescue. Evacuation and temporary shelter would be needed for residents. Treatment and mental health services would be required for psychological casualties. There would also be a requirement for rubble and debris clearance of the site to make it safe.

Recovery

It may take several years to rebuild, with residents residing in temporary accommodation for an extended period. There would be long-lasting impacts to both physical and mental health.

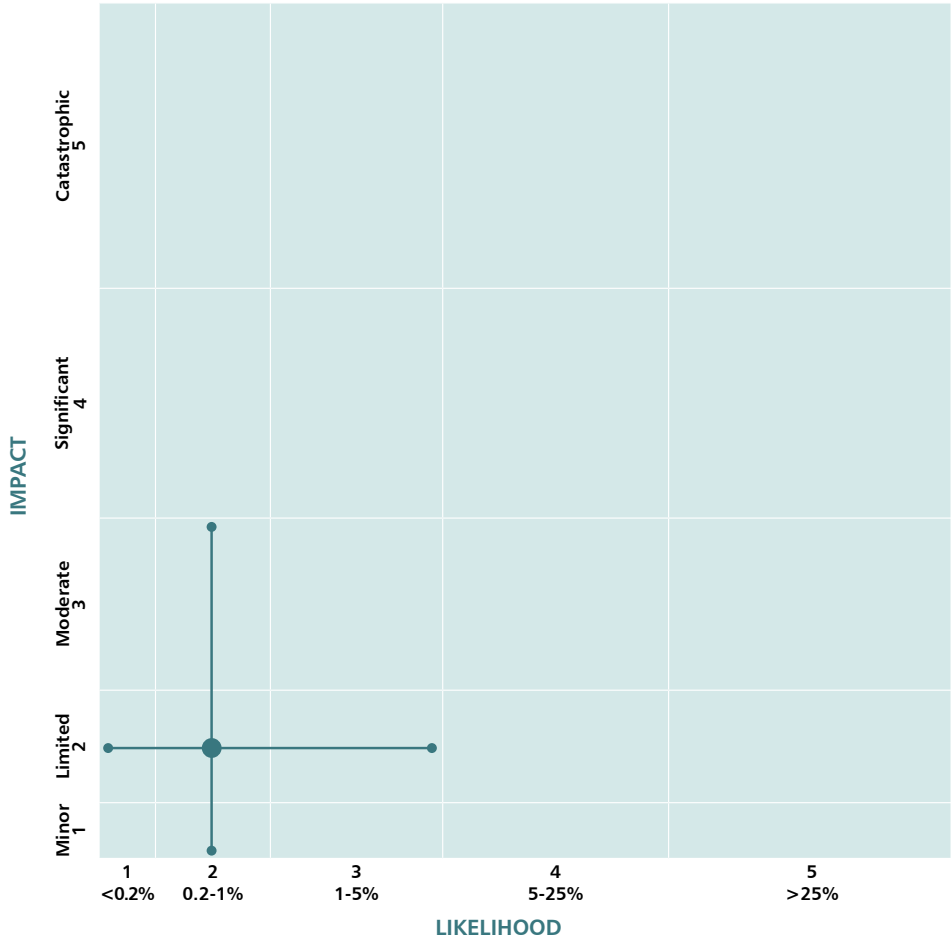
Natural and environmental hazards

Wildfire

A wildfire is an uncontrolled fire that burns vegetation, such as grass, heather, woodland, crops and scrubland.

Climate change is likely to lead to changes in the weather patterns that affect the UK, with longer drier summers anticipated. This could lead to drier vegetation and more frequent, larger wildfires. Fire and Rescue Authorities (FRAs) are required to plan for the foreseeable risks in their area, such as wildfires. Through their Integrated Risk Management Plan (IRMP). Based on their IRMPs, FRAs determine how best to respond to identified risks. This includes local decisions on the procurement of appropriate equipment to meet these risks and help deliver for their local communities.

The Home Office is working with partners across government and the National Fire Chiefs Council (NFCC) to understand the changing risk and to improve prevention of and response to wildfires. The Home Office also takes an active role in communicating wildfire prevention messages through its Fire Kills campaign. These provide outdoor fire safety messages to communication and community safety teams within Fire and Rescue Services to support local delivery of fire prevention.



Scenario

The reasonable worst-case scenario is based on a sustained and widespread extreme wildfire requiring protracted multi-agency attendance over 4 to 7 days, with a significant impact on responder resilience and business as usual activities. Evacuations would be necessary, with a high risk of casualties and/or adverse health impacts. The wildfire would cause significant disruption or damage to critical infrastructure, transport networks, utilities and the environment.

Key assumptions for this scenario

Wildfires typically occur between February and October. There are differences in nature, scale and timing of the risk across the UK. Responsibility for fire and rescue services is devolved.

Response capability requirements

Fire and Rescue services would lead on the response; putting out of the fire and emergency evacuation and rescue of residents. This would include utilisation of national capabilities, for example high-volume pumps and urban search and rescue. Mutual aid from unaffected Fire and Rescue Services would be requested.

Recovery

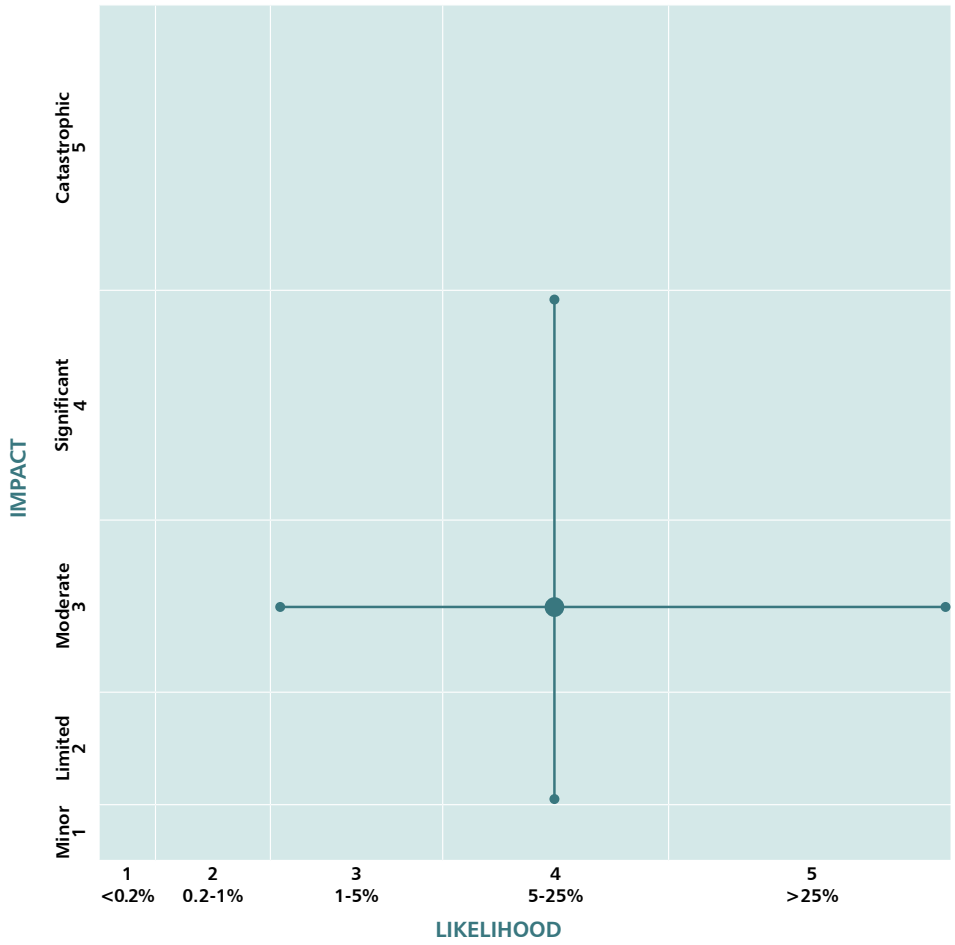
Recovery would be dependent on the location of fire and the vegetation/soil types impacted. Vegetation can take years to recover, with a sustained impact on local wildlife. If the location of the fire features peat in the soil there would be additional longer-term environmental implications due to the release of carbon from the burning.

Volcanic eruption

There are a number of volcanoes across Europe that could affect the UK, such as Santorini in the Aegean Sea and Vesuvius in Italy. However, volcanoes in Iceland (such as Bárðarbunga and Eyjafjallajökull) are of most concern because they are close to the UK, and the high volume of air traffic across Europe that could be impacted.

Scenario

The reasonable worst-case scenario is based on an ash-rich volcanic eruption into UK airspace that results in sporadic and temporary severe disruption to flights in parts of UK or international airspace. Severe disruption could occur for up to 15 days (potentially non-consecutive), with moderate disruption over an additional 10 days during a 3-month eruption period. The duration of severe disruption would be heavily influenced by eruption characteristics, meteorological conditions, concentration of ash and level of aviation activity. Disruption could include severe flight delays, diversions and cancellations, impacting passenger and freight flow. The greatest risk to the UK from volcanic eruptions comes from Iceland. British nationals may be stranded abroad, while foreign nationals in the UK (including those diverted to the UK) may find themselves being forced to delay their return home.



Key assumptions for this scenario

Volcanic eruptions are unpredictable in nature and the severity of volcanic eruptions can be vastly different depending on the type of volcanic eruption. Disruption to aviation services is also dependent on the meteorological conditions, which are also variable.

There are no assumptions about the specific locations. It is assumed that the eruption produces a large ash cloud rising to high altitude in conjunction with meteorological conditions causing major disruption to aviation in the UK and Europe. Some early warning signs may be observed, including volcanic earthquakes, seismic tremor (vibration), ground deformation (changes in elevation), gas emissions or meltwater from glaciers.

Variations of this scenario

A lower impact, higher probability scenario could see a volcanic eruption with explosive phases over a 2-week period with smaller ash plumes or winds that carry the ash further north/away from the UK. This would result in ash concentrations in the UK not being sufficient to cause significant travel disruption, but there is some anxiety and people could postpone travel resulting in an economic impact on the airline industry and wider UK. There could be disruption to aviation in Iceland and/or Scandinavia.

A higher impact, lower probability variation involves a large eruption (volcanic explosivity index 7, VEI7+) generating ash and gas that is carried across the northern hemisphere, causing widespread devastation. Aviation could experience significant disruption across several countries in this period. The eruption could lead to an international humanitarian crisis and include major disruption to supply chains, international displacement, and hazardous weather.

Response capability requirements

The London Volcanic Ash Advisory Centre (Met Office) would produce volcanic ash forecasts and guidance to the relevant agencies and airlines. Consular support would be required for British nationals stranded abroad.

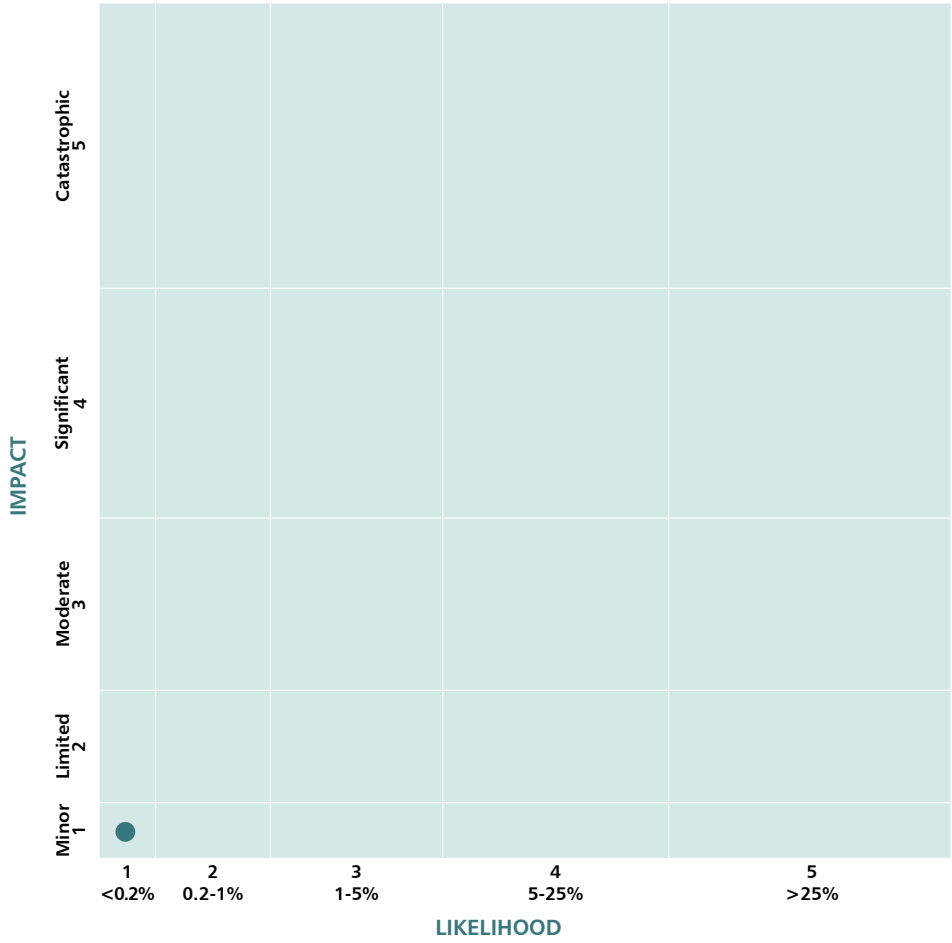
Recovery

Eruptions can last several months to a year with different explosive phases, with disruption to aviation services also being dependent on meteorological patterns. There could be a period of days before air services return to normal as the backlog is managed.

Earthquake

Earthquakes in the UK are rare, and an earthquake powerful enough to inflict severe damage is unlikely. Damage from UK earthquakes would be greatest in historic buildings such as churches, monuments and Victorian or Edwardian terraced housing. The risk of damage would be greatest closest to the epicentre and decrease with distance. In 2007, a very shallow earthquake occurred near Folkestone in Kent, resulting in power outages, transport disruption and widespread superficial damage. The most damaging UK earthquake in terms of intensity occurred in 1884 in Colchester, Essex. Approximately 1,200 buildings required repairs to collapsed walls, chimneys and roofs. The maximum observed intensity for the earthquake was 8 on the European Macroseismic Scale (EMS).

The British Geological Survey (BGS) operates a network of seismometers throughout the UK to acquire seismic data on a long-term basis and to help coordinate an appropriate emergency response, plan for future events and improve confidence in seismic hazard assessments. BGS also collates information on historic earthquakes, to improve estimates of earthquake recurrence rates, a key part of hazard assessment. These activities are part of its Seismic Monitoring and Information Service.



Scenario

The reasonable worst-case scenario is based on earthquake activity in the UK that results in the ground shaking with at least an intensity of 8 on the EMS, which causes damage to buildings and infrastructure.[2] This could result in some fatalities and casualties due to falling masonry or interior damage. Damage to buildings would include moderate structural damage along with heavy non-structural damage, for example extensive cracks in walls, complete collapse of chimneys. More substantial damage could

occur to more vulnerable structures. Such an earthquake may cause significant disruption to infrastructure, transport and communications, even if the physical damage is comparatively minor. There may be power outages caused by vibration of apparatus along with disruption to transport and communications networks. Safety inspections of high-consequence structures and installations including nuclear power plants, dams and reservoirs, bridges and tunnels would likely be required.

Key assumptions for this scenario

The risk assumes that no critical infrastructure is damaged to an extent that overwhelms existing emergency plans. It assumes one EMS 8 earthquake, with further related earthquakes having only minor impacts.

Variations of this scenario

A higher magnitude earthquake, or one that affects more critical infrastructure or built-up areas would have higher impacts.

Response capability requirements

Capabilities required to deal with the aftermath from an earthquake are largely covered by plans put in place by Local Resilience Forums (LRFs). This includes the restoration of essential services (gas, water, electricity, communications) due to pipes or cables being disrupted. Damage to infrastructure such as power or communications networks will require specialist intervention. Additional support could be provided via mutual aid agreements with neighbouring local authorities or LRFs – supplemented as necessary by national support (for example specialist Fire and Rescue equipment held as national assets).

Recovery

Temporary or permanent rehousing may be necessary where residential properties are unsafe or unliveable (due to a lack of access or a lack of services), and while clearance and assessment is carried out. Temporary relocation of commercial premises or other infrastructure such as schools might be necessary where the properties have been damaged and are considered unsafe or unusable. There are unlikely to be any significant long-term implications from an earthquake, although there may be a spike in numbers of people seeking access to mental health services for psychological support in the months after the incident. Vulnerable persons and children in particular are more likely to require support.

[2] A magnitude 6 earthquake at a moderate depth in a densely populated urban area would lead to ground shaking at intensity 8 EMS at distances of up to a few kilometres from the epicentre and 7 EMS at tens of kilometres away.

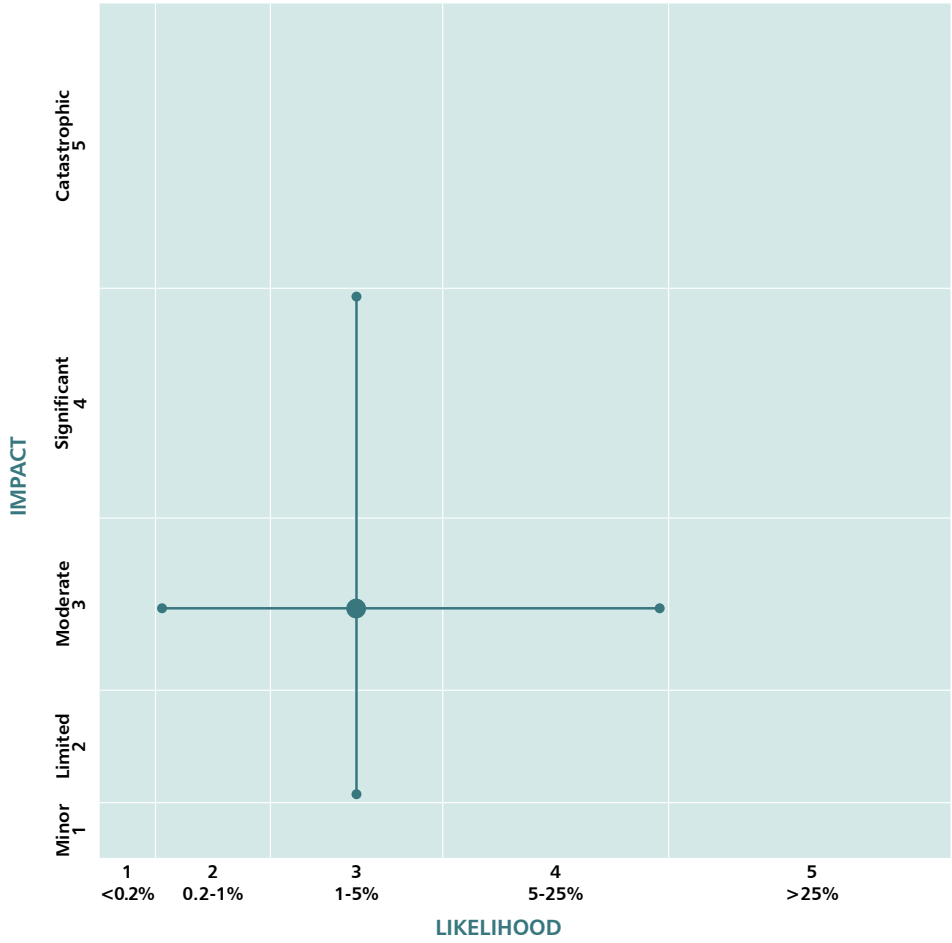
Humanitarian crisis overseas: natural hazard event

A natural hazard event such as an earthquake, hurricane or tsunami may result in a humanitarian crisis overseas that directly impacts UK interests or citizens. For example, the UK has provided extensive humanitarian support to Turkey and Syria following devastating earthquakes in February 2023. This includes millions of pounds of financial support, medical personnel, and items such as tents and blankets.

Scenario

The reasonable worst-case scenario is based on a major earthquake (magnitude 8.0+) occurring along the Sunda-Andaman fault zone in the Bay of Bengal. This would result in a tsunami that impacts Myanmar, Bangladesh, western India, and Sri Lanka, and cause casualties and fatalities among British and non-British nationals. The UK would also have a significant diaspora population from the affected regions.

This scenario could lead to the destruction of housing along the Bangladesh coast, impacting a significant number of people including refugees. In Dhaka, Chittagong and Kolkata, there would be destruction to critical infrastructure, with casualties, and displacement also expected. In Western Myanmar, a tsunami would impact the conflict-affected Ayeyarwady and Rakhine states. In Northeast India, populations would be impacted by destruction to property and infrastructure. In Sri Lanka, the north-eastern coast would be hardest hit.



Variations of this scenario

This scenario could manifest across different geographies and be caused by different natural hazards. An event impacting multiple countries would require the same capabilities.

Response capability requirements

The UK's capability to respond would be through the provision of international search and rescue, operational infrastructure support and humanitarian assistance. There may be an additional refugee dynamic, particularly for people with family based in the UK.

Recovery

Recovery from the disaster would require sustained financial support from donors and the UN system. Society and conflict dynamics in conflict-affected states would likely be altered geopolitically.

Disaster response in Overseas Territories

The Overseas Territories (OT) are particularly vulnerable to high-impact natural hazards such as hurricanes, volcanoes and earthquakes. For example, 2 devastating hurricanes (Hurricanes Irma and Maria) led to widespread destruction across the Caribbean in 2017.

Scenario

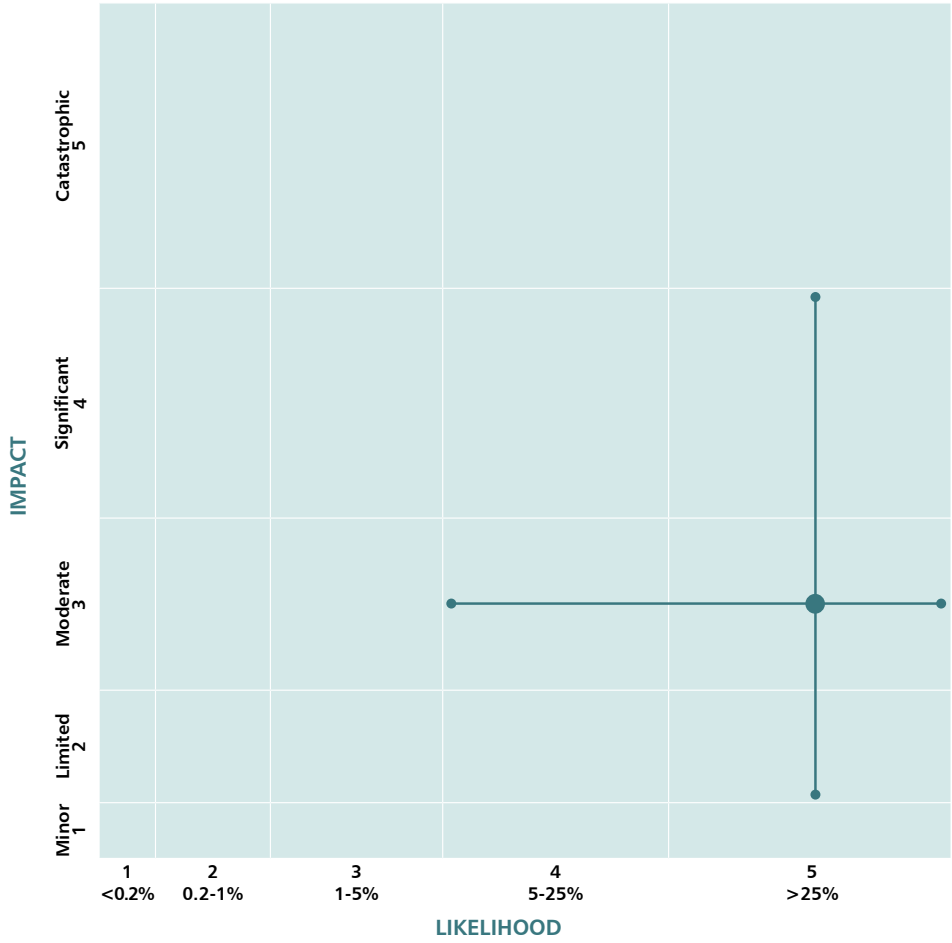
One possible scenario is based on a hurricane occurring in one of the Caribbean OTs that exceeds local response capacity and requires significant short-term support (humanitarian aid and emergency services) and long-term UK response (relief and recovery). It is possible that a natural hazard may hit several Caribbean OTs at once, such as Hurricanes Irma and Maria. Impacts could include fatalities and casualties, damage to infrastructure and security consequences (law and order breaking down). There would also be a significant impact on the economy and wider society, as well as a risk to the UK Government's reputation during the recovery operation.

Key assumptions for this scenario

The scenario assumes that the small government structures in the OTs do not have the capability to provide adequate crisis management.

Variations of this scenario

The 14 inhabited OTs are spread across the globe and are susceptible to different disasters, with a major disaster in any of them requiring some form of response. For example, a natural hazard hitting an OT will involve the local population and possibly large numbers of tourists. Some OTs have active volcanoes – were they to erupt, this would be another scenario that would cause widespread disruption and might require evacuation.



Response capability requirements

Initial support would need to be flown in from the UK, who would then work with the OT government to assess and plan for longer-term recovery. Cross-government support may be required in the immediate response phase.

Recovery

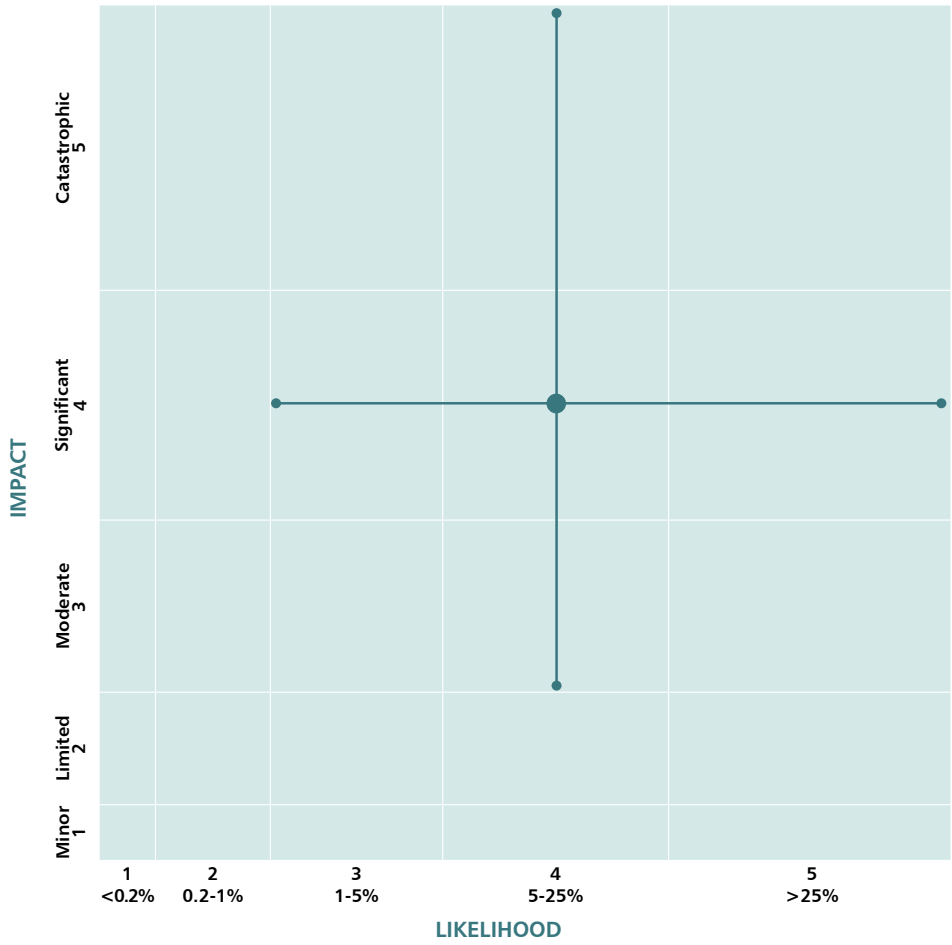
The first few days would be critical as UK support would be needed to reopen ports, re-establish order and repair key utilities (water, power, etc). The organisation would need to transition to a long-term support model to help the OTs rebuild over time. It is impossible to predict what the overall impact would be, but there would potentially be major reconstruction work required.

Severe space weather

The term 'space weather' describes a series of phenomena originating from the sun, which include solar flares, solar energetic particles and coronal mass ejections. Day-to-day space weather causes little more than the Aurora Borealis in polar regions, but strong space weather events can bring disruption to many vital technologies. Orbiting satellites are particularly vulnerable to space weather effects, and can be damaged or temporarily disabled.

Scenario

The reasonable worst-case scenario for this risk is based on a severe space weather event, approximately the same scale and magnitude as the Carrington Storm of 1859, lasting for 1-2 weeks. It includes a number of different solar phenomena including coronal mass ejections, solar flares, solar radiation storms and solar radio bursts. Each phenomenon would likely occur several times during a 2-week period, with each varying in magnitude, temporal and spatial extent. Impacts may include regional power disruptions, loss or disruption of Global Navigation Satellite Systems (for example Global Positioning System (GPS)) and some telecommunications (for example satellite communications and high-frequency radio), disruption to aviation, an increase in background radiation doses at high altitudes and in space, and possible disruption to ground-based digital components. The catalogue of tracked objects on-orbit would be significantly impacted, raising the risk of on-orbit collisions. There may also be second order impacts such as fatalities and casualties (for example, in the event of power disruptions).



Key assumptions for this scenario

The impacts of severe space weather would be global, although the magnitude would vary, with the key dependencies being latitude, reliance on access to space for the operation of key services and the resilience of engineered and digital infrastructure.

Variations of this scenario

Notable variations are possible in the timescale, type and magnitude of driving solar activity. Therefore, significant events with lesser or greater overall and/or differential impact spectra should be anticipated. This could lead to greater disruption in some sectors, such as aviation and the emergency services.

Response capability requirements

Mobile back-up power generation would be required in some areas for a sustained period, while damaged electricity transformers are replaced, which could take several months. Additionally, resilient communications systems and support for local emergency services and vulnerable members of these populations will be needed.

Recovery

Loss of power due to safety system trips in urban areas could be recovered in a matter of hours. In the event of electricity transformers needing to be replaced in remote coastal areas, recovery could take several months based upon current replacement transformer availability. Loss of, or disruption to, satellite based services and Global Navigation Satellite Systems (for example GPS) has a recovery time of several days, with a small number of satellites non-recoverable. It could take weeks for flight schedules (especially long-haul carriers) to fully return to normal. The catalogue of tracked objects on-orbit (satellites and debris) could similarly take weeks to re-establish, with this temporarily raising the risk of collisions.

Storms

Climate change has already altered the risk of certain types of extreme weather in the UK, with evidence suggesting that the frequency and intensity of storms is likely to increase in the future. The UK has experienced several severe storms over the last few years, including Storm Eunice in 2022, which brought gusts in excess of 100mph. The impacts of the storm across the UK included 3 fatalities, school closures, power cuts and nationwide cancellations of transport services.

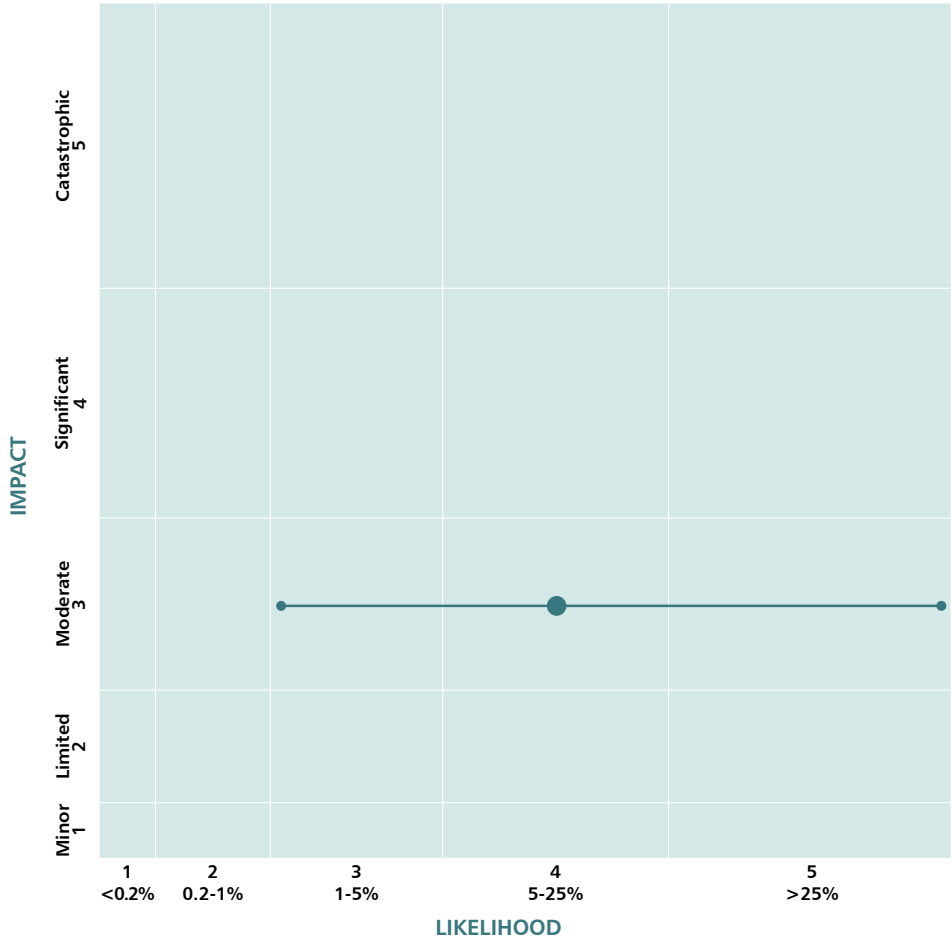
Scenario

The reasonable worst-case scenario is based on storm force winds affecting multiple regions of the UK for at least 6 hours during a working day. Most inland, lowland areas would experience mean (average) wind speeds in excess of 55mph, with gusts in excess of 85mph. Although the storm would be over in less than a day, disruption to infrastructure including power, communications, transport networks, homes and businesses could last for 1-4 days and for more than 5 days in remote rural locations.

There would likely be some casualties and fatalities, mainly due to falling trees, structures or other debris. Some environment and economic impact would also be expected, due to fallen trees and disruption to transport networks.

Key assumptions for this scenario

This risk is based on historical events, primarily combining the impacts of the October 1987 and Burns Day 1990 storms. The likelihood of these events varies, with northern areas more likely to be affected.



Variations of this scenario

In a variation, wind strengths may be less, but from a direction other than the prevailing westerly/southwesterly. This may bring additional hazards (for example snow) and vulnerabilities to trees and infrastructure.

Response capability requirements

The Met Office National Severe Weather Warning Service provides warnings for severe weather (including wind) up to 7 days ahead of it affecting the UK. This service gives advance warning of storms and enables individuals and organisations to plan and mitigate against the potential impacts ahead of the severe weather.

Recovery

For most of the impacts in this scenario, recovery would take place over several days, but could take longer in some instances once the storm has passed. Power and communications supplies to affected rural areas may be last to be restored. There may, however, be some long-term, even permanent, impacts to the environment, as trees and habitats that have been destroyed by the storm could take a long time to become re-established.

High temperatures and heatwaves

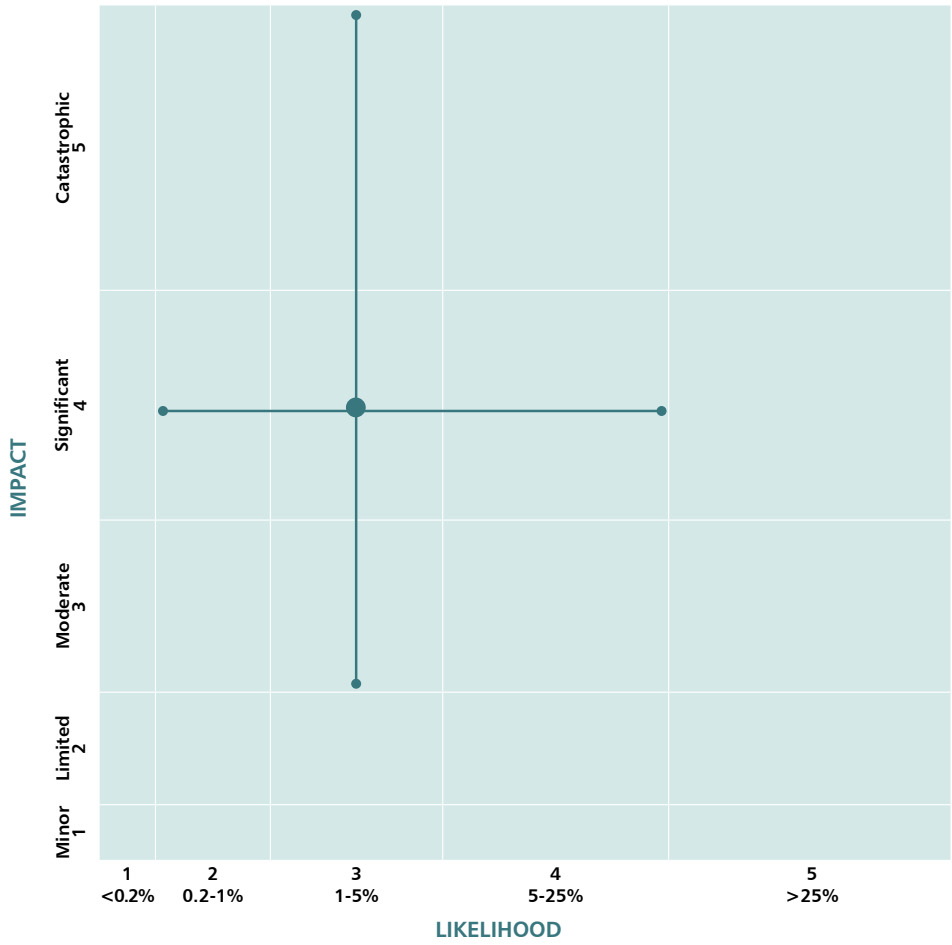
Climate change means that the risk of extreme heat has become more likely in the UK, with this trend expected to continue over the coming decades. A heatwave is defined as an extended period of hot weather relative to the expected conditions for an area at that time of year. The UK experienced a series of heatwaves in the summer of 2022, with temperatures reaching up to 40°C in some areas.

Scenario

The reasonable worst-case scenario is based on an extended period of high temperatures and would affect 50-70% of the UK population. This would take place over 5 consecutive days, with maximum temperatures exceeding 35°C. Temperatures may approach or exceed 40°C in some places, with this most likely in parts of south-eastern, eastern, or central England. Such a spell of weather would cause significant health impacts to the general population, with excess deaths above the number experienced in a normal summer expected. Disruption to transport networks, supply chains, power supplies and water supplies would be expected. Social and economic disruption would be likely as everyday behaviours have to change, including working patterns and levels of productivity. Other hazards are very likely to occur concurrently with, or immediately after, the heatwave, including flooding from severe thunderstorms, poor air quality, drought, and wildfires.

Key assumptions for this scenario

The influence of climate change on the increased likelihood and intensity of high temperature episodes is already being observed, and this increase will continue. Additionally, there is evidence that mortality increases significantly with increasing temperatures in heatwaves.



Response capability requirements

The Met Office National Severe Weather Warning Service provides warnings for severe weather (including extreme heat) up to 7 days ahead of it affecting the UK.

The UK Health Security Agency (UKHSA) has launched the Adverse Weather and Health Plan (AWHP) as part of a commitment under the National Adaptation Plan to bring together and improve existing guidance on weather and health. The AWHP brings together the previous Heatwave Plan for England, first published in 2004, and the Cold Weather Plan for England. The AWHP builds on existing measures taken by the government, its agencies, NHS England and local authorities to protect individuals from the health effects of adverse weather and build community resilience.

The Heat-Health Alert System will transition to impact-based alerting for summer season 2023, with the Cold Weather Alert system following in winter 2023/2024. The alerts will be issued by UKHSA in collaboration with the Met Office, with users needing to register for this new alerting system.

Recovery

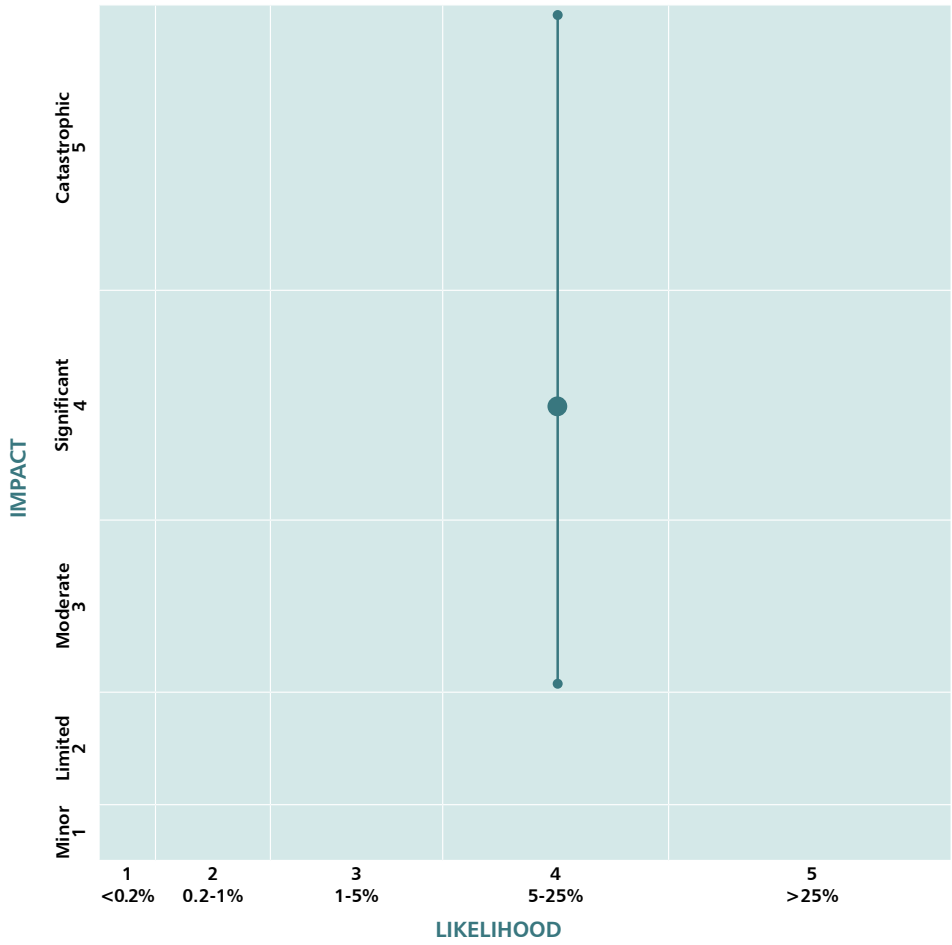
During periods of heatwave, there is generally an increased risk of sunburn, which in the long term could lead to an increase in skin cancer. However, it is not clear that a short period heatwave event such as this scenario, would really have a major long-term impact. Recovery from this event would be quite quick. Where high temperatures and heatwaves lead to secondary impacts such as an increase in the likelihood and impact of wildfires and longer-term drought conditions, recovery due to these secondary impacts may take longer.

Low temperatures and snow

Winters with low temperatures and heavy snowfall pose a significant threat to human welfare, essential services and the economy. In late February and early March 2018, the UK experienced a spell of severe winter weather with very low temperatures and significant snowfall. This event became known as 'The Beast from the East' in the media and led to widespread impacts across the UK, including disruptions to transport services, school closures and power cuts.

Scenario

The reasonable worst-case scenario is based on snow falling and lying over multiple regions of the UK and a substantial proportion of the UK population, including substantial areas of low-lying land (below 300m), for at least one week. After an initial fall of snow, there would be further snow fall on and off for at least 7 days, with brief periods of freezing rain also possible. Most lowland areas would experience some falls in excess of 10cm at a time, a depth of snow in excess of 30cm for a period of at least 7 consecutive days with daily mean temperature below minus 3°C. Overnight temperatures would fall below minus 10°C in many areas affected by snow. Such a spell of weather would affect vulnerable communities, particularly older people and those with pre-existing conditions (for example cardiovascular/respiratory disease). An increase in falls, injuries (for example fractures), road accidents and hypothermia would also be expected. There would be excess deaths, above what is experienced in a normal winter, with a significant number of casualties and fatalities, placing significant pressure on health and social care services. Considerable impact to essential services, along with economic impact, would be likely due to disruption to transport networks, power or heating fuel supplies, telecommunications and water supplies. Schools and businesses would also be impacted by such disruption.



Key assumptions for this scenario

The risk assumes that all types of impact experienced during previous cold and snow events are likely to occur during such a spell of weather described in the risk. High level and rural communities are likely to be affected for longer by snow than lower altitude towns and cities.

Variations of this scenario

Severe snow/cold events could be longer, cover more low-lying land, and be accompanied by significant drifting. An event affecting the rest of Europe could affect supply chains.

Response capability requirements

The Met Office National Severe Weather Warning Service provides warnings for severe weather (including snow) up to 7 days ahead of it affecting the UK. This service gives advance warning of snow and ice and enables individuals and organisations to plan and mitigate against the potential impacts ahead of the severe weather.

The Heat-Health Alert System will transition to impact-based alerting for summer season 2023, with the Cold Weather Alert system following in winter 2023/2024. The alerts will be issued by UKHSA in collaboration with the Met Office, with users needing to register for this new alerting system.

The UK Health Security Agency has launched the Adverse Weather and Health Plan (AWHP) as part of a commitment under the National Adaptation Plan to bring together and improve existing guidance on weather and health. The AWHP brings together the previous Heatwave Plan for England, first published in 2004, and the Cold Weather Plan for England.

The plan builds on existing measures taken by the government, its agencies, NHS England and local authorities to protect individuals from the health effects of adverse weather and build community resilience.

Recovery

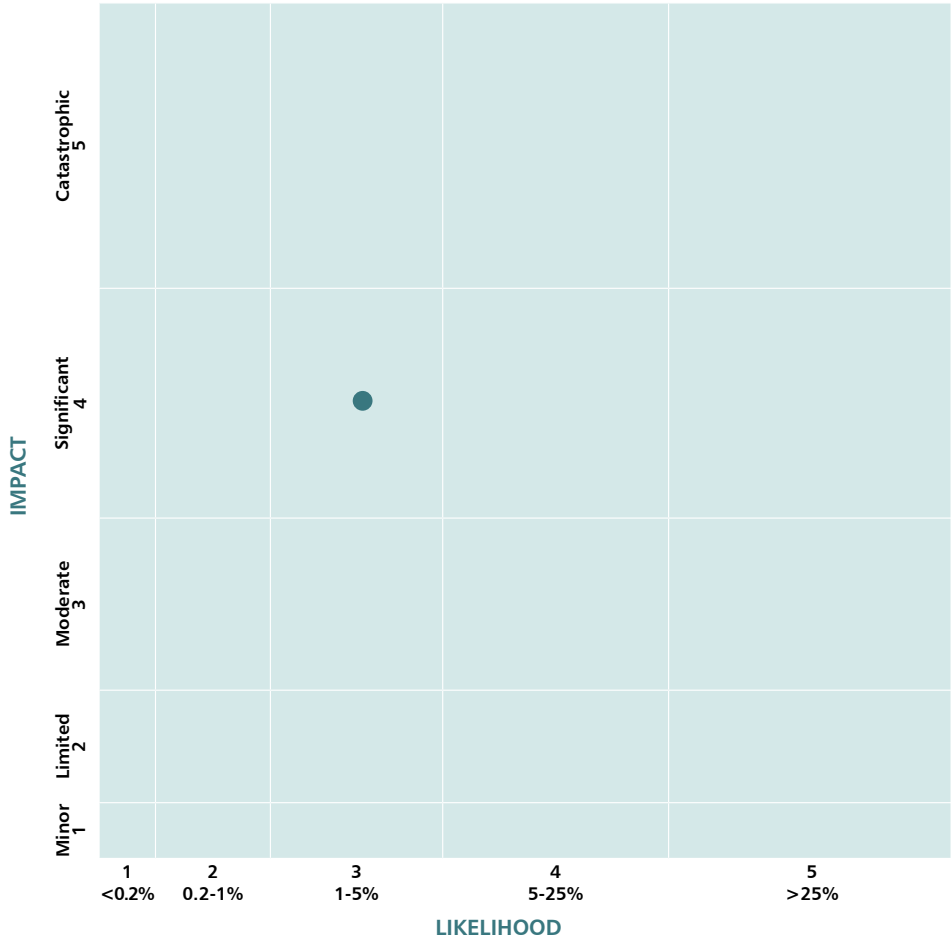
Longer-term impacts from low temperatures and heavy snow are not anticipated. Where low temperatures and snow lead to secondary impacts such as an increase in the likelihood of utility system failures or flooding due to snowmelt, recovery due to these secondary impacts may take longer.

Coastal flooding

Coastal flooding is caused by high tides, low pressure weather systems, and surge conditions caused by strong winds blowing large waves towards the shore. As sea levels continue to rise as a result of climate change, the risk of coastal flooding will also increase. Flooding events have serious consequences on coastal communities, including disruption to essential services, the economy and environment, with disproportionate effects on vulnerable groups. The government has well-established arrangements for minimising the risk from flooding including, the deployment of fixed and temporary defences, public warning and informing alert systems, and local and national response mechanisms.

Scenario

The reasonable worst-case scenario is based on coastal flooding across the east coast of England, impacting a very large number of residential properties. Comprehensive warning and informing systems would be employed and a large number of people would require evacuation and shelter, with a significant proportion of these requiring assistance. The number of people affected could be even greater during the holiday season. There would be fatalities and casualties, including those whose death, illness, or injury are an indirect consequence of flooding. Large areas of road and railway could be flooded, with other major infrastructure such as schools, hospitals, care homes, emergency services and agricultural land also affected.



Key assumptions for this scenario

A key assumption for this scenario is that the existing high levels of preparedness for local planning and response continue to operate. The Environment Agency (EA) and others continue investing in new coastal defences and maintaining existing coastal defences. There would be between 5-7 days of flood forecasts showing medium and then high risk of coastal flooding from the Flood Forecasting Centre (FFC). Severe Flood Warnings would be issued a minimum of 24 hours in advance by the EA.

Variations of this scenario

Coastal flooding is highly variable and dependent on where the flooding occurs. Certain areas are more vulnerable to flooding, and the impact there would be higher. Higher risk areas also have greater protections via barriers and advanced warning systems.

Response capability requirements

An advanced flood forecasting capability is available via the Met Office and the FFC. The FFC produces products that identify potential flood impacts from weather scenarios. These products help inform long-term emergency planning and in the lead up to a potential flooding event. The FFC target is to consistently provide at least a 3-day lead time for coastal events.

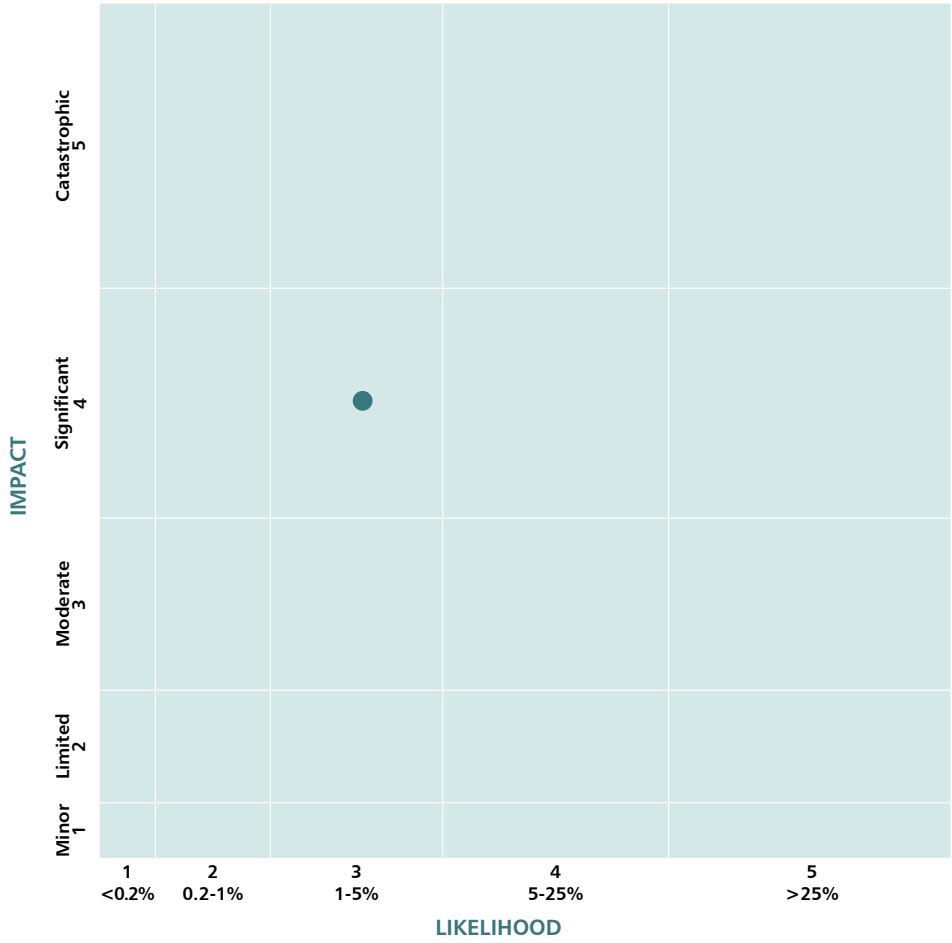
The EA leads operational preparedness and response to flood impacts and, during local-level operation response, would work as part of a multi-agency team, coordinated through the LRF to support flood preparedness, warning and informing the public, operating defences and systems and coordinating any evacuation including accommodation requirements. The local response will have access to operational resources including temporary flood barriers, mobile pumps and the necessary logistical support to transport and deploy these resources. Flood rescue teams (which consist of over 100 specialist flood rescue teams on standby to be deployed across the country), national mutual aid and military assistance can also support a local response. Any national coordination would be led by the EA and the Department of Environment, Food and Rural Affairs.

Recovery

A major recovery operation is required involving economic, environmental, infrastructure and humanitarian impacts. The recovery process would likely last beyond 2 years, especially if significant repairs are required to infrastructure, homes and businesses. Mental and physical impacts on affected citizens may also be longer-term.

Fluvial flooding

Fluvial flooding occurs when waterways such as rivers, streams or brooks overflow their banks into surrounding areas. This risk is most likely to occur following periods of intense rainfall and will become more frequent as a result of climate change. Impacts are widespread and may include damage to the local environment, properties and essential services, with disproportionate effects on vulnerable groups. The government has well-established arrangements for minimising the risk from flooding including, the deployment of fixed and temporary defences, public warning and informing alert systems, and local and national response mechanisms.



Scenario

The reasonable worst-case scenario is based on a significant river flood event, resulting from cumulative local events or a series of concurrent events across multiple geographic regions following a sustained period of heavy rainfall. This could possibly be combined with snow melt and surface water flooding. Flood defences would become overtopped by river levels and breaches may occur in river banks and hard defences as they are put under pressure. Across urban and rural areas there would be flooding of homes and businesses. There will be casualties and fatalities. A large number of people would require evacuation, with a significant proportion of these being vulnerable and requiring assistance. There would be medium-term (days to weeks) loss of essential services (electricity and telecoms) to up to a substantial number of homes and businesses, with disruption to water supplies.

Key assumptions for this scenario

The scenario assumes the event would occur at night time after an extended period of rainfall lasting 2 weeks in a large urban area. There would be a loss of essential services to homes and businesses possibly lasting several weeks.

Variations of this scenario

A lower-impact scenario could involve fewer breaches and an overtopping of flood defences, with more localised areas impacted. A higher-impact scenario would involve the additional risk of severe surface water flooding over already-saturated catchment areas.

Response capability requirements

An advanced flood forecasting capability is available via the Met Office and the Flood Forecasting Centre (FFC). The FFC produces products that identify potential flood impacts from weather scenarios. These products help inform long-term emergency planning and in the lead up to a potential flooding event. The FFC target is to consistently provide at least a 3-day lead time for fluvial events.

The Environment Agency (EA) leads operational preparedness and response to flood impacts and, during local-level operation response, would work as part of a multi-agency team, coordinated through the Local Resilience Forum (LRF) to support flood preparedness, warning and informing the public, operating defences and systems and coordinating any evacuation including accommodation requirements. The local response will have access to operational resources including temporary flood barriers, mobile pumps and the necessary logistical support to transport and deploy these resources. Flood rescue teams (which consist of over 100 specialist flood rescue teams on standby to be deployed across the country), national mutual aid and military assistance can also support a local response. Any England-wide coordination would be led by the EA and the Department for Environment, Food and Rural Affairs.

Recovery

Major recovery impacts and long-term economic, environmental, infrastructure and humanitarian implications would go beyond 2 years especially if significant repairs are required to infrastructure, homes and business. Mental and physical impacts on affected citizens will last for years. Businesses would experience significant impacts, and the long-term contamination of agricultural and other land would also be likely.

Surface water flooding

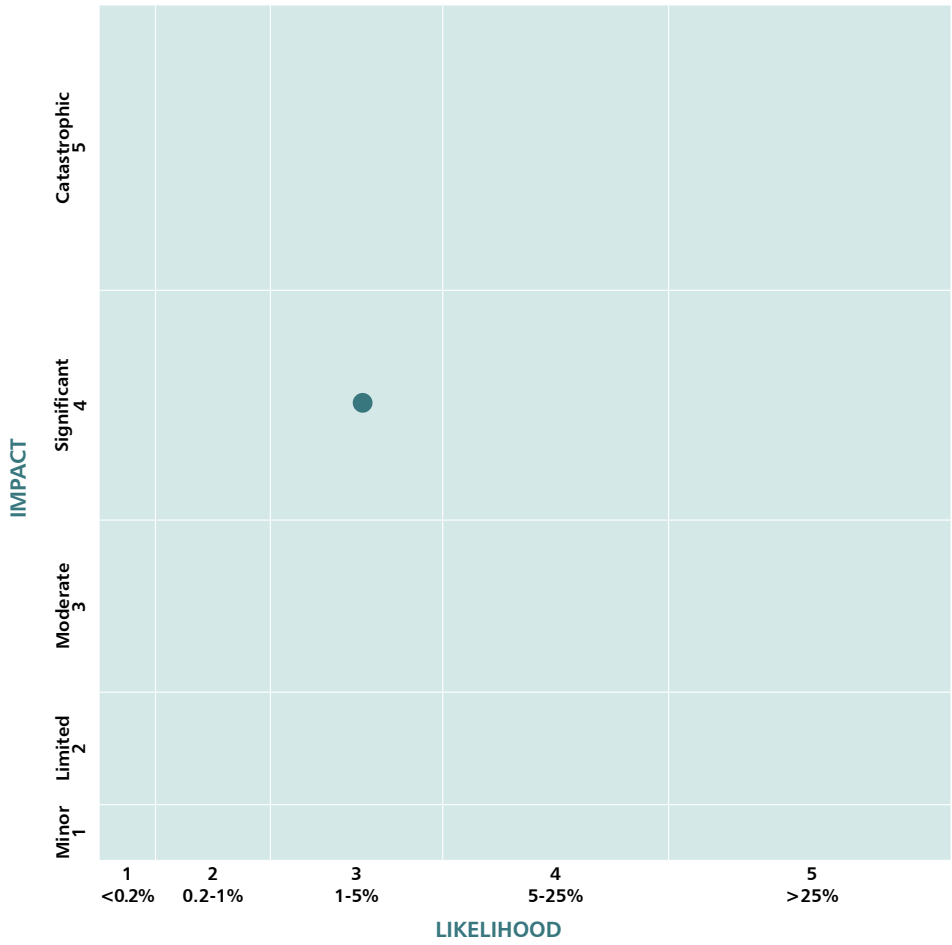
Surface water flooding occurs when rainfall overwhelms the capacity of drainage systems and surface water sewers, resulting in water flowing over the land instead of through drainage systems. This type of flooding can occur in a wide variety of locations, including towns or cities located far from the sea or rivers. It is also particularly difficult to forecast with accuracy and can happen at very short notice, with periods of short but intense rainfall likely to increase in the future due to the warming climate.

Scenario

The reasonable worst-case scenario is based on a large flood event in a metropolitan area, resulting from a pocket of exceptionally high rainfall in the south east. The most severe impacts in any metropolitan area would lead to significant damage to homes and businesses. The evacuation of residents would be necessary, with short- to medium-term shelter being required. Depending upon the geological conditions, surface water flooding may lead to an increased likelihood of geological instability (for example sinkholes or landslides) in the impacted area. This could cause significant impacts to the local response, transport infrastructure, and other infrastructure in the impacted area.

Key assumptions for this scenario

Areas most at risk would not be warned until 6-24 hours before the event and the exact location of the most intense rainfall would not be known in advance due to the unpredictability of where and when heavy thunderstorms will occur.



Variations of this scenario

A high impact but less likely variation could involve surface water flooding in an urban area exacerbated by coastal or fluvial flooding. There would also be greater disruption from surface water flooding in areas with dense populations, with poor drainage creating greater levels of property damage and displacement of possibly thousands of people.

Response capability requirements

Lead Local Flood Authorities have responsibility for managing surface water flood risks, including assessing the risks, implementing a local flood risk management strategy and working in partnership with other involved agencies. The Department for Levelling Up, Housing and Communities has well-established multi-Local Resilience Forums mutual aid arrangements in place to support flood preparedness and a coordinated national response. Pre-prepared national resources are available, including sandbags, mobile flood barriers and mobile pumps, ready to be moved where needed.

Recovery

There would be extensive damage to homes and businesses as people would be unprepared due to the lack of surface water specific warning systems. Surface water flooding would have major recovery impacts and long-term economic, environmental, infrastructure and humanitarian implications.

Drought

A drought may occur following a period of abnormally low rainfall, which results in a shortage of water. The future risk of droughts due to climate change is increasing, and there is a trend towards hotter summers with associated high water demand. Simultaneously, changes in consumer habits and population growth is increasing water use in the UK.

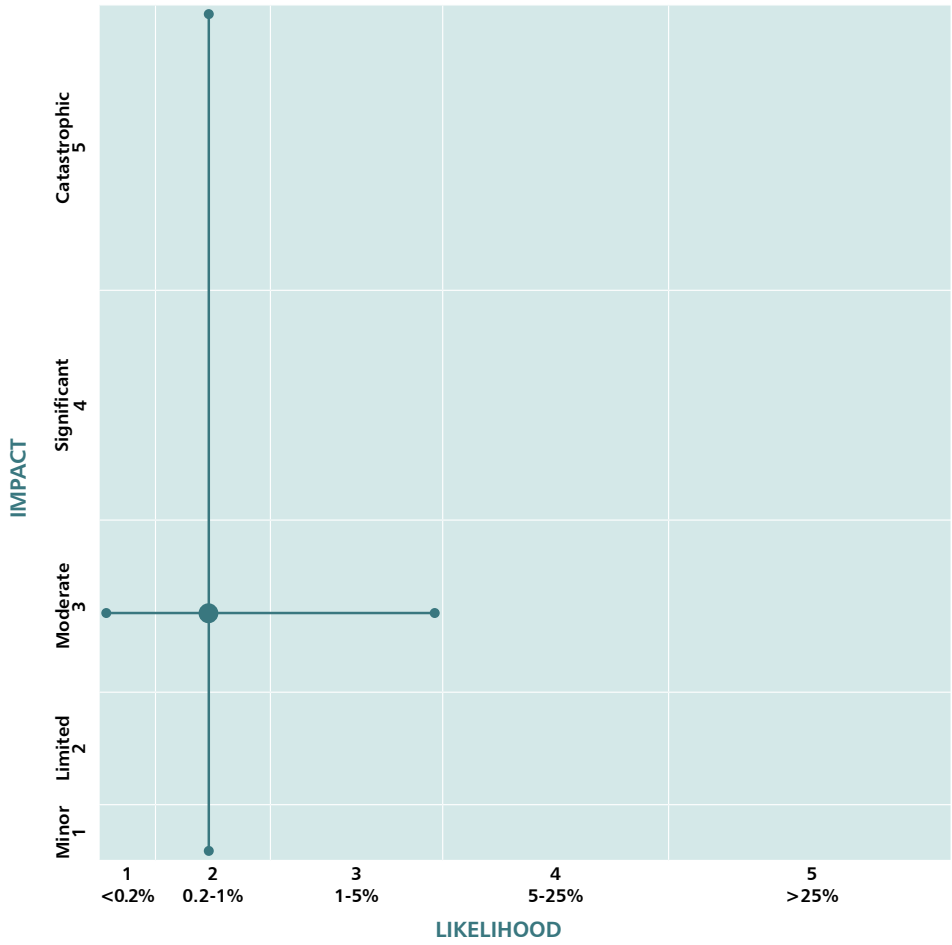
Drought impacts can be reduced through water efficiency campaigns and amplified via national messaging to encourage the public to reduce water demand. Interventions to support farmers are available, ranging from the protection of water rights to providing funding research and development on water management.

Scenario

The reasonable worst-case scenario is based on large parts of South and East England facing severe drought conditions after 3 consecutive dry winters. Neighbouring areas of the Midlands and South West would face drought-related impacts and there would need to be public water supply restrictions. There would be significant losses to the UK economy, with serious impacts on industry, agriculture and businesses. Severe environmental damage due to drought conditions would occur, along with an increased fire risk due to dry conditions. This would be combined with a reduced ability to fight fires due to water scarcity.

Key assumptions for this scenario

Three consecutive dry years would be required in order for a severe or emergency drought to occur. This would allow for preparations to begin ahead of time and for mitigations to be put in place.



Variations of this scenario

There are likely to be significant regional variations. A drought may end sooner than expected if a wetter period of weather occurs.

Response capability requirements

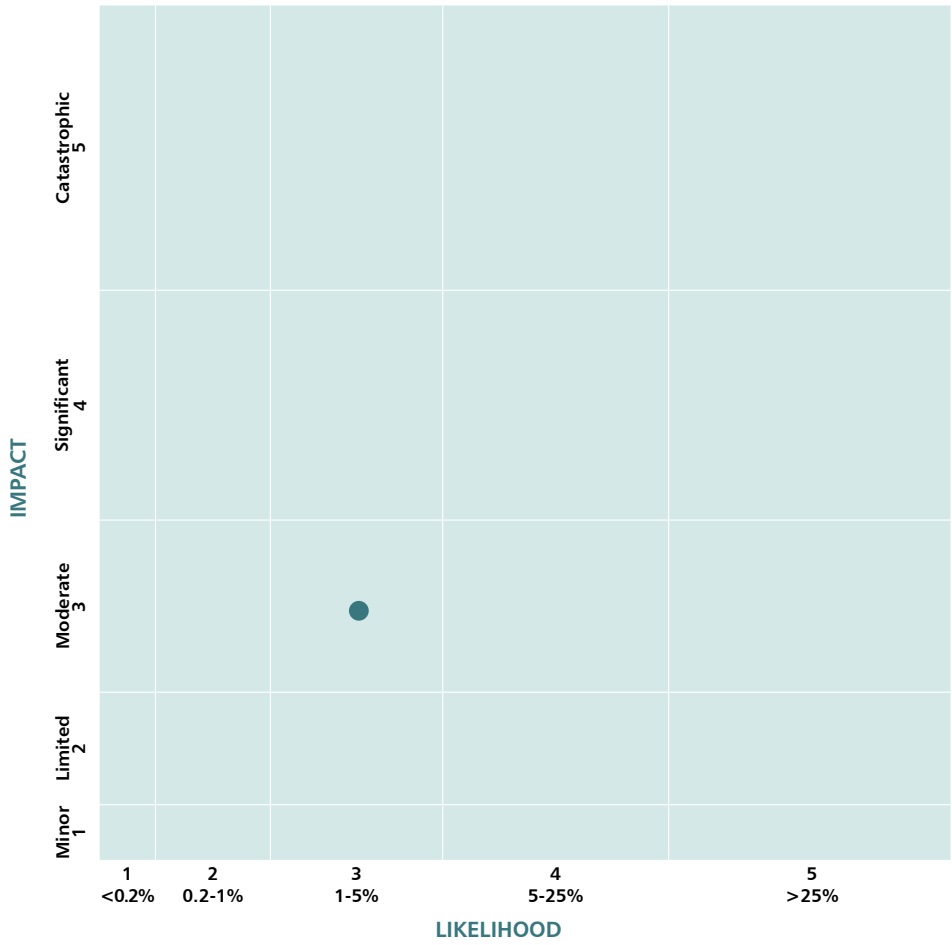
The Environment Agency (EA) and water companies have comprehensive systems in place to monitor rainfall and water resources. National coordination plans are in place through the EA and the Department for Environment, Food and Rural Affairs. This is overseen by the National Drought Group. A range of regulatory restrictions, including limiting the amount of water that farmers and businesses are allowed to abstract from rivers, and consumer communication campaigns to encourage reducing water consumption can help to make water supplies last as long as possible. Water companies may also consider Temporary Usage Bans to manage water resources.

Recovery

How quickly rainfall reaches normal levels, and the depth of impacts that have occurred during the drought, would impact the speed of recovery. Most businesses would recover as soon as normal water supply is resumed, though heavily water-reliant businesses may take several months or years to recover. A severe drought of the type modelled in this scenario would pose particularly difficult challenges for the recovery of the natural environment.

Poor air quality

Air quality has improved significantly over recent decades. However, air pollution remains the largest environmental risk to UK public health and is linked with reduced lifespans. Short-term surges in poor air quality occur primarily due to weather conditions preventing pollution from dispersing. These conditions include low winds or temperature inversion. Air quality is also worsened by the ultraviolet light from sunshine, as it reacts with the air to generate ozone. The government set out commitments to tackle all sources of air pollution and improve air quality for all through the Clean Air Strategy. The Environmental Improvement Plan sets out the actions that will support us to continue improving air quality and to meet our new interim and long-term targets for PM2.5 set under the Environment Act 2021. In addition, the UK Government has published a revised air quality plan for tackling nitrogen dioxide (NO2) emissions in urban areas.



Scenario

The reasonable worst-case scenario is based on a 30-day period of elevated ground level ozone or fine particulate matter. During a poor air quality event of this kind, the UK could experience significant health risks, including an increase in deaths from exacerbation of respiratory or cardiovascular conditions, with an associated increase in hospital referrals and pressure on emergency response services. The duration of an air quality episode would be heavily influenced by meteorological conditions. High ground-level ozone episodes in the UK occur most commonly in the summer months when high pressure weather systems dominate. Elevated ground-level ozone can also occur during springtime. At a national scale elevated fine particulate matter concentrations are most common in the spring. In urban centres however, high particulate matter events can occur at almost any time of year if emissions from road transport and domestic sources are released in certain weather conditions.

These episodes may be worsened when already polluted air from continental Europe is drawn over the UK. Fine particulate pollution events may also arise from other natural phenomena including the wind suspension of soil dust following drought, from long-range transport (for example Saharan dust), and from uncontrolled biomass combustion from wildfires.

Key assumptions for this scenario

The main assumption is that the air pollution event would last for up to 30 days, with elevated ozone and/or particulate matter.

Variations of this scenario

A less impactful but more likely variation involves a shorter 22-day air pollution event, although this would require the same response capabilities.

Response capability requirements

Communications networks to provide advice to those in affected areas (ensuring messaging reaches those who are most vulnerable, such as older adults) would be required. Access to healthcare professionals, including GPs to help individuals with less severe symptoms, and emergency services and hospitals to assist those with more severe symptoms would also be essential.

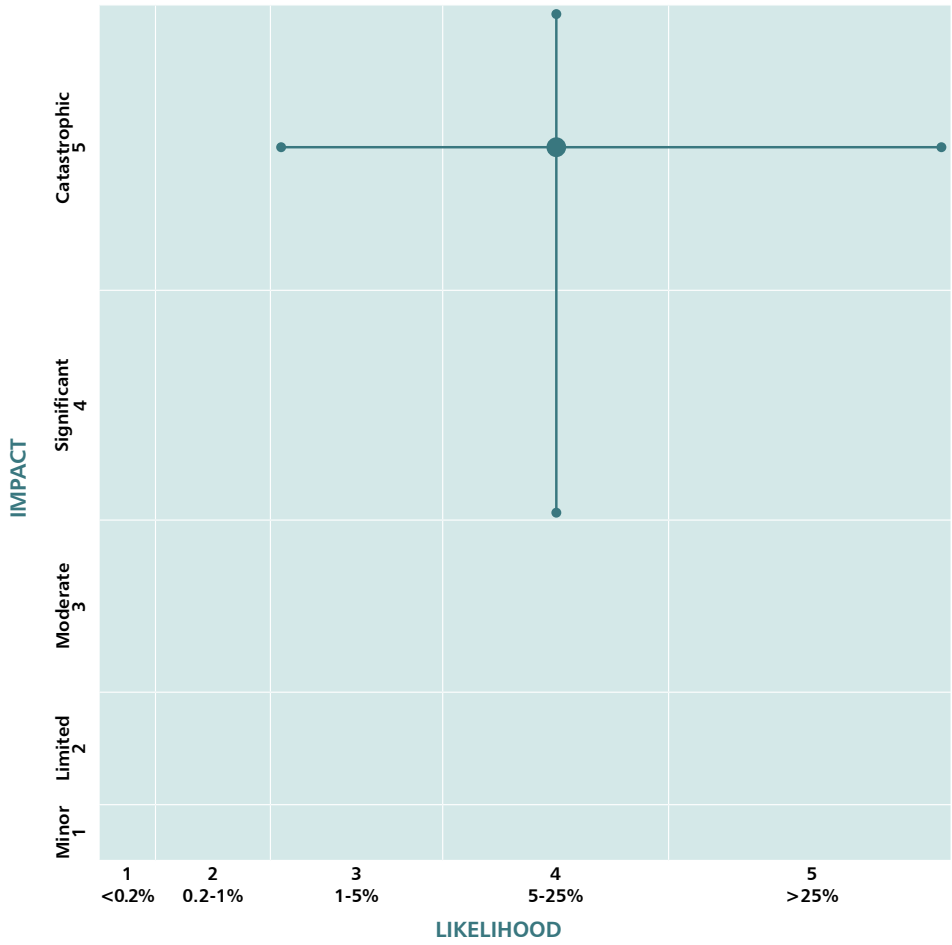
Recovery

Poor air quality is known to have long-term health impacts, such as cardiovascular and respiratory conditions. Based on current evidence however, it is not possible to distinguish the relative contributions from air quality episodes and longer-term exposure to lower levels of air pollutants.

Human, animal and plant health

Pandemic

Pandemics are usually the result of a novel pathogen (virus, bacteria, fungi or other organisms that cause disease) emerging and spreading quickly around the world due to lack of population immunity. Once the pathogen emerges it is crucial to gain a rapid understanding of the spread, transmission, symptoms, severity, immunity, treatments and healthcare pathways. Experts consider a respiratory pathogen to be the most likely cause of a future pandemic affecting the UK based on the emergence of pandemics since 1900 and, as such, assumptions based upon a respiratory disease underpin the reasonable worst-case scenario for government pandemic preparedness planning. However, the government continues to plan and prepare for a range of pandemic and emerging infectious disease scenarios, across the five different transmission routes: respiratory, blood and sexual, touch, oral (food and water) and by vectors such as mosquitos. This approach covers known or unknown pathogens (referred to as "Disease X" by the World Health Organisation). The UK has flexible pandemic response capabilities that are built on lessons learned from exercises and incidents, including the COVID-19 pandemic.



Scenario

The reasonable worst-case scenario is based on an unmitigated respiratory pandemic with an unassumed transmission route and a high attack rate, with 4% of symptomatic infections requiring hospital care and a case fatality ratio of 2.5%. From start to finish the emergency stage of the pandemic in the UK will last at least 9 months and potentially significantly longer. Response mechanisms are likely to be required beyond 9 months to manage the chronic stage of the risk and longer-term recovery. The pandemic may come in single or multiple waves. The wave number depends on the characteristics of the disease, public behaviour, and government intervention. The pandemic may lead to behaviour changes in the population depending on the nature of the

disease and the government's response. The scenario assumes 50% of the UK's population fall ill during the whole course of the pandemic, with about 1.34 million people estimated to require hospital treatment, possibly resulting in up to 840,000 deaths.

Key assumptions for this scenario

Each pandemic is unique and will be impossible to predict when it will occur. Impacts on society depend on many different factors – transmission route, the time of year it emerges, severity of disease, global travel, who gets ill or dies and where it happens. For the purposes of the assessment, the scenario is an unmitigated pandemic that does not make any assumptions about behaviour change or government interventions being successful at reducing transmission.

Variations

Variations of the reasonable worst-case scenario for the pandemic risk, which is based on an influenza-like illness, are based on different pathogens, some of which have different routes of transmission. These include a possible novel enterovirus pandemic (these viruses are usually mild, but if they infect the central nervous system, they can cause serious illness); a novel coronavirus pandemic; and, a novel sexually transmitted infection pandemic.

Response capability requirements

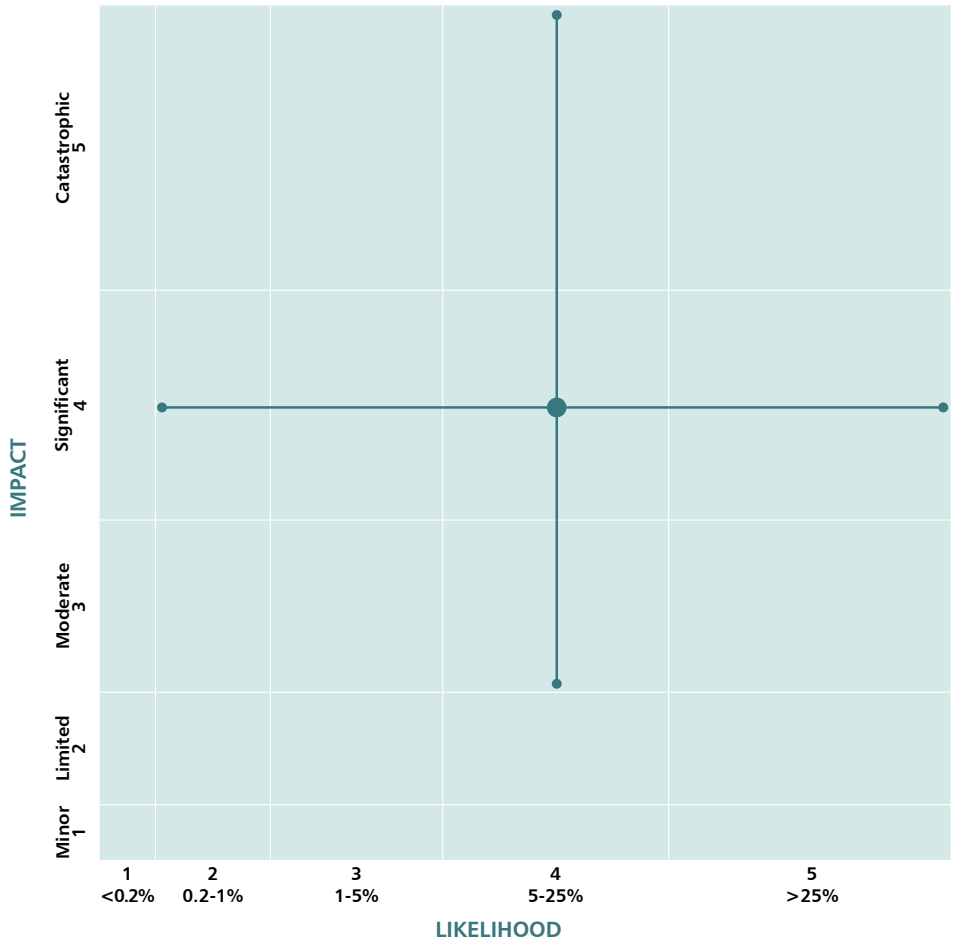
Disease surveillance and early detection, including timely and reliable data, is needed. There should be procedures to support the identification and isolation of suspected cases and scalable contact tracing, scalable diagnostics (both lab and rapid testing), as well as rapid development and procurement of pharmaceutical countermeasures with stockpiled countermeasures, including personal protective equipment, for known pandemic threats. Effective non-pharmaceutical interventions, including border measures, should also be considered as part of the response. Local and national plans for managing excess deaths should be present, and arrangements for effective UK and global coordination. Plans for social, educational, and economic impacts of the pandemic and expert scientific and clinical advice should also be in place. Our response capability would need to be able to channel significant research and development resource to genomics and development of tests, vaccines and therapeutics. A national communications plan would also be needed to increase awareness and encourage good hygiene. Every sector, including but not limited to health and social care, will be affected by the pandemic and will require capabilities to respond.

Recovery

It may take years for recovery to the health and social care sector (due to increased pressure on services throughout the pandemic) and impacts on society, education and the economy may last several years. Recovery from one wave of the pandemic may be hampered by the arrival of a subsequent wave of the same pandemic.

Outbreak of an emerging infectious disease

Emerging infectious diseases include new or newly recognised diseases and could result in large numbers of people falling ill. Some recently emerged diseases, such as Ebola and Middle East Respiratory Syndrome, are classified as High Consequence Infectious Diseases. These are acute infectious diseases that typically have a high case fatality rate and may or may not have effective prophylaxis or treatment and can be difficult to recognise or diagnose rapidly. They require an enhanced individual, population and system response to ensure management is effective, efficient and safe. The UK Health Security Agency and NHS responders have well-tested response capabilities to detect, contain and treat novel infectious diseases.



Scenario

The reasonable worst-case scenario is based on a novel respiratory-transmitted virus that emerges zoonotically (from animals to humans) in another country and causes a regional epidemic. This covers diverse virus families, which may acquire some degree of human-to-human transmission, such as influenza viruses, coronaviruses and nipah viruses. However, we must be prepared for a disease spread via any of the 5 main routes of transmission: respiratory, blood (including sexual contact), close contact oral (food and water) and by vectors such as mosquitos. There would be a small number of cases imported into the UK before border measures are applied, which could result in an outbreak of up to 2,000 cases with a case fatality rate of up to 25%. A significant number of contacts, up to 200,000, would need to be traced, isolated or monitored depending on exposure.

Non-pharmaceutical interventions, rapid isolation and contact tracing activities would need to follow on from the initial border measures, with limited virus transmissibility bringing the outbreak under control. Failure to contain the outbreak would result in a large epidemic in the UK, or a pandemic.

Key assumptions for this scenario

It is assumed that the novel pathogen causing the epidemic would emerge abroad, with no effective treatment or vaccine. It is assumed that the pathogen would be previously unknown or not normally found within the UK, resulting in a significant outbreak. Infections would be transmitted by the respiratory route, there would be limited human-to-human transmissibility and the outbreak is contained regionally. The outbreak would last between 2 to 6 months. Infected individuals would show identifiable and visible symptoms at the same time as, or preceding, the risk of transmission.

Variations

There are a range of different transmission routes and disease severities, which are reflected in the variations of a viral haemorrhagic fever, vector-borne disease and zoonotic infection.

Response capability requirements

The capability response would be focused on containment (stopping further transmission and reducing cases to zero). This would include the quick implementation of appropriate border measures, with a focus on scalable isolation capabilities, disease surveillance and early detection.

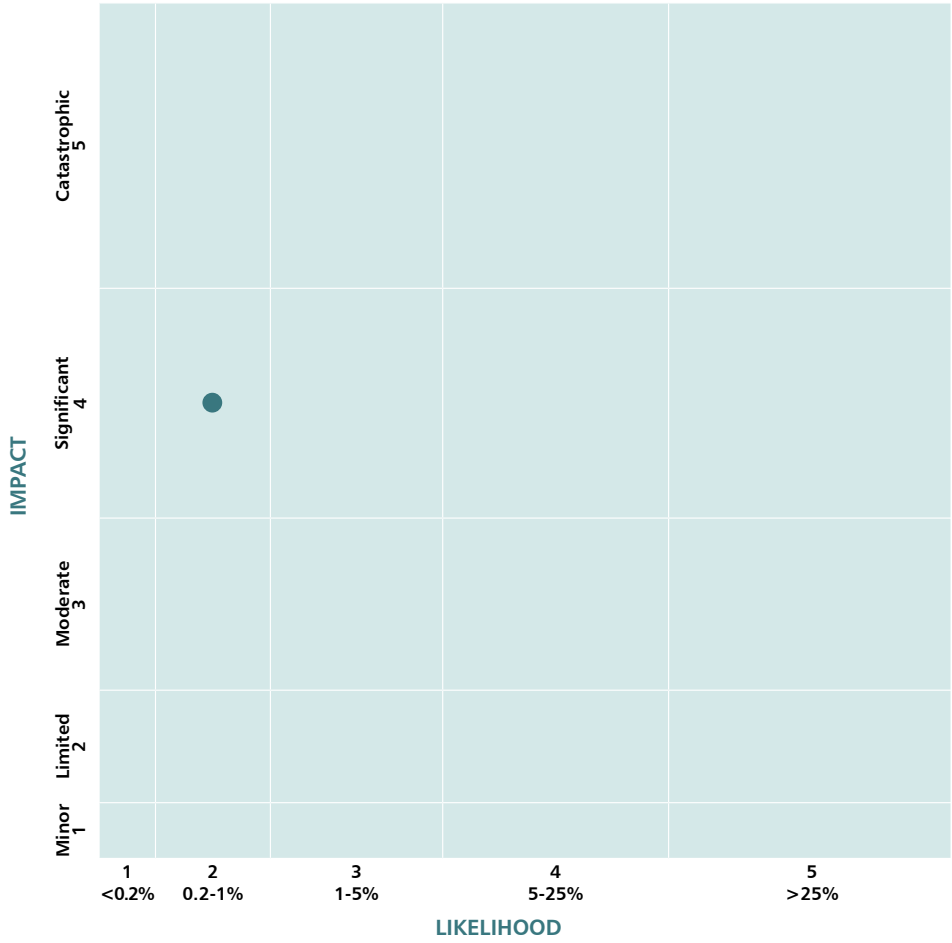
There would be a need for personal protective equipment supplies, scalable diagnostics (both lab and rapid testing) and decontamination services in place to prevent cases from rising. A national communications plan would also be needed to increase awareness and encourage good hygiene. Our response capability would need to be able to channel significant research and development resource to developing tests, vaccines and therapeutics.

Recovery

Long-term impacts would not be understood until several months or up to years later, with possible long-term consequences on the health and social care system.

Animal disease: major outbreak of foot and mouth disease

Foot and mouth disease (FMD) is a severe, highly infectious viral disease with significant economic impact, affecting several types of animal including cattle, pigs, sheep, deer and goats. This is spread easily, for example through direct contact with infected animals, with secretions of infected animals, with products of infected animals (meat, milk, hair), clothing, contact with contaminated equipment, vehicles and feed. The last major FMD outbreak in the UK was observed in 2001, which resulted in the culling of over 6 million animals. FMD is a notifiable disease throughout the UK and anyone who suspects disease must immediately report it. The Animal and Plant Health Agency monitors FMD outbreaks internationally and publishes outbreak assessments considering the risk posed to UK livestock on GOV.UK.



Scenario

The reasonable worst-case scenario assumes that FMD is introduced into a sheep-farming area. Infected animals that are not yet exhibiting clinical signs would be sold or moved to other premises before the disease is detected, resulting in multiple geographically dispersed outbreaks. The culling and disposal of approximately 1.9 million animals on over 2,900 premises could be required. This scenario is of much greater scale than the most recent FMD outbreak in 2007, but less than the 2001 outbreak due to improvements to livestock movement regimes and control policies.

Key assumptions for this scenario

There is a constant but low risk of an incursion of an exotic notifiable animal disease into the UK. The risk likelihood will vary throughout the year depending on season and disease status and trade status of other countries.

Variations of this scenario

If this scenario were to occur concurrently with another emergency, the scale, impact and duration of the outbreak is likely to increase.

Response capability requirements

Specialist staff would be required to conduct surveillance and dispose of infected animals. These include vets, animal technicians, licensed slaughterers and carcass disposal logistics experts, in addition to sufficient carcass transport, rendering and incineration capacity. Sufficient laboratory capacity to undertake surveillance in all susceptible livestock would also be needed, along with, disease-modelling experts, epidemiologists, wildlife experts, administrators and trained policy staff. Local authority staff would be required to conduct enforcement activities, which at the outset and peak of the outbreak could be on a national scale. Sufficient approved personal protective equipment (PPE), respiratory protective equipment (RPE) and approved disinfectant would be necessary across government and operational partners. If a vaccination policy is introduced, stocks of vaccines, capacity to roll out vaccination and additional surveillance would be needed.

Recovery

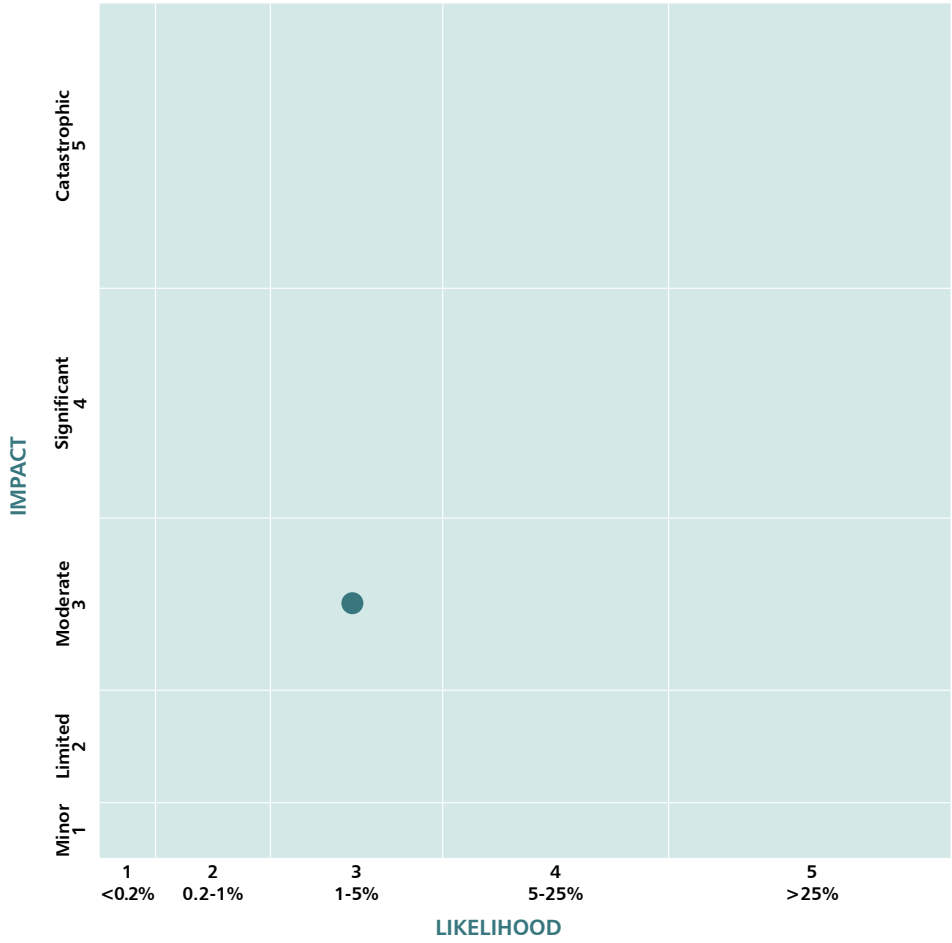
For foot and mouth disease, the minimum period to regain country-free status for international trade is 3 months from the date of culling and preliminary culling and disposal of the last FMD-infected premises. If vaccination is used, exports can resume no sooner than 3 months after the last vaccinated animal has been culled, or 6 months after the date of last vaccination if a vaccinate-to-live policy is adopted. There would also be long-term impacts on the environment (particularly around burial sites), livestock sector, and rural economy.

Animal disease: major outbreak of highly pathogenic avian influenza

Highly pathogenic avian influenza (HPAI) is a severe, highly infectious influenza causing significant morbidity and mortality in susceptible avian species. Avian influenza is primarily a disease of birds, but can be transmissible to humans through prolonged, direct contact with infected birds or contaminated material. All strains of HPAI are legally notifiable if suspected in the UK, with the biggest outbreak to date being recorded over 2021 to 2023. HPAI is a notifiable disease throughout the UK and anyone who suspects disease in poultry or captive birds must immediately report it. The Animal Plant and Health Agency (APHA) monitors HPAI outbreaks internationally and publishes outbreak assessments considering the risk posed to the UK livestock on GOV.UK.

Scenario

The reasonable worst-case scenario is based on an outbreak of a highly virulent strain of HPAI that is unlikely to transmit easily to humans. Disease would be introduced into multiple large-scale poultry businesses, through direct or indirect contact with wild birds. Viral spread from both wild birds and between infected premises occurs, leading to an outbreak of 250 large commercial premises in a 6- to 8-month period. About 8 million poultry and captive birds would either be killed by the virus or culled for disease control, and there would be restrictions on trade and exports. Multiple mass-die-off events in wild-bird populations are likely.



Key assumptions for this scenario

For a strain of HPAI readily transmissible to humans, the public health impact would be handled by the Department for Health and Social Care (DHSC). However, occasional spill-over to humans cannot be ruled out and therefore the local health protection teams would be involved in following up human contacts with each new infected establishment.

Variations of this scenario

A strain of HPAI with greater transmissibility to humans could increase the impact of the outbreak affecting poultry workers, slaughterhouse workers, APHA and contract staff dealing with the outbreaks, as well as those with close contact to wild birds. Disease control measures would need to be adapted to manage the public health risks, with further measures to protect food safety and essential services. The public health impact would be handled by DHSC.

Response capability requirements

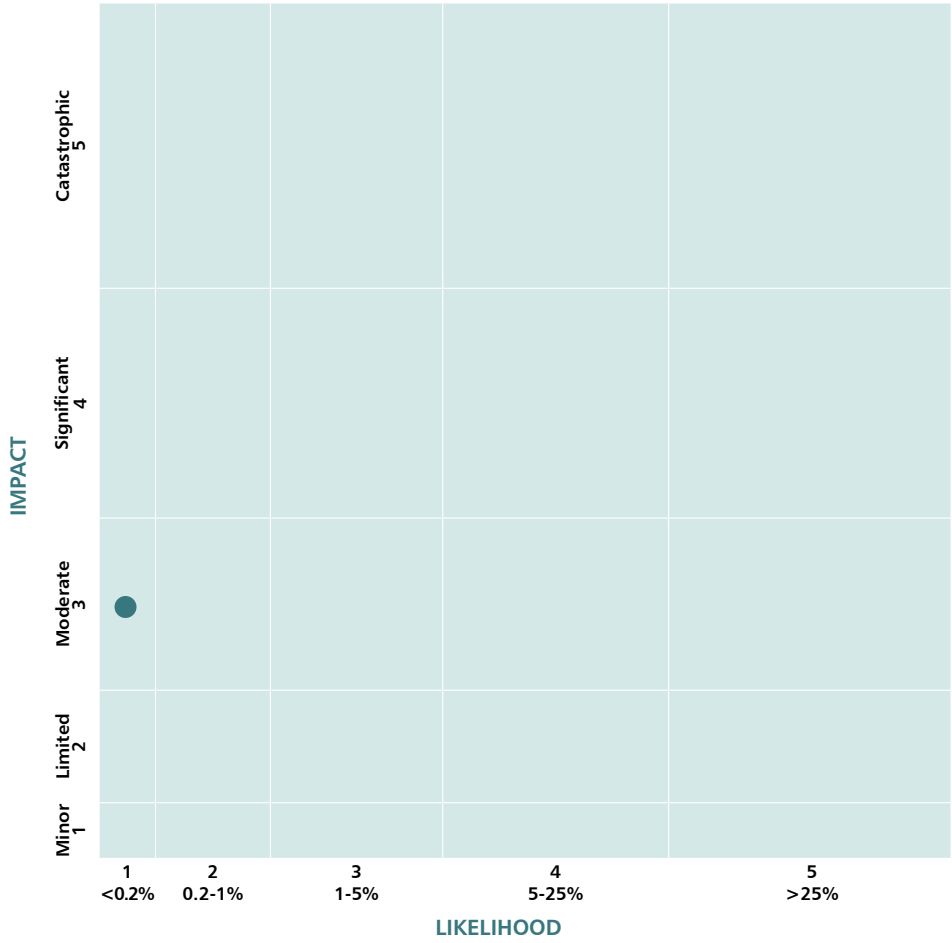
Specialist staff including vets, poultry catchers and staff to complete culling, disposal and cleansing and disinfection would be required, along with sufficient transport capacity and access to rendering or incineration. In addition, sufficient laboratory capacity is needed for diagnostic and monitoring purposes; local authority staff to conduct enforcement activities; and modelling experts, epidemiologists, disease experts, wildlife experts, administrators and trained policy staff to support would be needed. Sufficient personal protective equipment (PPE), respiratory protective equipment (RPE) and approved disinfectant would also be necessary across government and operational partners.

Recovery

The minimum period to regain regional disease-free status for international trade is a minimum of 28 days from completion of secondary culling and disposal at the last infected premises. Exports to the EU can resume following the completion of enhanced surveillance in the restricted region, usually no less than 30 days after effective culling and disposal of all infected premises in the region. Third-country exports will depend on the relevant bilateral trade agreements. Given the size and duration of this scenario, there would be long-term impacts on trade, the environment, poultry sector, and rural economy.

Animal disease: major outbreak of African horse sickness

African horse sickness (AHS) is a vector-borne animal disease that is spread by midges and affects horses, donkeys, zebras and mules. It does not affect humans but can be fatal in 90% of the horses, donkeys and mules that it infects. There have been no cases of AHS in the UK to date, with the majority of outbreaks occurring in Sub-Saharan Africa where the zebra acts as a reservoir. However, cases have also been detected in countries such as Spain, Portugal, Thailand, India and Pakistan. AHS is a notifiable disease throughout the UK and anyone who suspects disease must immediately report it.
The Animal and Plant Health Agency monitors AHS outbreaks internationally and publishes outbreak assessments considering the risk posed to the UK animals on GOV.UK. The UK's strict trade rules are the most important risk mitigation measure.



Scenario

The reasonable worst-case scenario assumes that an AHS infected horse is imported into the UK and bitten by midges, which would carry the virus to other horses. Although the infected horse will probably die within a few days it would not be necessarily suspected by the owner and samples may not be submitted to the reference laboratory at The Pirbright Institute. By the time the virus is identified, it would be well established in geographically dispersed midge populations around the UK. Control measures include movement restrictions, culling of infected horses and may include preventive vaccination. The restriction zones for AHS are very large, up to 150km radius, because of the movement of infected midges. The outbreak would last for a minimum of 6 months (depending on the season and the presence of midges) and result in long-lasting trade restrictions, affecting the international movement of equine animals and a range of very high-value commodities. The likelihood and impacts of an outbreak of AHS continue to be assessed.

Key assumptions for this scenario

It is assumed that a horse infected with a low- to medium-pathogenicity strain of AHS is imported into England in early spring (April) and is bitten by midges at the beginning of the midge season. The disease would replicate undetected in midge populations and spread to equine animals. Sporadic illness and deaths in infected horses may not be attributed to AHS for the first few weeks, allowing for a period of undetected spread as horses are moved around the country, facilitating a wider geographic dispersal of the disease.

Variations of this scenario

If the outbreak occurred at a time of increased global demand for AHS vaccine, the control strategy may be reliant on vector controls for midges and an increase in culling until vaccines become available.

Response capability requirements

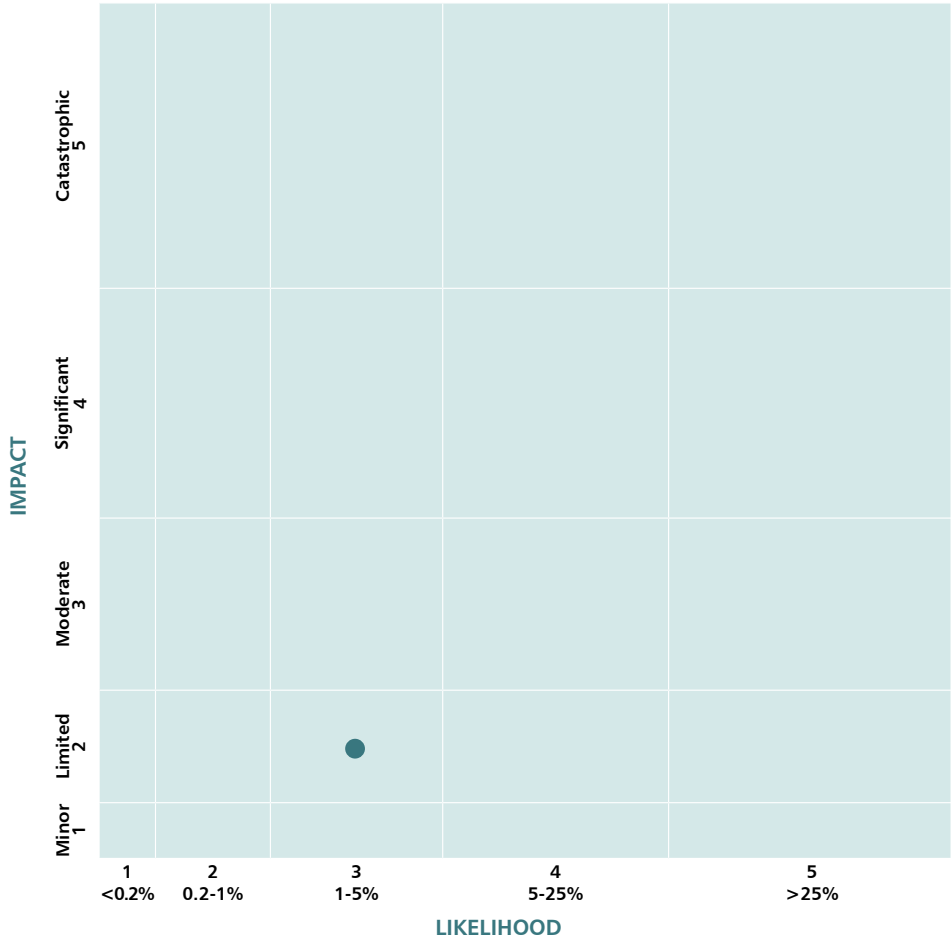
Specialist staff including equine vets (who may be private vets), animal technicians, licensed slaughterers, and carcass disposal personnel would be required to conduct surveillance and dispose of infected animals. In addition: sufficient laboratory capacity to monitor the situation, local authority staff to conduct enforcement activities, modelling experts, epidemiologists, wildlife experts, entomologists, administrative staff and trained policy staff to support, would be needed. Some parts of the horse-owning sector are difficult to reach and additional specialists may be needed. Sufficient approved personal protective equipment (PPE) and approved disinfectant would be necessary across government and operational partners.

Recovery

The minimum period to regain country-free status for international trade is 2 years from the last confirmed outbreak. Any trade permitted to continue would be subject to rigorous health certification and restrictions. During the outbreak, movement restrictions would have a devastating impact on the horse racing and breeding sector, and rare populations of wild ponies could be severely impacted. The rural economy would also suffer heavy losses.

Animal disease: major outbreak of African swine fever

African swine fever (ASF) is a highly contagious haemorrhagic viral disease that affects pigs and wild boar but does not infect humans. It can be spread by direct contact with infected live or dead pigs, their secretions, pork products, contaminated feed, and non-living objects such as shoes, clothes and vehicles. The only control options are culling and movement restrictions; there is no vaccine or antiviral therapy available. Although no cases of ASF have been reported in the UK, the virus is currently spreading in Europe, Asia and Africa. ASF is a notifiable disease throughout the UK and anyone who suspects disease must immediately report it. The Animal and Plant Health Agency monitors ASF outbreaks internationally and publishes outbreak assessments considering the risk posed to the UK animals on GOV.UK.



Scenario

The reasonable worst-case scenario is based on an incursion of an acute strain of ASF into a feral pig population in England, which spreads before detection to domestic and commercial pig farms. Acute forms of ASF are highly pathogenic and have case fatality rates as high as 100%, but the virus remains stable in the environment for several weeks and in frozen products such as meat for many months. Feral pigs are only found in some areas of England, Scotland and Wales. The outbreak in kept pigs could last for about 16 weeks, with restrictions on exports remaining in place for a minimum of 9 months following the last confirmed infection. The outbreak in feral pigs could persist for up to 70 weeks. However, the scale of this scenario continues to be assessed.

Key assumptions for this scenario

The scenario is based on an outbreak of ASF strain that causes acute infection. Disease would begin by spreading undetected through the feral pig population until it reaches nearby domestic pig farms. The incursion into a commercial pig farm is assumed to be human mediated.

Variations of this scenario

Some strains of ASF produce less intense clinical signs that can be expressed for much longer periods. Case fatality rates are lower but can still range from 30-70%. An outbreak of such a strain of ASF would affect the impact and duration.

Response capability requirements

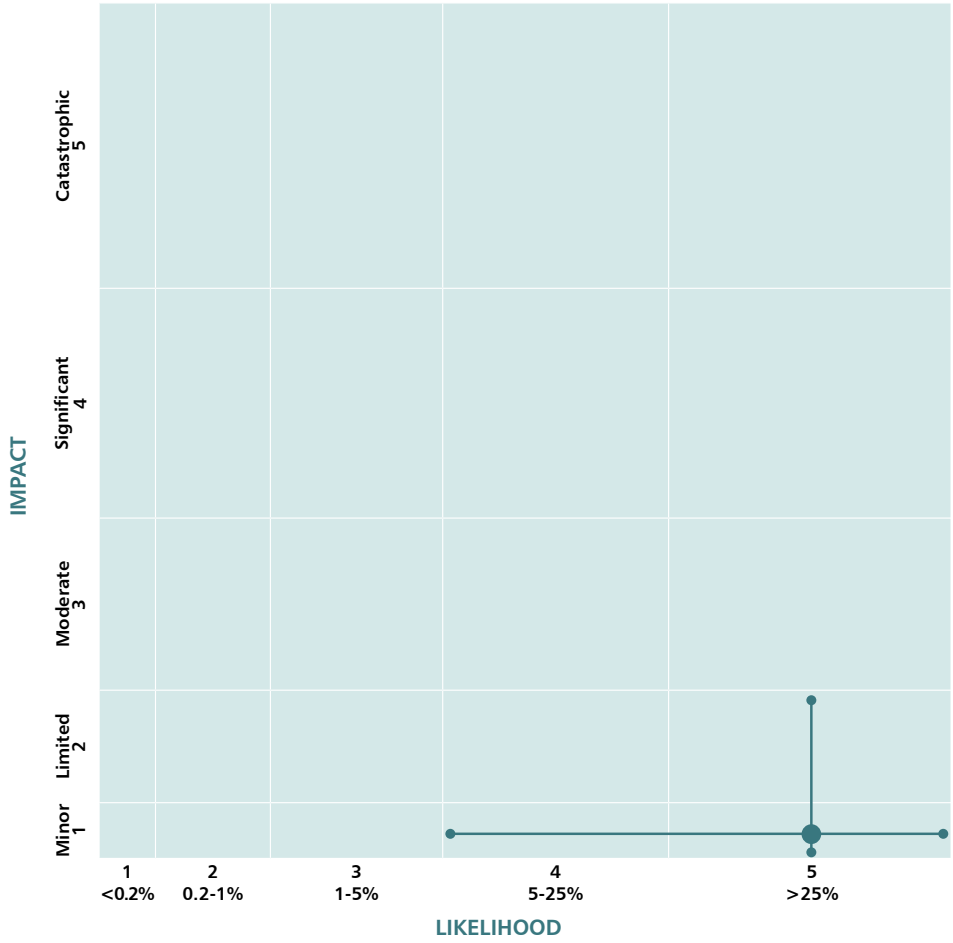
Specialist staff would be required to conduct surveillance and dispose of infected animals. These include vets, wildlife experts and marksmen, licensed slaughterers and carcass disposal logistics experts, in addition to carcass transport, rendering and incineration. Sufficient laboratory capacity to undertake surveillance in susceptible species would be needed, along with local authority staff to conduct enforcement activities, modelling experts, epidemiologists, disease experts, administrative staff and trained policy staff. Sufficient personal protective equipment (PPE), sample kits and approved disinfectant would be necessary across government and operational partners.

Recovery

For captive pigs, the minimum period to regain ASF Country-Free Status for international trade is 3 months after cleansing and disinfection of the last infected premises. In feral pigs, the minimum period to recover ASF free status is 12 months. It is expected that some of our trading partners would implement national export bans upon confirmation of ASF in captive or feral pigs.

Major outbreak of plant pest: *Xylella fastidiosa*

Xylella fastidiosa is a bacterium that is responsible for causing a number of named plant diseases. It was first detected in Europe in 2013 and is now established in France, Italy, Portugal and Spain. The bacterium has been reported from a very wide range of hosts, and the number of plant species that have been shown to be infected is constantly increasing. Legislation has been updated to prevent the introduction of X. fastidiosa on certain hosts, such as olive and rosemary, which are considered to be highly susceptible to the bacterium. The Animal and Plant Health Agency and Forestry Commission also carry out annual surveillance for X. fastidiosa.



Scenario

The reasonable worst-case scenario is based on an outbreak of Xylella in an area containing 3 to 5 plant nurseries, with evidence of possible spread on plants and plant products to multiple premises across the UK. While it is difficult to quantify the costs associated with Xylella impacting plant nurseries, there could be moderate economic costs relating to lost working hours, lost stock and restrictions on trade (estimated to be over £7.5 million for 5 nurseries over 5 years). The cost of government intervention, including surveillance, is estimated to be £5 million over 5 years. In the short term, measures to remove plant species may impact air quality (through the burning of material) and water quality (through the use of herbicides and insecticides).

Key assumptions for this scenario

It is assumed that if multiple outbreaks or outbreaks of other pests occur simultaneously, these would drain resources and likely mean that increased levels of impacts are seen.

Variations of this scenario

A high-impact variation involves the bacterium being found in an area with large plant nurseries reliant on growing host plants of Xylella. The nurseries would be significantly impacted due to the scale of eradication needed. The risk could be compounded if a coordinated approach to mass testing between Northern Ireland and Great Britain is hampered, during the period where future arrangements for laboratory accreditation schemes and mutual recognition are being developed, following the UK's exit from the EU.

Response capability requirements

Surveillance to monitor the spread of the bacterium, capabilities to diagnose the pest and procedures to report suspected cases would be required. In addition, the removal and disposal of infected and suspect plants, and the application of pesticides by registered spray operators to control vectors of the bacterium, would be necessary.

Recovery

Depending on the situation, businesses such as garden centres and nurseries may be able to recover after a short period, whereas others may need longer or may never recover.

Major outbreak of plant pest: *Agrilus planipennis*

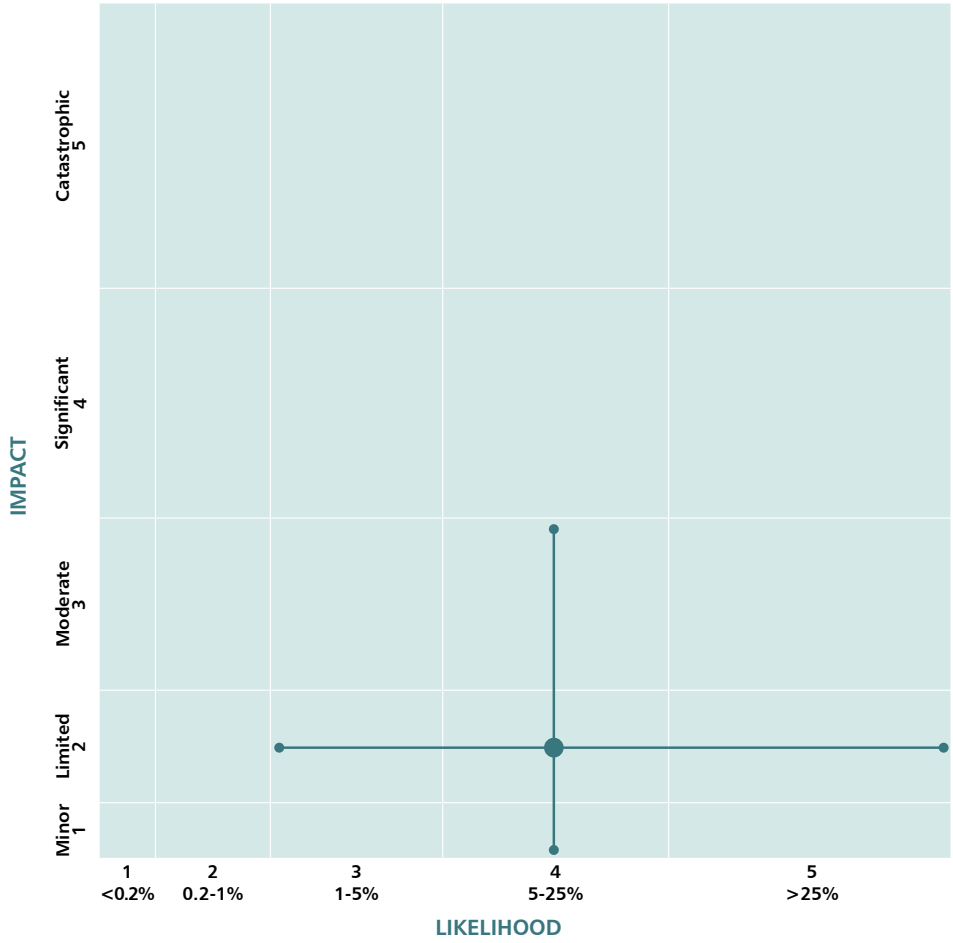
Larvae of the emerald ash borer beetle (*Agrilus planipennis*) bore into the inner bark and outer sapwood of ash trees, weakening the trees and causing them to die. There have been no previous outbreaks in the UK, but as the beetle spreads across Europe, there is an increasing likelihood that it will enter the country. This would result in significant damage to both the environment and economy. Import restrictions have been introduced to mitigate the risk of entry on host plants, host wood, wood chips and bark. The Forestry Commission also carries out annual surveillance for the beetle.

Scenario

The reasonable worst-case scenario is based on an outbreak in a mature, mixed woodland, which has remained undetected for 5 years. Initial surveillance would show that the beetle has spread beyond a 100x100m area, with the spread having occurred over multiple other sites. The beetle would have been present at these sites for 2 years. Damage could be partially reversed through the replanting of trees, although this is likely to have significant economic costs. The economic cost of the outbreaks could be over a billion pounds in environmental losses from impacts on air quality, biodiversity loss and carbon release (from burning).

Key assumptions for this scenario

It is assumed that the beetles would remain undetected for a long period of time, meaning that they spread a significant distance and cannot be eradicated. It is also assumed that resources would be drained if multiple outbreaks or outbreaks of other pests occurred simultaneously, with increased levels of impacts being seen.



Variations of this scenario

A high-impact variation involves a beetle found in southern England (with a more favourable, warm climate with ash trees within flight distance), allowing the beetle to spread further and impact a wider area. In comparison, an outbreak of the beetle in Scotland, which has a less favourable climate, will not grow as quickly and would have lower impacts on ash trees.

Response capability requirements

Surveillance to monitor the spread of the beetle, capabilities to diagnose the pest and procedures to report suspected cases would be needed. Additionally, capability to destroy the worst-affected trees would be required, including tree-felling services to remove seriously damaged trees and dispose of them via chipping or incineration. Response capabilities also include research and development to improve detection and management methods, including research to approve biological control agents.

Recovery

It is likely that the majority of ash trees would be impacted. However, there are some long-term management options that could be introduced to reduce the impact of the beetle, including chemical trunk injections for valuable trees and the release of biological control agents that parasitise the beetle. Where ash trees have been killed, replanting with resistant ash species (if identified) or other tree species would be possible, although regeneration could take many years.

Societal

Public disorder

Public disorder is a highly unpredictable risk. Although the majority of protests in the UK remain peaceful, on rare occasions these events can escalate towards conflict. The primary driver may be long-standing grievances, or it could occur as a spontaneous response to a single incident. Peaceful protests are not considered a form of public disorder, and the right to protest is enshrined in UK law.

Scenario

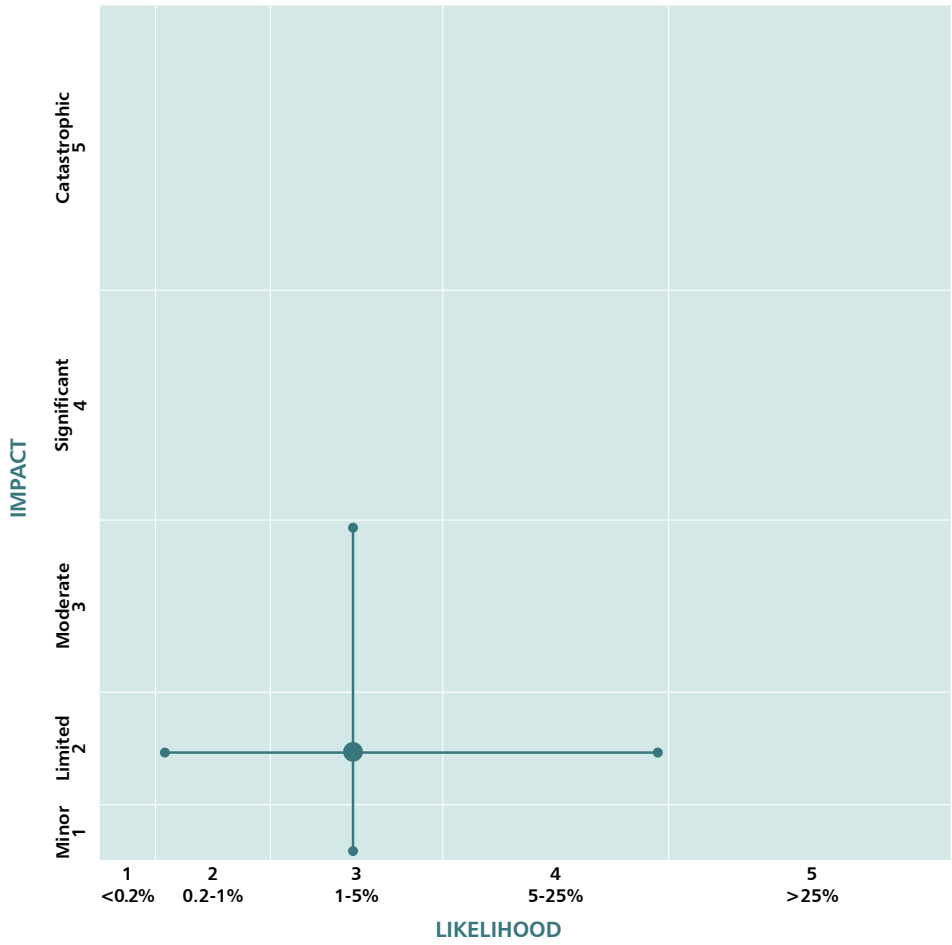
The reasonable worst-case scenario is based on large-scale disorder that significantly impacts the emergency services and government. In this scenario there is criminal damage to public and private property, increased acquisitive crime, arson, rioting, looting and reduced community cohesion. Injuries would be expected to both members of the public and those involved in the emergency services response. There would be a risk of fatalities, with health services coming under increased pressure. There may also be reduced confidence in the police and government.

Key assumptions for this scenario

It is assumed that there may be a number of specific trigger or flash points, which would lead to localised disorder across urban locations, simultaneously or sequentially.

Variations of this scenario

A more impactful variation is large-scale disorder breaking out at multiple sites across large parts of the UK, which could stretch police resources. A less impactful variation would be large-scale disorder breaking out in a single large city or region in the UK.



Response capability requirements

Key response capabilities could include police support units, evidence gathering teams, custody, mounted police and baton rounds.

Recovery

There would be long-term consequences on the economy – especially in areas that are already experiencing an economic downturn.

Industrial action

Industrial action happens when trade union members are in a dispute with their employers that cannot be solved through negotiations. It can take the form of a strike where workers withdraw their labour for a period of time, or action short of strike such as a work to rule. Both forms of action can lead to disruption affecting critical services or infrastructure. In order for industrial action to be legal, there are a number of conditions set out in the Trade Unions and Labour Relations (Consolidation) Act 1992, as amended by the Trade Union Act (2016). These conditions are that there must be a trade dispute between the union and the direct employer, the union must notify the employer of its intention to ballot for industrial action, that the ballot is conducted by post overseen by an independent scrutineer, and that the union notify the outcome of the ballot and intended strike dates to the employer in advance.

The impact and likelihood of industrial action varies across different organisations in both the public and private sector and is typically a reflection of the industrial relations landscape within organisations. Unofficial or wildcat action is possible, where workers take action having not complied with the law governing industrial action or where action is taken by workers without the right to take action, such as prison officers. Such instances are rare, as the workers taking unofficial or wildcat action expose themselves to summary dismissal by the employer without recourse to an employment tribunal.

The Civil Contingencies Act (2004) places a duty on certain organisations to have in place plans for maintaining key services in the event of significant workplace absences including strikes. Other critical sectors also have comprehensive plans in place.

Scenario

The reasonable worst-case scenarios for industrial action are based on action being taken by a significant number of staff and/or staff in critical roles taking action over a prolonged period. In disrupting an organisation's ability to function normally, industrial action can lead to temporary closures of sites, reductions in the availability of key services with impacts ranging from inconvenience and frustration to severe risk to welfare and safety. Services might continue, but at a reduced capacity during a strike period. The disruption could lead to economic consequences.

Key assumptions for this scenario

Different assumptions apply to industrial action in different sectors. For some sectors, the risk of industrial action has increased, due to external factors such economic pressures or changes to working conditions and other organisational changes. This is heightened by ongoing pay restraint in the context of inflation. Having a comprehensive engagement framework with recognised trade unions is an essential enabler to early dispute resolution and to averting industrial action. Depending on scale or duration of the strike pattern, industrial action can lead to disruption at the regional or national level.

This risk is featured in the full matrix on page 15, representing the averages of multiple different scenarios presented together in the 'industrial action' category.

Variations of this scenario

Alternative scenarios include long periods of discontinuous industrial action and strike action by different groups of staff within the sector. Events may be localised or national, and the duration could vary significantly, which would impact the response. The duration of strike action can also be affected by the union's agreement to, and ability to, offer strike pay to compensate striking workers for their loss of pay. Other factors that would exacerbate the impact of a strike include ongoing short- or long-term incidents or challenges.

Response capability requirements

Organisational resilience to industrial action varies by organisation and is typically a product of an organisation's reliance on workers with special knowledge or skills, access to contingency labour and, to some extent, the ability to agree derogations to protect critical services during periods of strike action. Appropriate contingency arrangements are enacted while the matter is resolved and operators are required to maintain plans for business continuity. Wherever possible, the government encourages negotiation and mediation, such as via the Advisory, Conciliation and Arbitration Service, as a means of resolving industrial action both before and during a strike.

Recovery

Recovery is dependent on the sector and the duration and extent of the action, however for the majority of situations it is likely to be swift. There could be broader implications for relationships between staff and employers, and between striking and non-striking staff.

Reception and integration of British Nationals arriving from overseas

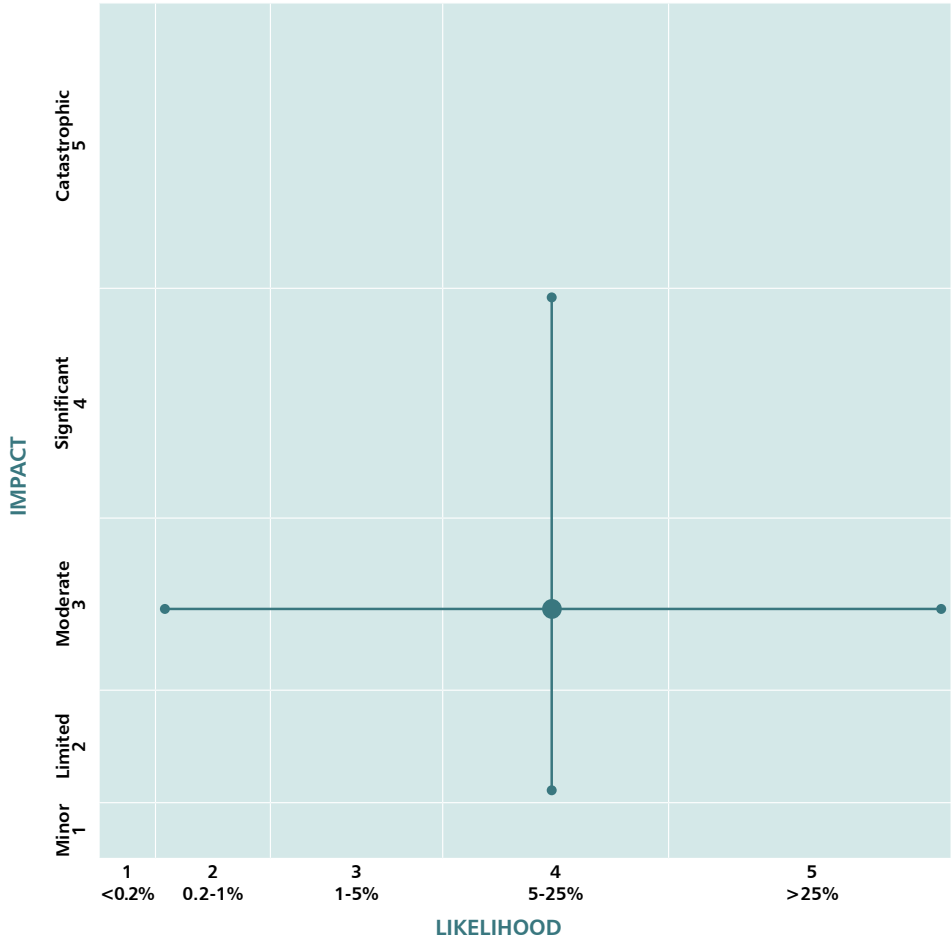
A significant proportion of British nationals (BNs) reside abroad, with approximately 5.5 million BNs estimated to live overseas in 2022. An adverse event in another country, such as a terrorist attack or natural disaster, may result in a sudden influx of BNs returning to the UK. For example, the COVID-19 pandemic saw BNs travelling to the UK with the intention to reside from 57 countries and territories.

Scenario

The reasonable worst-case scenario assumes the reception and integration of a large number of destitute or vulnerable BNs arriving from overseas who do not normally reside in the UK and are unable to stay with family or friends. These individuals could arrive within a 3- to 4-week period following an emergency/crisis overseas, such as conventional war, widespread civil unrest, political instability, sustained terrorism campaign or a natural hazard. There could be a small number of casualties or fatalities depending on the type of emergency overseas.

Key assumptions for this scenario

It is assumed that BNs would seek to enter the UK as opposed to another country, with minimal notice. Government support and funding may be required for local authorities and other agencies to deliver this and cover recovery costs.



Response capability requirements

There would need to be wide-ranging support services available for the proportion of BNs that are destitute or vulnerable on arrival. This could range from a small proportion (meaning 10%) to a greater proportion (meaning 50% or higher), depending on the circumstance of the event. Local authorities (in conjunction with other agencies and the voluntary sector) should have support packages in place for vulnerable or destitute BN arrivals. This would include support at airports or arrival locations (such as food, water, clothing and medicines), and emergency shelter or temporary accommodation as part of the immediate response. Government support and funding may be required for local authorities and other agencies to deliver this and cover recovery costs.

Recovery

A long-term integration package would need to be provided by local authorities (including engagement with other agencies and the voluntary sector). This would include employment assistance, education for school-aged BNs, and child and adult social care. Additional services may include mental-health screening, psychological support, counselling and victim support. There could also be longer-term housing requirements.

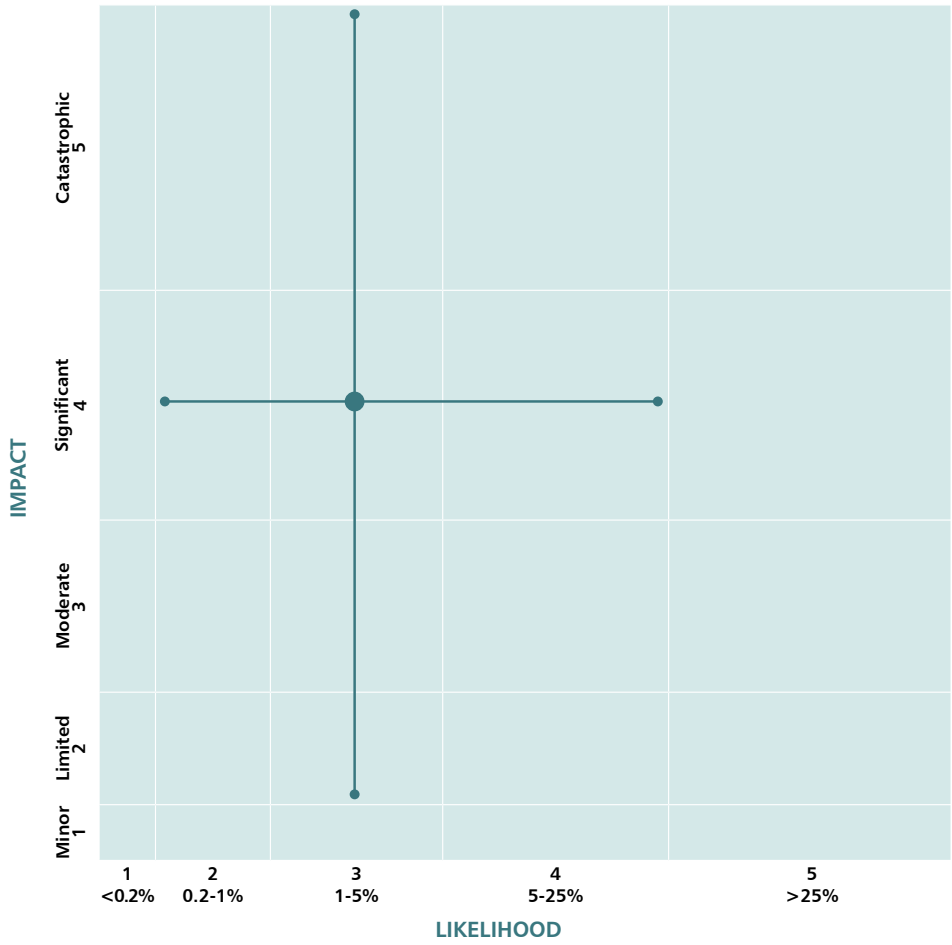
Conflict and instability

Deliberate disruption of UK space systems and space-based services

The UK relies on a broad range of space capabilities every day. These include infrastructure in orbit and on the ground, the people that operate it, and the applications and services that run on it. Secure global communications are key to our ability to protect and defend and support high-speed connectivity to remote and rural communities. Satellite-derived position, navigation and timing signals underpin services such as banking and transportation, as well as almost all the UK's critical national infrastructure (including energy, emergency services and healthcare) and defence operations. Space capabilities are already central to many basic and safety-critical civil functions, and this dependency on space will only increase.

Scenario

The reasonable worst-case scenario is based on an attack on UK or allied space-based systems or services by a hostile state or a proxy. The attack would aim to further their economic, political or military objectives, while attempting to reduce the risk of attribution. There would be immediate and longer-term impacts on UK space systems and services, resulting in severe disruption to essential services downstream. These could include food and water, and financial market infrastructure and communications (both voice and data services).



Response capability requirements

Response capability requirements would depend on the attack method and how it impacted space-based infrastructure, ground-based facilities and essential radio frequency links. Cyber security measures, counter-jamming technology and interference detection capabilities could help to protect against an electronic attack. Space domain awareness would support attack attribution and impact assessment. The continued development of highly secure and resilient space-based services would reduce the potential impact to the UK's most critical defence and security functions. Collaboration with international partners offers further opportunities to enhance the overall resilience of our collective space capabilities. We should also exploit the potential offered by alternative infrastructure and service solutions (such as terrestrial-based navigation and timing systems).

Recovery

Recovery timelines would depend on the attack method and how it impacted space-based infrastructure, ground-based facilities and essential radio frequency links. For temporary and reversible disruption to space assets, recovery timelines could be measured in minutes. However, a permanently damaged satellite could take years to replace.

Attack on a UK ally or partner outside NATO or a mutual security agreement requiring international assistance

Scenario

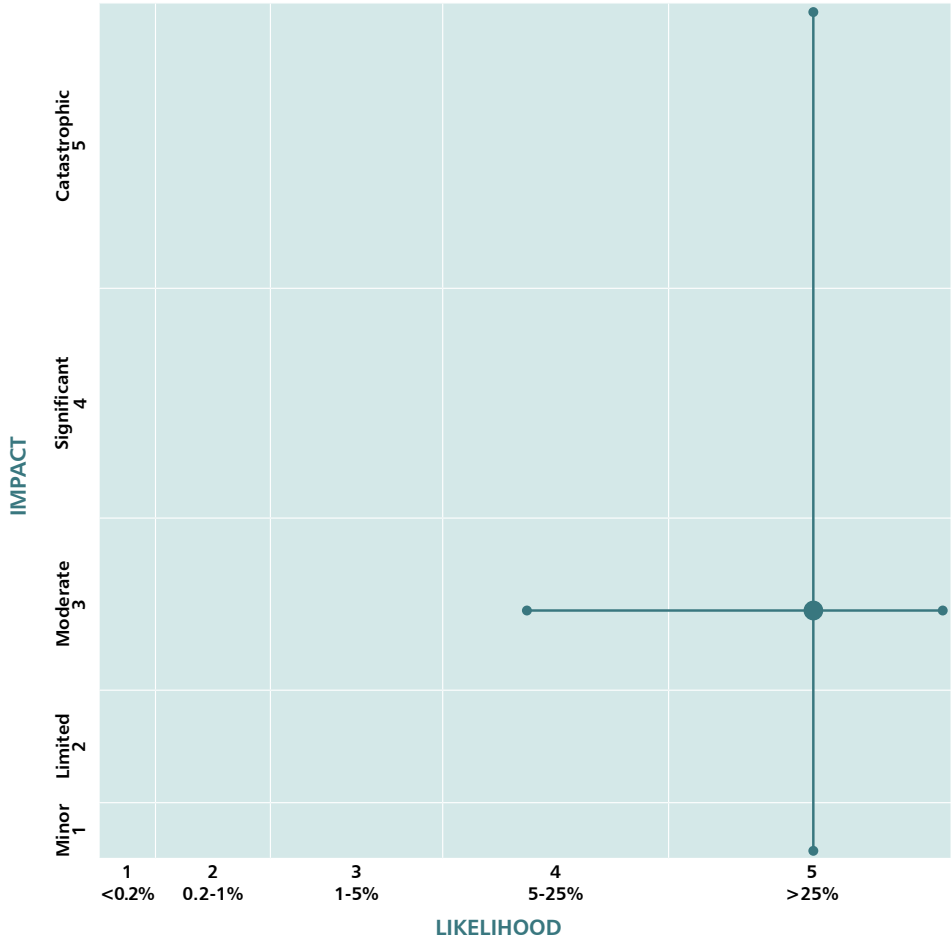
The reasonable worst-case scenario for this risk involves an adversary state with a large, advanced military conducting a major air and land assault on a non-North Atlantic Treaty Organization (NATO) security partner of the UK. The partner state suffers mass military and civilian casualties and a refugee crisis develops. Although the scenario is not UK based, there are likely to be British Nationals involved and humanitarian assistance will be required.

Response capability requirement

To contain aggression and deter further aggression from an adversary state, military, diplomatic and economic (sanctions) capabilities will be needed.

Recovery

This event would result in impacts lasting several years. Economically, the disruption to global markets (depending on the location) could be impacted by disruption of supply chains, reduction or prevention of fuels (gas and oil) and global economic instability.



Attack against a NATO ally or UK deployed forces, which meets the Article 5 threshold

The North Atlantic Treaty Organization's (NATO) purpose is to guarantee the freedom and security of its members through political and military means. NATO is committed to the principle that an attack on one or several of its members is considered as an attack on all. This is the principle of collective defence, which is enshrined in Article 5 of the Washington Treaty. So far, Article 5 has only been invoked once, in response to the September 11th terrorist attack in the US in 2001.

Scenario

The reasonable worst-case scenario involves a hostile state launching an invasion of a NATO ally or an attack on UK deployed forces, which causes NATO allies to unanimously invoke Article 5 of the Washington Treaty. NATO activates its response plans but hostile state forces are not ejected and the crisis continues. There is disruption to UK and European economies as economic ties with the hostile state are severed. There would be large numbers of casualties and fatalities. Although the scenario is not UK based, there are likely to be some British Nationals involved. Depending on the region where the crisis occurs, there could be severe disruption to gas supplies.

Response capability requirements

This would require a full range of military, diplomatic, economic and information capabilities to contain aggression and deter further aggression.

Recovery

This event would result in impacts lasting several years. Economically, the disruption to global markets (depending on the location) could be impacted by disruption of supply chains, reduction or prevention of fuels (gas and oil) and global economic instability.

Conventional attack on the UK mainland or overseas territories[3]

Protection of the UK, its citizens, property, and territory, from adversarial states, remains one of the highest priorities of the government. This defence and security protection extends to UK overseas territories and crown dependencies. NATO provides the backbone of the UK's collective defence within the Euro-Atlantic, however sovereign options are required to support overseas territories that may fall below the NATO Article 5 threshold.

Scenario

The reasonable worst-case scenario of this risk involves an adversary nation attacking the UK mainland or overseas territories using a combination of conventional missiles and cyber operations. For this scenario, targets are related to infrastructure. Although no population centres are deliberately targeted, a successful attack is likely to result in civilian fatalities as well as members of the emergency services. The economic costs of such a scenario would be high, as well as significant impacts to essential services.

[3] A separate scenario involving a nuclear attack on the UK mainland or UK overseas interests exists and is held at a higher classification.

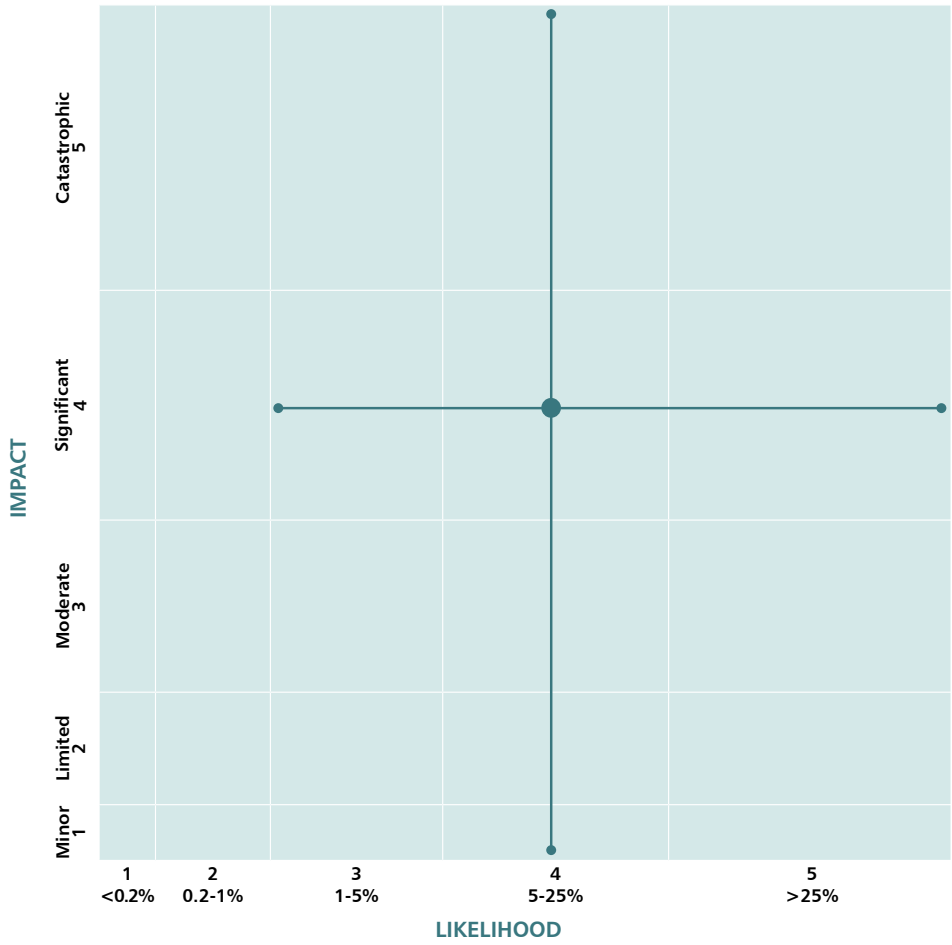
Nuclear miscalculation not involving the UK

Some countries possess nuclear weapons, so this will always remain a risk. Nuclear miscalculation refers to the risk that a state will mistakenly understand the intentions of another state and respond by launching a nuclear strike. The false belief that an attack is imminent causes a country to 'miscalculate' the risk of full-scale war and escalate a conflict to the nuclear level.

The UK works within the Non-Proliferation Treaty to stop the spread of nuclear weapons, promote cooperation and advance nuclear disarmament. The UK does everything it can to promote diplomatic solutions to every conflict.

Scenario

The reasonable worst-case scenario for this risk involves a limited nuclear conflict between two states that does not involve the UK. The impacts in the affected region would be catastrophic, particularly in terms of numbers of casualties and fatalities. There would be famine as a result of the event (caused from the fallout and the impact on the climate affecting food production). This would increase demand for imported foods leading to a dramatic increase in the cost of basic and staple foods in the UK. The human and economic impact of the event would necessitate enormous long-term humanitarian assistance. There would be implications for UK businesses with direct or indirect ties to the affected region. British Nationals in the region would require support. There would be the potential for high levels of migration to the UK, increasing pressure on infrastructure.



Response capability requirements

The UK maintains a civilian staff qualified to monitor radiation levels. Humanitarian assistance would be provided and our border staff would prepare to handle higher numbers of refugees needing assistance.

Recovery

The extent of the recovery needed for the UK would depend on the scale of the secondary impacts. Recovery in the affected areas would take many years and large-scale investment would be required.

© Crown copyright 2023

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated.

To view this licence, visit nationalarchives.gov.uk/doc.open-government-licence/version/3

Any enquiries regarding this publication should be sent to us via: gov.uk/contact/govuk

Open Government Licence

HM Government