

National Risk Register

2026 edition

HM Government

Contents

Foreword 6

Chapter 1: Introduction 8

What are the key changes in this edition? 10

How does the government plan for risk? 11

Who should use the National Risk Register (NRR)? 12

Chapter 2: Risk assessment methodology and matrix 13

How are risks identified and assessed? 14

How risks inform capabilities 14

Assessing likelihood 15

Assessing impact 16

Expert challenge 17

Risk matrix 17

Chronic risks 21

Chapter 3: Individuals and communities 22

Preparedness advice 23

Preparedness tips from GOV.UK/Prepare 23

During an emergency 24

Help with recovery 24

Supporting communities and volunteering 25

Guidance for responding organisations 26

Identifying and assessing the disproportionate impacts of emergencies to vulnerable people 27

Chapter 4: Risk Summaries 29

Terrorism **30**

International terrorist attack 31

Northern Ireland-related terrorism 33

Terrorist attacks in venues and public spaces: explosive devices 35

Terrorist attacks in venues and public spaces: marauding attacks 37

Malicious maritime incident 39

Malicious rail incident 41

Malicious aviation incident 43

Strategic hostage taking 45

Assassination of a high-profile figure 47

Chemical, Biological, Radiological and Nuclear (CBRN) attacks 49

Conventional attack: gas infrastructure 51

Cyber attack: gas infrastructure 53

Conventional attack: electricity infrastructure 55

Cyber attack: electricity infrastructure 57

Conventional attack: civil nuclear 59

Conventional attack: fuel supply infrastructure 61

Cyber attack: fuel supply infrastructure 63

Attack on a government building 64

Cyber **66**

Cyber attack: health and social care system 67

Cyber attack: transport sector 69

Cyber attack: telecommunications systems 71
Cyber attack: data infrastructure 73
Cyber attack: water infrastructure 75
Cyber attack: police systems 77

State threats 79
Malicious attack: civil nuclear 80
Malicious attack: UK financial CNI 82
Malicious attack: UK retail bank 84
Major disruption to international subsea telecoms cables 85

Geopolitical and diplomatic risks 87
Disruption to global oil trade routes 88
Interference in UK democratic process 90

Accidents and systems failures 91
Major adult social care provider failure 92
Insolvency of supplier(s) of critical services to the public sector 94
Insolvency affecting fuel supply 96
Rail accident 98
Large passenger vessel accident 100
Major maritime pollution incident 102
Vessel blocking a major UK port 104
Accident involving high-consequence dangerous goods 106
Aviation collision 108
Malicious drone incident 110
Disruption to space-based services 111
Loss of Positioning, Navigation and Timing (PNT) services 113
Simultaneous loss of all fixed and mobile forms of communication 116
National power outage 118
Regional failure of the electricity network 120
National gas and electricity shortfall 122
Civil nuclear accident 124
Radiation release from overseas nuclear site 126
Radiation exposure from transported, stolen or lost goods 128
Technological failure at a systemically important retail bank 130
Technological failure at a UK critical financial market infrastructure 132
Accidental fire or explosion at an onshore major hazard (COMAH) site 134
Accidental large toxic chemical release from an onshore major hazard (COMAH) site 136
Accidental fire or explosion on an offshore oil or gas installation 138
Accidental fire or explosion at an onshore fuel pipeline 140
Accidental fire or explosion at an onshore major accident hazard pipeline 142
Accidental work-related (laboratory) release of a hazardous pathogen 144
Reservoir/dam collapse 146
Water infrastructure failure or loss of drinking water 148
Food supply contamination 150
Major fire 152
National disruption to data infrastructure 154
Digital resilience failure 156
Accidental damage on the National Gas Transmission Network 158

Natural and environmental hazards 160
Wildfire 161

Volcanic eruption 164
Earthquake 166
Humanitarian crisis overseas: natural hazard event 168
Disaster affecting a UK Overseas Territory 170
Severe space weather 172
Storms 174
High temperatures and heatwaves 176
Low temperatures and snow 178
Coastal flooding 180
Fluvial flooding 182
Surface water flooding 184
Drought 186
Poor air quality 188

Human, animal and plant health 190
Pandemic 191
Outbreak of an emerging infectious disease 194
Animal disease: major outbreak of foot and mouth disease 196
Animal disease: major outbreak of highly pathogenic avian influenza 198
Animal disease: major outbreak of African horse sickness 200
Animal disease: major outbreak of African swine fever 202
Major outbreaks of plant pest: *Xylella fastidiosa* 204
Major outbreaks of plant pest: *Agrilus planipennis* 206

Societal 208
Public disorder 209
Industrial action 211
Reception and integration of British nationals arriving from overseas 213
Significant disruption to the Criminal Justice System 215

Conflict and instability 217
Deliberate disruption of UK space systems and space-based services 218
Attack on a non-NATO partner requiring UK assistance 220
Attack against a NATO ally or UK deployed forces, which meets the Article 5 threshold 221
Conventional attack on the UK mainland or Overseas Territories 222
Nuclear miscalculation not involving the UK or its allies 223

Foreword

The risks the UK faces are more volatile, varied and interconnected than any time in living memory. In 2026 alone, the terrorism threat has increased to SEVERE, there has also been significant disruption to oil and gas supplies from the middle east and severe weather. There has also been continued conflict between Russia and Ukraine, a hantavirus outbreak linked to a Dutch cruise ship, rapid AI developments and cyber-attacks which have impacted businesses and institutions. The whole of the UK's national resilience - our economy, defences and biosecurity - is being tested like never before, and effective risk identification and assessment is crucial.

Now more than ever, national security and domestic resilience are the government's top priority. This resilience relies on continuously assessing our risks and vulnerabilities as they continue to change rapidly. The UK has improved its approach to assessing these risks over the last two decades, to better understand what action is appropriate. This document – the National Risk Register (NRR) – is based directly on the internal, classified National Security Risk Assessment (NSRA), the UK government's single, authoritative articulation of the most serious acute risks facing the UK and its interests overseas. The NRR and NSRA provide a foundation for the UK's resilience system.

As the world changes, we must adapt, too. The NSRA is updating to respond to these risks, becoming a more dynamic assessment process. Risks can now be updated as frequently as needed, driven by the best evidence of real-world changes. We must learn from experience and not fall foul of 'Groupthink' and conventional wisdom, which are now challenged through the refreshed Expert Advisory Programme. This new edition of the NRR captures recent updates to these internal processes.

We continue to strengthen our domestic resilience, as outlined in last year's Resilience Action Plan. For example, it reflects the conclusions of the UK government's review of resilience which included consideration of the findings from the COVID-19 Inquiry Module 1 and the Grenfell Tower Inquiry. The Plan recommended the UK government issued new guidance for lead government departments in 2025, setting out six principles to identify and assess which individuals and communities may be disproportionately impacted during an emergency. This is the first edition of the NRR to reflect this strengthened understanding of the disproportionate impact of emergencies.

This edition of the NRR also includes a number of new risks. These include:

- a new risk for digital resilience failure – based on lessons from the global IT outage in July 2024;
- a 'cyber attack water infrastructure' risk – to reflect learning from reported cyber attacks targeting the water sector;
- two new risks focused on data infrastructure (one focused on a cyber attack and the other on disruption);
- One risk has been added focused on interference in democratic processes; and
- Two risks focused on operational and system-wide pressures - 'significant disruption to the criminal justice system' and 'accidental damage to the national gas transmission network'.

This government is committed to sharing risk information as openly as possible, to support all those working to build the UK's resilience with their planning, preparation and response activity. Greater transparency also means that people can scrutinise our assessments, and challenge us to do things differently when needed. We need everyone to play their part in building resilience – so this National Risk Register underpins the public guidance on the Prepare website, which sets out the simple and effective steps we can all take to prepare for emergencies.

I want citizens in the UK to live in a society that is as resilient as anywhere else in the world. A whole of society approach is required to increase resilience, therefore, I encourage all risk and resilience professionals to consider the risks in this publication, and join our collective endeavour to make the UK more prosperous and secure.



Dame Angela Eagle DBE MP
Security Minister



Chapter 1

Introduction

The UK faces a landscape of volatile, diverse, and interconnected risks, ranging from geopolitical instability to rapid technological change. As emphasised in the June 2025 National Security Strategy, these risks may be non-malicious, such as accidents or natural hazards or they may be malicious threats from actors who seek to do us harm.

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 NRR and NSRA provide a foundation for the UK's resilience system. The Resilience Action Plan published in July 2025 sets out further detail on our plan to strengthen our domestic resilience and how the UK government is investing to protect the nation, defining our objectives and the actions we will take to become more resilient.

Building resilience to these risks needs a shared effort between government, local communities, businesses, individuals and allies. This process starts with building greater public awareness of the risks we face. The National Risk Register (NRR) takes a "transparent by default" approach to inform that collective effort, as part of a national conversation about risks and preparedness. The UK has well established arrangements in place to manage the range of risks, including flooding, pandemics and terror attacks. In addition, to help mitigate risks to the British people and national security from international conflict and instability, the government has announced its Home Defence Programme - an additional layer of defence, security, and resilience planning, focused on alignment between military and civilian effort in a period of international hostilities affecting the UK.

The risks that meet the threshold for inclusion in the NRR would have a substantial impact on the UK's safety, security or critical systems at a national level.

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). Relevant bodies consider many variations of scenarios at the planning stage. The NRR includes information on the response capabilities required to respond to and recover from the emergency, should the risk materialise.

The NRR is based directly on the NSRA – an internal, classified risk assessment that is used within government and by Local Resilience Forums (LRFs) and their equivalents across the four nations.

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, the devolved governments, the government scientific community, intelligence and security agencies, and independent experts.

While the NRR focuses on 'acute' risks – discrete events requiring an emergency response – it is part of a broader resilience framework. It sits parallel to the Chronic Risks Analysis (CRA), which identifies the medium-to-long-term threats that gradually undermine our economy, security, and way of life. Although risk owners incorporate an

understanding of these enduring drivers when assessing acute threats, the CRA provides the comprehensive view of the nation's evolving strategic risk profile. Used together, these documents allow practitioners to plan for both immediate crises and the underlying trends that shape future risks.

What are the key changes in this edition?

The NSRA operates as a dynamic assessment process, with risks reassessed on a more regular basis to reflect the changing risk landscape.

Within this NRR edition, the following changes have been made for all risks:

- text has been updated to reflect the **latest developments** in the risk landscape;
- text added on **common consequences** – to enable further clarity on the impacts that flow from risks,
- text added on the **impacts to vulnerable people** – to reflect further work across government to explore the disproportionate impacts of emergencies on people. These sections will be strengthened further in future editions as the understanding of this topic continues to grow.
- the **response and capabilities section is split out by actors** (1. 'Government and Agencies', 2. Critical National Infrastructure owners and operators (referred to as CNI) and the wider Private Sector, 3. 'Voluntary Community and Faith Sector') - to draw out examples of the different roles of different actors involved in the response to emergencies.
- **scoring** has been adjusted for some risks – to reflect further assessment of the impacts and likelihood.

A number of risks have been added to the NRR, including:

- **digital resilience failure** – to reflect learning from incidents such as the Crowdstrike IT Outage in July 2024.
- two risks on **data infrastructure** (one focused on a cyber attack and the other on disruption) – following further assessment of potential risks to this sector following its establishment as a CNI sub-sector in 2024.
- **cyber attack: water infrastructure** – to reflect learning from reported cyber attacks targeting the water sector.
- **cyber attack: police systems** – to reflect the heightened risk of cyber attacks across all systems and work carried out by government and the police to strengthen resilience.
- **significant disruption to the operation of the Criminal Justice System** – to explore disruption to the criminal justice system following lessons from previous overcrowding incidents.
- **accidental damage on the National Gas Transmission Network** – to explore damage to the gas transmission network as a result of agricultural digging.
- **interference in UK democratic process** – to explore threats to democracy and potential interference.

The disruption of Russian gas supplies to Europe risk has been removed as reliance on Russian gas imports has significantly reduced.

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 been based on influenza. Any new pathogen transmitted by the respiratory route is likely to share characteristics with influenza. Therefore the plans for pandemic influenza are likely to have considerable overlap which means lessons can be drawn across where relevant.

Lessons from COVID-19 have been incorporated into the government's risk assessment methodology and the UK government will continue to strengthen its approach. For example, updating the assessments dynamically in response to changes in the risk landscape and where appropriate including multiple and varied scenarios.

The Resilience Action Plan published in July 2025 sets out further detail on our plan to strengthen our domestic resilience. The plan reflects the conclusions of UK government's review of resilience which included consideration of the findings from the COVID-19 Inquiry Module 1 and the Grenfell Tower Inquiry.

How does the government plan for risk?

Having a clear understanding of the risk landscape amongst those who need to respond is essential for preparing for and dealing with emergencies. The National Risk Register (NRR) is our public facing articulation of the risks facing us. A world-leading "transparent by default" approach has been adopted, declassifying and sharing information from the NSRA except in a small number of highly sensitive areas. It enables more effective decision-making, better communication and coordination, and more efficient resource allocation. 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. Devolved governments in Scotland, Wales and Northern Ireland also maintain their own risk assessment processes which complement the UK wide risk assessments.

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 Forums' 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, community and faith sector (VCFS) organisations who may play a central role in planning for and responding to emergencies and crises 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 available to all but not targeted at the general public. Advice for individuals, households and communities on preparing for a wide range of risks can be found on the Prepare website.

The government (at both the national and local level) also provides 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 via specific campaigns. 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's Emergency Alerts service is used to issue urgent messages to compatible mobile phones when there is a live or imminent risk to life in a defined area, and specific instructions on how to respond are required. While the alerting service has already been used in practice as part of the government's severe weather and flood warning response capabilities, it also serves a wider purpose; it can be used to support emergency response in a range of scenarios such as public health emergencies, fires, and in the case of Plymouth in February 2024, a residential evacuation.



Chapter 2

Risk assessment methodology and matrix

The 2026 NRR is based directly on the government's internal NSRA. The NSRA now operates on a dynamic process, where risks can be updated on a more regular basis to reflect the changing risk landscape.

How are risks identified and assessed?

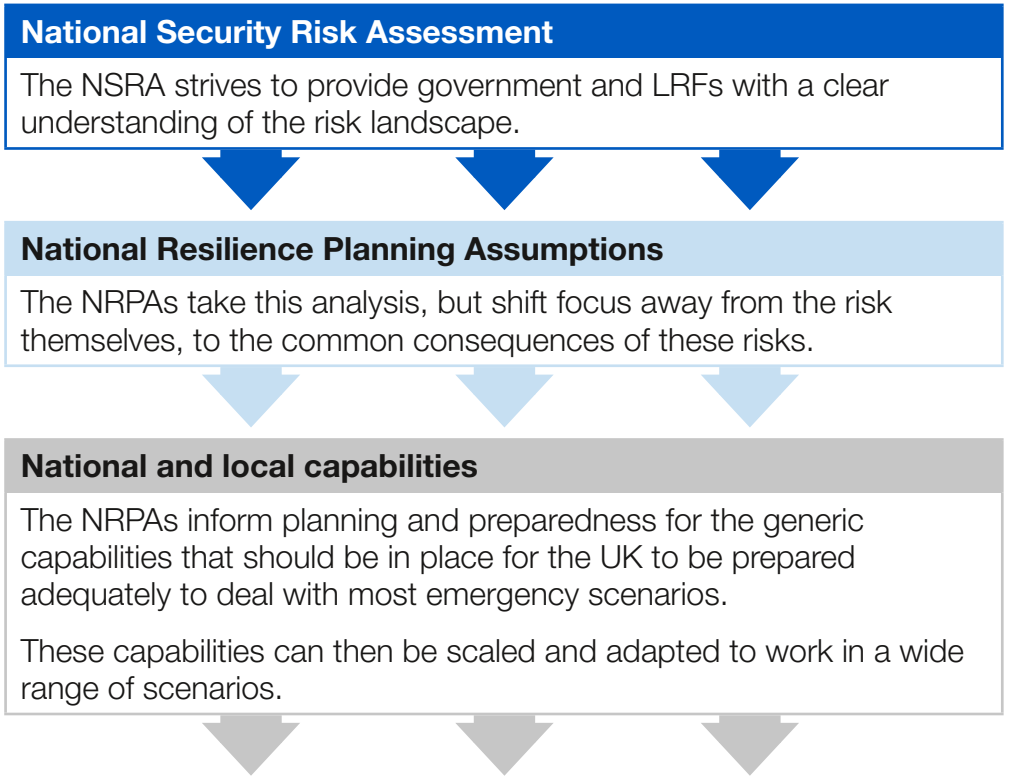
Risks are identified for inclusion in the NSRA and NRR by consulting a wide range of experts from across UK government departments, the devolved governments, the government scientific community and outside of government (for example, in partner agencies, academic institutions, the local level and industry). 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.

At the local level, Local Resilience Forums (LRFs) utilise the NRR and NSRA to create Community Risk Registers (CRRs) which are vital for local level planning.

How risks inform capabilities

As set out in Chapter 1, the NSRA and NRR do 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 serve as a cause-agnostic basis for planning for the common consequences. The UK government maintains 23 generic response capabilities that can be stood up to respond to the impacts of the risks identified in the NSRA and NRR. Furthermore, catastrophic risks may result in whole-system civil emergencies. These are likely to require the activation of multiple response capabilties at once, and others not identified within the programme, to mitigate the initial incident and its cascading impacts. The visual below demonstrates how an understanding of the risks we face informs what generic response capabilities are required.



Within this edition of the NRR common consequences relevant to each risk have been highlighted on each risk summary page.

Assessing likelihood

When a risk assessment is carried out, the relevant government departments and agencies assess the likelihood of the reasonable worst-case scenario occurring within the assessment period (which is 5 years for non-malicious risks and 2 years for malicious risks) using insight, 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. Please see table 2 which details how the likelihood scale corresponds with the Professional Head of Intelligence Assessment (PHIA) yardstick.

For malicious risks, there are 3 key parameters considered, the intent to carry out an attack, which 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).

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:

Table 2: 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

Score	Percentage chance	PHIA yardstick designation
5	>25%	Almost certain (95-100%) Highly likely (80-90%) likely or probable (55-75%) Realistic possibility (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%	

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 impact,** including cost of working hours lost, assets lost, cost of shelter and accommodation and wider expenses.
- **environmental impact,** taking into account impacts on different types of habitat, impacts on air and water quality, carbon release, significance of the impact and timescales for reparation.
- 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 future trends, interactions between acute and chronic risks, impacts to critical supply chains and the disproportionate impact of the reasonable worst-case scenarios on vulnerable people. In the individuals and communities section, further guidance is given on identifying and assessing vulnerable people.

The assessment and scoring of a risk focus primarily on domestic impacts – even where the risk occurs internationally. Each of the dimensions listed on the 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 3 on page 17 for a selection of example impact scale indicators). These scores are then combined to provide a single overall impact score. Risks assessed to have the highest impact score (5) are considered catastrophic.

Table 3: Example impact scale indicators for fatalities, casualties and economic cost

	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 £

Expert challenge

To ensure that the assessment process is robust, risks are reviewed by panels of technical and scientific experts, each led by an independent chairperson. Each panel is focused around different impact dimensions. The experts include professionals from industry, local level, 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.

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 (low, medium or high) 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 is represented as lines extending from the plotted dots in the individual risk matrices in Chapter 4 to provide a more comprehensive picture of the risk landscape and prevents planning or strategic decisions from being made with false confidence.

Although the 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 single topic 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 linked scenarios. For example, the flooding risks are split across three risks (coastal, fluvial and surface water flooding respectively).

The response capability requirements listed in the text are non-exhaustive. This has been split up by different actors involved i.e. government and agencies, CNI owners and operators and the wider private sector; and voluntary, community and faith sector. They are intended to provide a high-level overview of the potential response capability that may be needed.

Despite the extremely wide range of risks represented in the NRR, the capabilities required to respond to their emergence are common to many, necessitating much fewer response capabilities to be managed by the government than there are scenarios. These are overseen at the national level which aims to ensure response capabilities can be stood up immediately in the event of a risk materialising.

Impact		1 <0.2%	2 0.2-1%	3 1-5%	4 5-25%	5 >25%
Catastrophic	5	7, 27, 28		25a	38, 56	
Significant	4	21	23, 37, 58a	9, 10, 26, 51, 53a, 53b, 53c, 65	22, 41, 42, 49, 52, 57, 64	3
Moderate	3	17, 19, 31, 32, 33, 34, 35, 58c	54	4, 12, 24, 25b, 30a, 43, 46, 47, 55, 58b, 58d	11, 39, 45, 50, 59b, 60, 62	30b, 48
Limited	2	18, 29, 36	5, 16, 40, 44	20, 61, 63	2, 8, 13, 14	6, 59a
Minor	1				1, 15	

Likelihood

Terrorist and state threats

1 International terrorist attack
2 Northern Ireland related terrorism
3 Terrorist attacks in publicly accessible locations
4 Terrorist attacks on transport
5 Strategic hostage taking
6 Assassination of high-profile figure
7 Larger-scale CBRN attacks
8 Smaller-scale CBRN attacks
9 Medium-scale CBRN attacks
10 Conventional attacks on infrastructure[1]
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

[1] On the matrix the scores of a number of NRR risks are grouped together into two broader categories; 'conventional attacks on infrastructure' and 'cyber attacks on infrastructure', due to the sensitive, classified nature of the information. These categories therefore encapsulate a range of threats with varying scales of impact from different actors, ranging from small scale cyber attacks with limited impact to more significant threats to CNI, the UK mainland and interests.

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 Vessel blocking a major UK port
20 Accident involving high-consequence dangerous goods
21 Aviation collision
22 Disruption of space-based services
23 Loss of Positioning, Navigation and Timing (PNT) services
24 Simultaneous loss of all fixed and mobile forms of communication
25a National power outage
25b Regional failure of the electricity network
26 National gas and electricity shortfall
27 Civil nuclear accident
28 Radiation release from overseas nuclear site
29 Radiation exposure from transported, stolen or lost goods
30a Technological failure at a systemically important retail bank
30b Technological failure at a UK critical financial market infrastructure
31 Accidental fire or explosion at an onshore major hazard (COMAH) site
32 Accidental large toxic chemical release from an onshore major hazard (COMAH) site
33 Accidental fire or explosion on an offshore oil or gas installation
34 Accidental fire or explosion at an onshore fuel pipeline
35 Accidental fire or explosion at an onshore major accident hazard pipeline
36 Accidental work-related (laboratory) release of a hazardous pathogen
37 Reservoir/dam collapse
38 Water infrastructure failure or loss of drinking water
39 Food supply contamination
40 Major fire
41 National disruption to data infrastructure
42 Digital resilience failure
43 Accidental damage on the National Gas Transmission Network

Natural and environmental hazards

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

Human, animal and plant disease

56 Pandemic
57 Outbreak of an emerging infectious disease
58a Animal disease – major outbreak of Foot and Mouth Disease
58b Animal disease – major outbreak of highly pathogenic avian influenza
58c Animal disease – major outbreak of African horse sickness
58d Animal disease – major outbreak of African Swine Fever
59a Major outbreak of plant pest – *Xylella fastidiosa*
59b Major outbreak of plant pest – Agrilus planipennis

Societal

60 Public disorder
61 Industrial action
62 Reception and integration of British nationals arriving from overseas
63 Significant disruption to the operation of the Criminal Justice System

Conflict and instability

64 Deliberate disruption of UK space systems and space-based services
65 Nuclear miscalculation not involving the UK or its allies

The NRR includes 87 standalone risks, and 8 linked scenarios for a total of 95 risks. Some are not shown in the matrix above or are grouped together due to national security or commercial implications.

Chronic risks

The risks listed in the NRR are acute risks—discrete events that may require an emergency response from the government. Chronic risks, such as antimicrobial resistance (AMR), impacts of artificial intelligence (AI), reliance on global supply chain and climate change, are not included in this list. The government continues to work to strengthen its understanding of these risks. For example, in relation to AI, the government is focusing on how it develops and proliferates. The growth and use of AI may exacerbate NRR risks but also provide opportunities to mitigate them.

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. Due to the systemic and enduring nature of chronic risks, traditional probabilistic impact assessments are made less effective. Consequently, the government has established a parallel risk assessment framework, the Chronic Risks Analysis (CRA), which uses futures and systems thinking to help policymakers develop long-term mitigations.

The CRA identifies 26 chronic risks facing the nation, providing a comprehensive view of the underlying trends shaping our strategic risk profile. The public version was published alongside the Resilience Action Plan in July 2025 and is available on GOV.UK.

During every update of the NSRA, risk owners must also evidence how chronic risks – as set out in the Chronic Risks Analysis, including risks such as AI, climate change and reliance on global supply chains – manifest in, interact with and exacerbate acute events. Policy makers are also encouraged to identify both linked risks and compounding risks to ensure preparedness for simultaneous challenges.



Chapter 3

Individuals and communities

Preparedness advice

The information included here is for organisations that might have a role in communicating preparedness 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. In May 2024, the government published advice for individuals, households and communities on the Prepare webite on preparing for emergencies, including a number of low and no cost options. The Prepare website also includes specific advice for disabled persons and carers. For advice specific to Scotland, the Ready Scotland website contains information on preparing for and responding to emergencies affecting Scotland. For advice specific to Northern Ireland, please visit the NIDirect government services website for information on being ready for emergencies.

More information about the risks in a specific area can be found in local community risk registers:

- Community risk registers in England and Wales
- Community risk registers in Scotland

Preparedness tips from GOV.UK/Prepare

Below are five simple steps people could consider taking to improve their preparedness for emergencies. More can be found on the Prepare website, including advice related to specific risks (e.g. power cuts and fires). Taking action now will make it easier to manage if an emergency does happen.

1 Find out if you are eligible to sign up to your gas, electricity and water supplier's Priority Service Register, so they know that you need additional support, including when there is an interruption to your supply. Ask anyone you provide care for if they are registered.
2 Set a reminder in your phone or make a note on your calendar to check your smoke alarms at least once a month. You can involve children in the monthly test too.
3 Write down important phone numbers on paper such as the number to report a power cut (105) and the numbers of anyone you might want to contact in an emergency.
4 Talk to your children about emergencies – teach them how and when to call 999 and what they should do if there's an emergency, such as a fire at home.
5 Check your long-term flood risk and sign up for flood and weather warnings.

During an emergency

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.

In an emergency pay attention to official sources of information such as the websites and social media accounts of local authorities, government agencies or emergency services, or messages to your mobile phone from the UK Government Emergency Alerts Service.

You should check local radio stations and local TV broadcasts, internet and news sources for specific advice from local emergency partners.

The internet can be a helpful source of information. However, some information found online can be misleading and inaccurate, making it harmful to share with friends, family or colleagues. Use the online media literacy resources guidance to help you navigate the online world with confidence.

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. More advice on coping with trauma following emergencies can be found on the Prepare website, which includes links to relevant NHS pages.

Supporting communities and volunteering

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.

The information at GOV.UK/Prepare | Get involved in your community provides information and advice to individuals and community groups about:

- ways to safely get involved and support their communities before, during and after emergencies.
- how community groups can build networks and support their communities before, during and after an emergency.
- donating during an emergency – including information for businesses about how they can support communities when an emergency happens.

When emergencies happen, people often feel compelled to help. Some 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.

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 recommended 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 voluntary, community and faith sector organisation. If it's safe to do so, people can also help by checking on neighbours and vulnerable people in their community, to see if they need any help or assistance.

Some examples of the ways the public can support their community:

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
- **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 an emergency, the public can also offer their help to clean up, help others to get back on their feet, or support their community with any longer term impacts.

Guidance for responding organisations

Emergency 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.
- 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.

The UK government has published:

- the Community Resilience Development Framework and
- guidance on 'Planning the Coordination of Spontaneous Volunteers' in 2019.
- Identifying and Supporting People who are Vulnerable in an Emergency

The Community Resilience Development Framework is a reference tool for the delivery of strategic approaches to community resilience at the local level, in collaboration with non-statutory partners, such as voluntary, community and faith sector organisations and businesses. 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. The above also includes guidance for Local Resilience Forums on identifying and supporting people who are vulnerable in an emergency, outlines the responsibilities of Category 1 and 2 responders to plan for, and meet the needs of, those who may be vulnerable in an emergency, including information on establishing and embedding considerations into plans, and examples of multi-agency partnership activity to support community resilience building.

Additionally, guidance is available from the Scottish government on the topic of Building Resilient Communities. This guidance recommends that responders consider best practice for community resilience, 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.

Identifying and assessing the disproportionate impacts of emergencies to vulnerable people

The UK's Resilience Action Plan (2025) highlights that although emergencies can affect anyone. However, the impacts are not felt equally across society. Understanding such disparities are critical to increasing national resilience and reducing the impacts of emergencies.

The Resilience Action Plan defines vulnerable people as individuals or communities who may experience more significant and disproportionate impacts during emergencies. Vulnerability is not a fixed characteristic; it is shaped by a complex interplay of factors, which are intersectional and interconnected. These factors can be temporary or long-lasting, and their significance may differ based on the specific context of the emergency. Furthermore, emergencies can create new vulnerabilities and exacerbate existing ones. It is often assumed that vulnerability stems from a lack of ability or agency to meet basic needs. However, many groups labelled as vulnerable actively exhibit a sustained capacity to cope with conditions of adversity. Therefore, it can be difficult to assess who is most 'at risk'.

In preparing for emergencies, it is important not to solely focus on individuals or groups who are already known to be vulnerable or at risk (e.g., those on the Priority Service Register). Emergencies can create disproportionate impacts on people who might not be considered vulnerable in everyday scenarios. Moreover, many people often labelled as 'vulnerable' do not, in fact, consider themselves as such. Relying on tools such as Priority Service Registers and other public sector vulnerability lists is a useful start but is unlikely to capture all individuals or groups who could be more severely impacted.

As a key recommendation of the UK's Resilience Action Plan, the UK government commissioned experts in the Government Office for Science to examine how different risk scenarios could make people more vulnerable, or exacerbate existing vulnerabilities. New guidance was issued across government in 2025, setting out six principles to identify and assess which individuals and communities may be disproportionately impacted during an emergency. The principles can also be used to help risk practitioners think through different dimensions of an emergency (and recovery period) and consider which members of society are most likely to be disproportionately impacted.

Six principles to identify and assess which individuals and communities may be disproportionately impacted during an emergency:

- **Principle 1:** *consider who is likely to be disproportionately impacted in an emergency beyond those already considered 'at risk' in non-emergency contexts*
- **Principle 2:** *consider how social and environmental factors, especially poverty and marginalisation, may be influencing the disproportionate impacts of an emergency*
- **Principle 3:** *consider how individuals and communities can be disproportionately impacted due to the indirect consequences or 'secondary effects' of an emergency*
- **Principle 4:** *consider how disproportionate impacts might change over time*
- **Principle 5:** *consider how response and recovery actions (by central government, community organisations or local authorities) may inadvertently create new forms of disproportionate impacts or exacerbate conditions for people already in precarious situations*
- **Principle 6:** *consider those who are not on Priority Service Registers (PSRs) or alternative public sector lists, who may be more or equally at risk*

Vulnerability is complex and non-static, the impacts of an emergency change over time and are influenced by other wider concurrent and contextual factors. 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. 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 impact on people 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 individuals and communities.



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. Since 2017, 47 British nationals have died in terrorism events, including most recently in the New Orleans vehicle attack and the Bondi attack in Australia.

Scenario

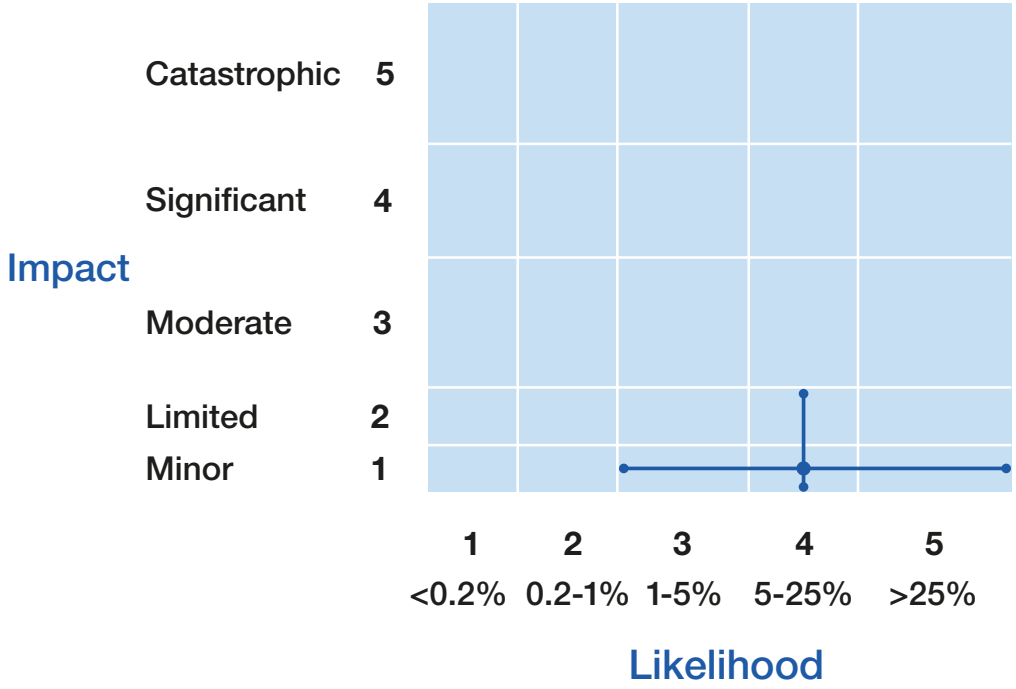
The reasonable worst-case scenario of this risk considers a large-scale terrorist attack occurring overseas, involving a significant number of British nationals. There would be casualties and fatalities, which would include a diverse range of visitor nationalities, including tourists.

Key assumptions for this scenario

This scenario assumes that a non-state actor, likely a known terrorist group, or an inspired self-initiated terrorist or group of people, is behind an attack.

Variations

The attack methodology could vary substantially which would impact the number of casualties and fatalities.



Response capability requirements

Government and Agencies. Host authorities would coordinate the immediate response. The Foreign, Commonwealth & Development Office (FCDO) would lead the UK government response, supported by stakeholders including Counter Terrorism Police. Capabilities required include resilient communications systems, humanitarian assistance, and victim support.

CNI and Wider Private Sector. Travel providers, insurers, and telecommunications operators support the response through customer identification, repatriation, medical logistics, and maintaining critical connectivity.

Voluntary Community and Faith Sector. Humanitarian organizations assist by delivering specialised victim support and welfare services to those affected.

Recovery

This event is less likely 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.

Impact on vulnerable people

Vulnerable individuals may be more likely to sustain physical or mental injuries during, or post-incident. Survivors may suffer from physical or mental health difficulties requiring enhanced support post-incident, some of which is provided through FCDO Consular support to victims and their families through approved providers.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

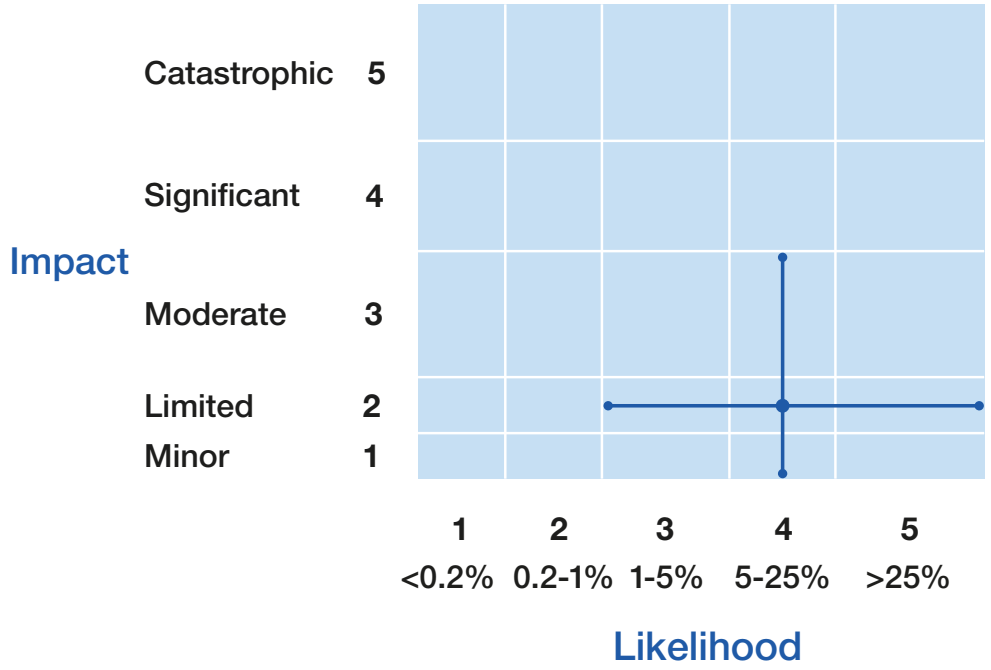
- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including government services and food)
- overseas response
- disruption to security
- potential changes to public behaviour
- impact on threat and risk assessments

Northern Ireland-related terrorism

The current threat level for Northern Ireland-related terrorism in Northern Ireland is substantial, meaning an attack is 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. Examples in 2026 include attacks at the Dunmurry police station and the Lurgan police station.

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

Government and Agencies. The Police Service of Northern Ireland (PSNI) leads the immediate security response, supported by other emergency services to treat casualties and secure the site. Regional and local government will coordinate the response and recovery.

CNI and Wider Private Sector. Utility and transport operators lead response to restore critical services, and manage disruptions to travel networks.

Voluntary, Community and Faith Sector. Organisations provide welfare support, mental and physical health support, logistic and communications, and search and rescue where applicable. This includes, but is not limited to, managing respite centres for evacuated residents, assisting with alternative accommodation and distribution of support and aid.

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.

Impact on vulnerable people

Vulnerable people such as the elderly, children, disabled individuals, foreign nationals (including immigrants/asylum seekers) and those with underlying health conditions would be affected by longer-term evacuation plans. VCFS organisations may have capacity to provide welfare support for vulnerable persons.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated and accommodated elsewhere
- disruption to essential services (including health, government services, transport, energy, emergency services, communications)
- disruption to business
- disruption to security, including perceived security threats
- potential changes in public behaviour

Terrorist attacks in venues and public spaces: explosive devices

An explosive attack can occur as a result of 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 strengthening 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, or on transport infrastructure. These scenarios would result in multiple fatalities and casualties, potentially exacerbated by structural collapse (enclosed areas), fire/smoke or fleeing crowds. An attack may temporarily impact utility supply, transport services and put pressure on emergency services.

Key assumptions

The scenario assumes the intention of the attack is to cause harm to people and/or infrastructure.

Variations

The attack could vary in the level of coordination. Attacks may form part of multiple coordinated incidents or may be singular events.

Response capability requirements

Government and Agencies. Emergency services coordinate the multi-agency response using Joint Emergency Services Interoperability Principles. Specialist capabilities like Explosive Ordnance Disposal, Urban Search and Rescue, and the Forensic Explosives Laboratory are deployed for scene safety, rescue, and investigation. Support for non-UK nationals may be required.

CNI and Wider Private Sector. Utility providers may be required to secure and repair damaged underground cables, pipes, and infrastructure affected by the explosion.

Voluntary, Community and Faith Sector. Humanitarian organizations and victim support structures assist by delivering specialised support and welfare services to those affected.

Recovery

Local, regional, and national victim support will be required. The short-term excessive hospital demand may cause delays for several weeks, while forensic investigations could disrupt communities for 1-2 weeks. There would be a potential impact, in the medium term, on the tourism industry and businesses in affected areas. Extensive damage to structures or transport infrastructure (such as tunnels) may cause long-term closures, utility disruption, and residential displacement.

Impact on vulnerable people

Individuals with physical disabilities or mobility issues may find evacuation difficult, particularly from complex environments like tunnels or damaged buildings. Noxious gases or smoke may disproportionately affect those with respiratory conditions. Groups associated with the perpetrator may face targeted hostility, regardless of any affiliation to the attack itself.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities
- disruption to essential services (including water supply, sewage management, education, health, transport, energy, emergency services, communications)
- potential need to assist people evacuating the site(s)
- disruption to security
- disruption to financial services
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘terrorist attacks in publicly accessible locations’ category is 4 (significant) and the average likelihood score is 5 (>25%).

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 UK examples include the 2017 London Bridge attack, where terrorists killed 8 people, the 2020 Reading attack, where a knife was used to kill 3 people, the 2025 Manchester synagogue attack, which resulted in the deaths of 2 people and the 2026 Golders Green attack which included the stabbing of 2 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. New legislation, the Terrorism (Protection of Premises) Act, also known as Martyn's Law, will also require those responsible for certain premises and events to take steps to reduce the risk of harm or, for larger venues, reduce vulnerability.

Scenario

The reasonable worst-case scenarios for marauding terrorist attacks in the assessment include the use of firearms or low-sophistication methods, such as vehicles and bladed weapons with the incidents taking place in a venue, public space or on transport infrastructure. 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.

Key assumptions

The scenario assumes the intention of the attack is to cause harm to people and/or infrastructure.

Variations

The attack could vary in the level of coordination. Attacks may form part of multiple coordinated incidents or be singular events.

Response capability requirements

Government and Agencies. The response is coordinated using Joint Emergency Services Interoperability Principles and MTA Joint Operating Principles. Specialist responders (e.g., armed police, Hazardous Area Response Teams, Fire and Rescue Service MTA teams) are deployed to neutralise the threat and treat casualties in high-risk environments. Local Resilience Forums' partners and devolved equivalents support wider consequence management.

CNI and Wider Private Sector. Venue operators and local businesses may need to initiate lockdown procedures, assist with site evacuation, and support police investigations. Transport providers may need to manage service disruptions.

Voluntary, Community and Faith Sector. Humanitarian organisations and victim support structures assist by delivering specialised support and welfare services to those affected, including support for non-UK nationals.

Recovery

Local, regional, and national victim support will be required. The short-term excessive hospital demand may cause delays for several weeks, while forensic investigations could disrupt communities for 1-2 weeks. Physical damage to transport infrastructure (such as tunnels) may be extensive and cause prolonged closures. There would be a potential impact in the medium term on the tourism industry and businesses in affected areas.

Impact on vulnerable people

Individuals with physical disabilities, the elderly, or the young may be less able to flee, increasing the risk of injury or death. Evacuation from complex environments like trains or vessels presents specific challenges for those with mobility issues or language barriers. Groups associated with the perpetrator may face targeted hostility, regardless of any affiliation to the attack itself.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities
- potential need for people to be evacuated
- disruption to essential services (including transport, education, energy, health and emergency services)
- disruption to security
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘terrorist attacks in publicly accessible locations category’ is 4 (significant) and the average likelihood score is 5 (>25%).

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. An example of global incidents of this nature include the bombing of the Superferry 14 in the Philippines in 2004. 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 in some scenarios may lead to the vessel partially 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.

Key assumptions

Contamination is limited and fuel and waste tanks of the vessel are not breached.

Variations

The scenario assumes that the fuel tanks of the vessel are not breached. If the scenario also involved the breaching of the fuel tanks this would significantly increase the environmental damage and economic cost of the incident.

Response capability requirements

Government and Agencies. HM Coastguard coordinates the search and rescue response, which may require military intervention in some scenarios. Medical professionals triage casualties, while the Victims of Terrorism Unit and the Foreign, Commonwealth and Development Office manage the administration of domestic and international victims.

CNI and Wider Private Sector. Port operators would help facilitate the evacuation and reception of passengers at the port.

Voluntary, Community and Faith Sector. Organisations provide mental health support and recovery victim support services to 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.

Impact on vulnerable people

This scenario would likely have a greater impact on the elderly, young children and those less mobile or with a physical disability. Consideration should be given to the fact that the separation of children from parents during evacuation may cause distress, and language barriers could hinder the communication of evacuation orders to non-English speakers.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, transport, energy, communications)
- contaminated environment or the presence of potentially hazardous materials
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'terrorist attacks on transport category' is 3 (moderate) and the average likelihood score is 3 (1-5%).

Malicious rail incident

The domestic rail network in Great Britain has historically been a target. More recently, there have been a number of notable attacks such as the London bombings on 7 July 2005 and 2025 Cambridgeshire train stabbing. 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 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.

Key assumptions

The scenario presumes this would be a no-notice attack.

Variations

The scenario could vary in the number of attacks, location, and attack methodology. A higher-impact scenario would involve a multiple concurrent incidents on a number of trains and/or stations, leading to a greater number of fatalities and damage to more rolling stock and infrastructure.

Response capability requirements

Government and Agencies. Emergency services lead the immediate response, deploying specialist teams (such as firearms officers) to neutralise threats and non-specialist responders to treat casualties and extract victims. The British Transport Police and local forces coordinate security and investigation, potentially requiring mutual aid to manage resources effectively.

CNI and Wider Private Sector. Rail operators provide access to the network and infrastructure to support the emergency response, while transport providers may need to arrange alternative travel for displaced passengers. Access to remote parts of the rail network would present a significant challenge and extend the initial response and recovery time.

Voluntary, Community and Faith Sector. Organisations assist by providing medium- to long-term psychosocial support for victims and their families.

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, during which time some rail services or routes may be unavailable. 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.

Impact on vulnerable people

Closures during police investigations will disproportionately impact those dependent on the railway for work, healthcare, or carer access. However, this may be mitigated to some extent by alternative transport provisions.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, education, health, transport)
- contaminated environment or the presence of potentially hazardous materials
- disruption to security
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘terrorist attacks on transport’ category is 3 (moderate) and the average likelihood score is 3 (1-5%).

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 and government also work 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, resulting in the deaths of all passengers and crew. The falling wreckage would disperse over a wide area, damaging ground infrastructure. 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. There would be significant domestic and international societal impacts, influenced by the public response.

Key assumptions

The scenario presumes this would be a no-notice attack in which the aircraft is brought down by an IED.

Variations

A higher-impact scenario would involve the wreckage falling on a densely populated urban area or multiple concurrent aircraft attacks, leading to a greater number of fatalities and damage to more buildings and infrastructure.

Response capability requirements

Government and Agencies. Emergency services lead the immediate response, deploying specialist teams to the scene. Mutual aid arrangements are likely to be required to support emergency services in managing the scale of the incident.

CNI and Wider Private Sector. Specialist contractors or industry partners support in providing decontamination expertise to clean up aviation fuel and hazardous debris.

Voluntary, Community and Faith Sector. Organisations assist by providing victim support for casualties and people nearby, including psychological treatment and support.

Recovery

In the reasonable worst-case scenario, significant time will be needed for the local area to recover depending on the nature and scale of debris, fire, and other damage. 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. Long-term effects would be felt by the aviation and wider tourism industry.

Impact on vulnerable people

An attack would have an indiscriminate impact in terms of fatalities. If there is significant damage on the ground due to wreckage, individuals with limited mobility or disabilities may be more adversely affected, and there could also be an increased risk of mental health trauma as a consequence. Separately, there could be societal impacts in response to an attack.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, education, transport)
- disruption to security
- contaminated environment or the presence of potentially hazardous materials
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘terrorist attacks on transport’ category is 3 (moderate) and the average likelihood score is 3 (1-5%).

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. The 1980 Iranian Embassy Siege serves as an example of this type of risk, where 26 people were taken hostage for up to 6 days on UK soil.

Scenario

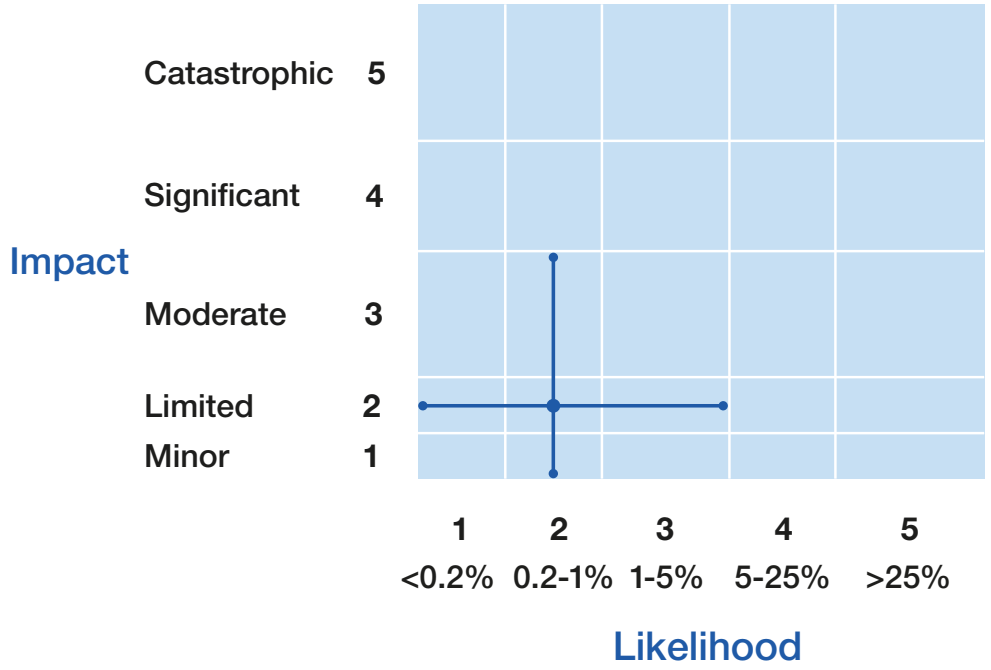
The reasonable worst-case scenario of this risk involves a group of people, potentially VIPs, being held hostage as part of a planned siege. Potential impacts include fatalities and casualties, damage to property and infrastructure, increased demands on the emergency services, disruption to essential services and economic damage. Public outrage at the perpetrator(s) would be significant and widespread. There is likely to be a large international media presence and coverage of the siege.

Key assumptions

Hostage taking is carried out for a variety of reasons which can include raising awareness of key issues or attempting to leverage policy decisions.

Variations

The attack methodology could vary, which could impact the length and impact of the siege.



Response capability requirements

Government and Agencies. The Joint Emergency Services Interoperability Principles enable a coherent multi-agency response. Specialist responders, including 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, deploying from key locations across the country.

CNI and Wider Private Sector. Owners and operators of venues or infrastructure involved would need to support police operations, potentially providing site plans, access, or CCTV footage to assist the response.

Voluntary, Community and Faith Sector. Organisations would be required to provide victim support and welfare services to hostages and their families during and after the incident.

Recovery

The international standing of the UK, and its ability to project soft power, may be impacted depending on how the situation is handled. Physical and psychological support for victims and their families will be required, alongside long-term mental health support for victims.

Impact on vulnerable people

Those with physical disabilities, the elderly, or young may be less able to flee from an attack, increasing injury or risk of death. Depending on the siege duration, individuals with ongoing medical requirements may be disproportionately impacted.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, transport and education)
- disruption to security
- potential changes in public behaviour

Assassination of a high-profile 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 15 October 2021 at a constituency surgery in Leigh-on-Sea.

Scenario

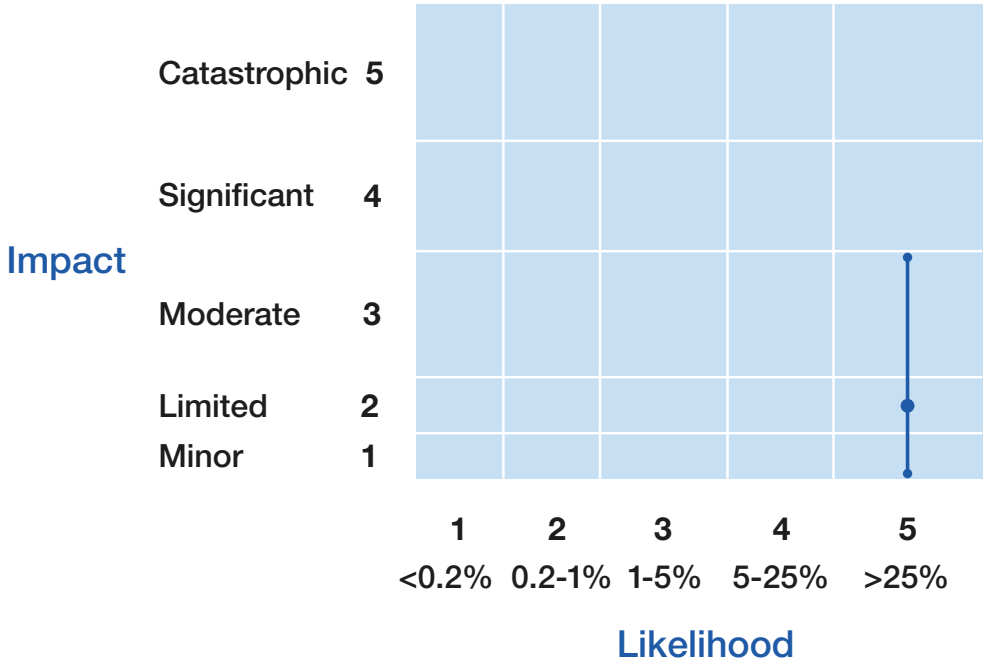
The reasonable worst-case scenario for this risk concerns the assassination of a high-profile public figure. There is also the potential for a small number of casualties in close proximity to the intended target. This high-profile target would be attacked because of the symbolic value and therefore there 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 as well as diplomatic repercussions. Some initial, short-lived anger may be felt about the inability to protect such a high-profile figure.

Variations

This scenario could vary depending on who is targeted and the operational arrangements around their security.



Response capability requirements

Government and Agencies. A suite of protective security measures are managed by the government, including police protection and the provision of specialist security advice to mitigate the risk.

CNI and Wider Private Sector. Venue operators and security companies may be required to support the police by implementing technical security measures and facilitation measures to decrease vulnerabilities at locations visited by high-profile figures.

Voluntary, Community and Faith Sector. Organisations may provide support to witnesses and bystanders affected by the incident and assist in maintaining community cohesion following public outrage.

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.

Impact on vulnerable people

An attack against a principal holding a protected characteristic could have a significant societal impact and lead to heightened feelings of vulnerability for those sharing this characteristic. Similarly, if the attacker holds a protected characteristic, members of that community may feel more vulnerable as a result of sharing that characteristic.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including government services, emergency services and transport)
- disruption to security
- potential changes in public behaviour

Chemical, Biological, Radiological and Nuclear (CBRN) attacks

Malicious actors including terrorists, states or criminals remain interested in CBRN attack methods. Current assessments suggest terrorists are more likely to use conventional attack methodologies, however, a CBRN attack cannot be ruled out. Fortunately, the UK has not suffered a large-scale CBRN attack, but emergency services respond to small-scale events that include hazardous materials regularly. In the UK, there have been two high-profile malicious CBRN attacks in recent history. 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 continually working to improve the response and improving methods to detect and monitor CBRN materials, including at the UK border, and by limiting access to hazardous materials and their precursors.

Scenarios – Chemical, Biological, Radiological and Nuclear

The scenarios included in the assessments involve the release of a toxic chemical, dispersal of a biological agent or dissemination of radiological material into a widespread area, and a nuclear event. All scenarios in the assessments could result in potentially large numbers of casualties and fatalities and with all scenarios there is the potential for significant economic damage.

Response capability requirements

Government and Agencies. Emergency services provide an Initial Operational Response to save lives and minimise harm before specialist elements arrive. Specialist operational response teams, supported by CBRN resources, manage the scene and hazard, providing further lifesaving actions such as mass decontamination and specialist medical treatment. Emergency services coordinate the multi-agency response using Joint Emergency Services Interoperability Principles. Local authorities support wider consequence management, while public health bodies may coordinate wider health responses, as necessary. Government would coordinate nationally if required.

CNI and Wider Private Sector. Specialist contractors may be required to support the remediation of land, property, and infrastructure, depending on the scenario.

Voluntary, Community and Faith Sector. Organisations can helpfully assist by providing long-term psychosocial support to affected individuals and communities, as well as practical and humanitarian aid during evacuation or displacement.

Recovery

Both the immediate remediation and longer-term recovery from a CBRN attack could be time-consuming and costly, depending on the nature of the material dispersed. In some scenarios there could be long-term environmental hazards that may be difficult to fully remediate, necessitating the adaptation to a new normal.

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.

Impact on vulnerable people

A number of vulnerable people may face a disproportionate risk of the physiological effects of chemical, biological, radiological or nuclear exposure. This includes those with underlying health conditions such as respiratory disease, the very young and elderly, those less able to follow the instructions of the attending emergency services due to language barriers, those with physical and visual impairments and those reliant on assistance animals that may also be impacted. Vulnerable people may need enhanced support from the emergency services during evacuation and decontamination processes to ensure their safety. Some people may be permanently or temporarily displaced due to the damage and contamination of their homes, loss of house keys, phones or means of payment which have become contaminated. Some vulnerable people will not always have access to alternative transport or housing and may require assistance from the local authorities until they can return home safely.

Common consequences

Bespoke planning for some of these risks is done at a national level due to the catastrophic scale of the impacts, and this planning utilises national and local capabilities where practicable.

The exact consequences of a CBRN event will be dependent on the nature of the attacks, but could include the following:

- human health impacts, which may include a large number of fatalities and casualties and those who need ongoing, mental health support
- some people are likely to be sheltered and/or evacuated
- overseas impact or reaction e.g. loss of confidence in tourism
- minor to catastrophic destruction or disruption to essential services including health, food, government services, emergency services, water supply, sewage management services
- a contaminated environment or the presence of hazardous materials for significant periods of time
- changes in public behaviour e.g. avoidance of the locality in the medium term or of specific associated contexts with knock-on impacts on services and spending patterns

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘larger-scale CBRN attacks’ category is 5 (catastrophic) and the average likelihood score is 1 (<0.2%). The average impact score for risks grouped under the ‘medium-scale CBRN attacks’ category is 4 (significant) and the average likelihood score is 3 (1-5%). The average impact score for risks grouped under the ‘smaller-scale CBRN attacks’ category is 2 (limited) and the average likelihood score is 4 (5-25%).

Conventional attack: gas infrastructure

Great Britain has a highly resilient gas network and a conventional attack on gas infrastructure has never occurred in Great Britain. 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). 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 National Gas 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 low-sophistication attack on gas infrastructure which results in a significant loss of gas supply capacity to Great Britain. This would cause a national shortfall of gas supply, requiring emergency measures to balance the gas network. While domestic gas customers and some critical users are prioritised from gas disconnection, the majority of industrial gas users, including electricity generators, will be instructed to cease taking gas, causing significant cascading impacts. 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 may be required to balance supply and demand. This could affect between 1 and 11 million customers for a period of over two months. While domestic gas supply is maintained, widespread power cuts would pose significant risks to public health and welfare, particularly for those reliant on electrically powered medical equipment or heating controls**.** Within this process, some critical sites would be protected from electricity 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.

Key assumptions

The attack occurs during an extended period of cold weather across Europe, maximising the reliance of gas supplies and the subsequent impacts.

Response capability requirements

Government and Agencies. The government and emergency services activate established response plans (such as the National Emergency Plan for Downstream Gas and Electricity) and the Electricity Supply Emergency Code (ESEC) to manage wider recovery.

CNI and Wider Private Sector. There would need to be preparations in place to support wider recovery and the continued operation of critical infrastructure, including those in health, such as hospitals, and fuel distribution, potentially utilising backup generators to maintain services to critical sites.

Voluntary, Community and Faith Sector. Organisations work alongside Local Resilience Forums' partners and Gas and Electricity Network providers to provide support to vulnerable people, particularly those on the Priority Service Register who may be affected by power cuts or heating loss.

Recovery

Restoration of the affected gas infrastructure could take approximately 3 months. However, rolling power cuts would likely end sooner than this, once the gas shortfall is resolved through other supply points or weather changes to support renewable generation. It would take a further week for industrial gas customers to be fully restored and weeks or months for some industrial sites to return to normal service.

Impact on vulnerable people

No domestic gas customers will lose supply, but all domestic customers are at risk of being disconnected from electricity supply. Customers will receive advanced notice of any rolling outages that can ensure preparations can be made. During outages, customers on the Priority Service Register, including those reliant on continuous electricity supply for medical needs, will receive tailored support from their energy network providers and Local Resilience Forums' partners. The provision of additional welfare provisions such as hot meals and alternative accommodation during the rolling outages (approximately 3-hours at a time) will be assessed based on customer needs, but will also be limited by the widespread nature of the disruption.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities - saving lives and alleviating suffering is a top strategic priority
- contaminated environment or the presence of potentially hazardous materials
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, communications, water supply and sewage, education)
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'conventional attacks on infrastructure' category is 4 (significant) and the average likelihood score is 3 (1-5%).

Cyber attack: gas infrastructure

Gas infrastructure may represent a potential target for cyber attacks. Our critical operators that meet the relevant thresholds are in scope of the Network and Information Systems Regulations 2018, mandating them to adhere to certain cyber security requirements. 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. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the energy sector will continue to monitor how current and emerging AI influences this risk.

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 to gas-fired power stations. Disconnecting gas supply to electricity power stations could cause a shortfall in electricity generation. In the event of a prolonged electricity supply shortfall, action would be taken either to restore the network and/or balance supply and demand. Within this process, some critical sites could 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.

Key assumptions

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, and would worsen impacts on society.

Response capability requirements

Government and Agencies. The government and emergency services activate established response plans (such as the National Emergency Plan for Downstream Gas and Electricity) to manage wider recovery.

CNI and Wider Private Sector. Critical infrastructure operators, including those in telecommunications and fuel distribution, would aim to ensure continued operation, potentially utilising backup generators to maintain services to critical sites.

Voluntary, Community and Faith Sector. Organisations work alongside Local Resilience Forums' partners to provide support to vulnerable people, particularly those on the Priority Service Register who may be affected by power cuts or heating loss.

Recovery

Restoration of the affected gas infrastructure could vary significantly depending on the sophistication of the attack and the extent of the damage caused.

Impact on vulnerable people

Vulnerable customers will receive support from Local Resilience Forums' partners but this is expected to be hindered by the widespread nature of the disruption. In the interim, critical sites (such as hospitals) will be supplied by operational back-up generators.

Common consequences

Bespoke planning for these risks is done at a national level due to the potentially catastrophic scale of impacts. Planning draws on national and local generic capabilities. The exact consequences will be dependent on the nature of the attack, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including health, government services, food, transport, communications, water supply and sewage, cyber)
- loss of or disruption to Global Navigation Satellite Systems
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on Infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Conventional attack: electricity infrastructure

Great Britain 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 Ukraine, 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 National Energy System Operator (NESO) 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 concurrent explosive attacks against electricity infrastructure in an urban area. This would lead to multiple fatalities and a loss of electricity output from the infrastructure instantly, resulting in power outages of approximately 1.5 million people, including essential services without back-up generation, in the region of the attacks. Due to the significant loss of demand on the network, an electricity system imbalance will occur and as a result, emergency procedures (Low Frequency Demand Disconnection) would take place immediately, automatically disconnecting 5% (1.5 million) of consumers spread across the entire GB network. This emergency measure is to avoid worsening impacts and national disconnections would be restored within 2 hours. The National Energy System Operator control room would utilise system mechanisms to take mitigating action in the immediate aftermath of the attacks, re-balancing the local network and restoring customers in the vicinity of the attack within 14 days, with customers gradually restored over this period.

Key assumptions

The low sophistication attack takes place during winter in an urban area where the number of connected customers is higher.

Variation

The conventional attack on electricity infrastructure occurs in the summer.

Response capability requirements

Government and Agencies. The government and emergency services activate established response plans (such as the National Emergency Plan for Downstream Gas and Electricity) to manage wider recovery.

CNI and Wider Private Sector. There would need to be preparations in place to support wider recovery and the continued operation of critical infrastructure, including those in health, such as hospitals, and fuel distribution, would ensure continued operation, potentially utilising backup generators to maintain services to critical sites.

Voluntary, Community and Faith Sector. Organisations work alongside Local Resilience Forums' partners to provide support to vulnerable people, particularly those on the Priority Service Register who may be affected by power cuts or heating loss.

Recovery

Nationally disconnected customers would be restored within 2 hours. The vast majority of customers would be restored within 2 days. However, for customers in the immediate vicinity of the attack, restoration could take up to 14 days. There is likely to be cascading impacts to essential services such as transport and health following the outages. It could take 6-12 months for the affected infrastructure to be fully repaired, reducing the resilience of the network during this time which may result in some frequent but short-term electricity outages until the infrastructure is fully repaired.

Impact on vulnerable people

Customers on the Priority Services Register will receive additional support to help cope with cascading impacts, including welfare provisions to support vulnerable people who have lost power, such as food vouchers, accommodation and tailored support to meet their needs. Welfare provisions are expected to also focus on those customers in the vicinity of the attack however may be hindered by emergency services management of the impacted area of the attack, for example managing people coming in and out of the area. The Energy Networks Association (ENA) has a free-to-dial 105 service which connects consumers experiencing power outages to their local network operator and the GOV.UK Prepare website has a dedicated sector for power outage preparation.

Common consequences

The exact consequences will be dependent on the nature of the attack, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- contaminated environment or the presence of potentially hazardous materials
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, communications, water supply and sewage)
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘conventional attacks on infrastructure’ category is 4 (significant) and the average likelihood score is 3 (1-5%).

Cyber attack: electricity infrastructure

The National Electricity Transmission System (NETS) transports electricity across Great Britain. Our critical operators that meet the relevant thresholds are in scope of the Network and Information Systems Regulations 2018, mandating them to adhere to certain cyber security requirements. A cyber attack may involve disrupting or damaging critical systems leading to the failure of the NETS and a National Power Outage (NPO). A failure of the electricity supply has the potential to severely disrupt all other critical sectors, resulting in greater consequences than smaller scale 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 and the National Energy System Operator (NESO). AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the energy sector will continue to monitor how current and emerging AI influences this risk.

Scenario

The reasonable worst-case scenario is based on a malicious cyber attack on a critical electricity system, leading to an NPO. 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, and would worsen impacts on society.

Response capability requirements

Government and Agencies. Emergency services and government bodies would coordinate to support wider recovery and maintain resilient communications systems to manage the response effectively.

CNI and Wider Private Sector. The National Energy System Operator is legally required to have a plan to restore the electricity network in the event of a National Power Outage.

Voluntary, Community and Faith Sector. Organisations assist by providing humanitarian assistance and victim support to help populations cope in the immediate aftermath of the incident.

Recovery

If there are no additional complications as a result of the cyber attack, 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 at least 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.

Impact on vulnerable people

It is not possible for any customer's electricity supply to be prioritised during a National Power Outage. Customers on the Priority Service Register will receive support from Local Resilience Forums' partners but this is expected to be hindered by the widespread nature of the disruption.

Common consequences

Bespoke planning for these risks is done at a national level due to the catastrophic scale of impacts. Bespoke planning will draw on national and local generic capabilities.

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including health, government services, food, transport, communications, water supply and sewage, cyber)
- contaminated environment or the presence of potentially hazardous materials
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Conventional attack: civil nuclear

The civil nuclear sector is of strategic importance to the UK's national security, energy resilience and clean energy transition. The UK's civil nuclear industry covers a broad spectrum of the nuclear fuel cycle, including fuel enrichment and fabrication, electricity production, transportation of nuclear materials and nuclear waste management. Within the UK, and in line with international good practice, an independent regulator holds operators to account. The Office for Nuclear Regulation requires site licensees 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 chosen scenario is extremely unlikely. It is based on a physical attack at a UK civil nuclear installation resulting in radiological contamination beyond site boundaries. 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

A scenario could occur in which a lesser percentage of inventory could be released, and it could also occur at a different UK civil nuclear installation.

Response capability requirements

Government and Agencies. Local Resilience Forums' partners have a collective responsibility to plan, prepare and communicate in a multi-agency environment. Interagency coordination must be exercised to minimise the impact of incidents on local communities and dovetail with national incident management objectives. A robust communication strategy will be required to minimise misinformation and disinformation.

CNI and Wider Private Sector. Nuclear site operators and transport carriers are responsible for maintaining robust security measures to defeat advanced attacks and must implement immediate protective actions to safeguard health and safety.

Voluntary, Community and Faith Sector. Organisations assist by providing support to vulnerable people, particularly those with pre-existing medical conditions who may need extra help with evacuation or face difficulties due to reduced fuel availability.

Recovery

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

Impact on vulnerable people

Vulnerable people with pre-existing medical conditions may be more vulnerable to effects of exposure (e.g. to smoke and fumes) and they may need extra support with evacuation. Reductions in fuel availability could impact ability for vulnerable people to receive continued care across regional and rural areas. In addition, vulnerable or stigmatised communities may be deliberately targeted by mis/disinformation campaigns online, particularly via social media, increasing the public's exposure to harmful narratives.

Common consequences

The exact consequences will depend on the nature of the incident, but this could include:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- contaminated environment or the presence of potentially hazardous materials
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, communications, water supply and sewage)
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘conventional attacks on infrastructure’ category is 4 (significant) and the average likelihood score is 3 (1-5%).

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 deliberate sabotage of a critical part of the UK's downstream 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. The fuel sector would take time to adapt fully to the temporary or permanent loss of a critical asset. News of the attack could lead to adaptive purchasing by the public, creating further fuel supply disruption beyond the immediate capability of the government or industry to fully mitigate.

Key assumptions

News of the attack would become public knowledge and adaptive purchasing could cause or exacerbate a national fuel supply incident.

Variations

An alternative, less likely scenario involves the use of remote attack methods (e.g. drones).

Response capability requirements

Government and Agencies. A multi-agency response is vital to address immediate threats to life and environmental hazards, such as oil spills. The government may use measures to assist industry in recovering supply, for example deploying military personnel to make fuel deliveries, or providing additional tanker capacity. If required by the severity of the situation, emergency powers are available under the Energy Act 1976 to manage supply and demand.

CNI and Wider Private Sector. The downstream oil industry works in coordination with the government and Local Resilience Forums' partners to manage impacts on supply. Operators are responsible for resuming operations at affected sites to allow fuel stocks to recover.

Voluntary, Community and Faith Sector. Organisations work alongside Local Resilience Forums' partners to provide support to vulnerable people who may be affected by disruption to the supply of transport and heating fuels.

Recovery

Once operations at the affected site have resumed, fuel stocks would be expected 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, extent of adaptive purchasing (if any) and demand levels.

Impact on vulnerable people

Vulnerable people with pre-existing medical conditions may be more susceptible to the effects of smoke and fumes if the attack results in a fire, and may need extra support with evacuation. Additionally, vulnerable people could be disproportionately exposed to the impacts of disruption to the supply of transport and heating fuels, especially where there is a direct reliance on fuel supply to access health services or generate income.

Common consequences

The exact consequences will be dependent on the nature of the attack, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, communications, water supply and sewage, energy, education)
- contaminated environment or the presence of potentially hazardous materials
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'conventional attacks on infrastructure' category is 4 (significant) and the average likelihood score is 3 (1-5%).

Cyber attack: fuel supply infrastructure

A cyber attack on the UK's fuel supply infrastructure could have implications for UK fuel production or distribution. Our critical operators that meet the relevant thresholds are in scope of the Network and Information Systems Regulations 2018, mandating them to adhere to certain cyber security requirements. However, threats in this space are evolving at pace and so it is a risk that government monitors closely. Historically, fuel supply disruptions in the UK have been significantly exacerbated by adaptive purchasing, which can deplete stocks faster than the initial disruption itself. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the energy sector will continue to monitor how current and emerging AI influences this risk.

Scenario

The reasonable worst-case scenario is based on a disruptive, coordinated cyber attack on a system critical to the UK's fuel distribution and supply, impacting multiple sites simultaneously. Some regions would be significantly impacted, but there would be increased output from unaffected terminals and refineries to balance this.

Key assumptions

Fuel disruption as a result of the cyber attack itself is minor, however, adaptive purchasing behaviours could result in significant shortages. The Department for Energy Security and Net Zero (DESNZ) may deploy non-emergency fuel supply mitigation measures. Disruption could last for at least 5-10 days.

Response capability requirements

Government and Agencies. The government could activate contingency plans listed in the National Emergency Plan for Fuel. For example, deploying military personnel to make fuel deliveries or providing a reserve fleet of fuel tanker vehicles to industry.

CNI and Wider Private Sector. Industry operators work to readjust supply routes once operations at the affected site have resumed.

Voluntary, Community and Faith Sector. Organisations may assist in ensuring vulnerable people receive continued care, particularly those living in regional and rural areas where alternative transport or heating options may be limited.

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.

Impact on vulnerable people

Reductions in fuel availability could impact the ability for vulnerable people to receive support, particularly those living in regional and rural areas where alternative transport or heating options may be limited.

Common consequences

The exact consequences will be dependent on the nature of the attack, but this could include potential changes in public behaviour and disruption to essential services (including health, energy, emergency services, transport, water supply and sewage).

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on Infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Attack on a government building

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. This risk focuses specifically on physical, conventional attacks against the government estate.

Scenario

The reasonable worst-case scenario involves a targeted explosive attack on a government building in the Whitehall area of central London. This would cause significant damage to the building and surrounding infrastructure, resulting in fatalities and casualties in the immediate vicinity, including trauma and crush injuries and those caused by flying glass and debris. Buildings could suffer total loss and partial collapse.

An attack on government assets could also 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; the possibility of reputational damage for the UK overseas and the loss or compromise of sensitive information held by the government.

Key assumptions

The attack takes place during working hours causing a considerable loss of life.

Variations

An attack on a government building outside of London would have a different impact.

Response capability requirements

Government and Agencies. Central government functions coordinate business continuity and the immediate response, supported by the Metropolitan Police and local authorities. Emergency services and the military deploy specialist capabilities, including search and rescue, armed response, and bomb disposal teams.

CNI and Wider Private Sector. Specialist contractors and engineering firms may be required to support the complex recovery operation, including assessing structural damage and clearing debris from partial collapses.

Voluntary, Community and Faith Sector. Organisations may be required to assist by providing immediate and longer-term mental health support to survivors and witnesses to help manage the psychological impact of the event. Long term, the sector will assist in design works of any damaged historic and cultural assets.

Recovery

Affected buildings could suffer severe structural damage or partial collapse, requiring a complex recovery operation that could take years to complete. 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, especially if the attack was on a critical government building.

Impact on vulnerable people

In the event of an attack, all individuals within the affected buildings would be considered vulnerable. Specific evacuation plans are essential for those with physical impairments or mobility issues to ensure their safe exit. Survivors and witnesses would likely require access to immediate and longer-term mental health support to manage the psychological impact of the event.

Common consequences

The exact consequences will be dependent on the nature of the attack, but could include:

- potential human health impacts, such as physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including government services)
- disruption to security
- disruption to public transportation services
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘conventional attacks on infrastructure’ category is 4 (significant) and the average likelihood score is 3 (1-5%).



Cyber

Cyber attack: health and social care system

The health and social care system remains a target for cybercriminals. In December 2025, DXS International which provides healthcare technology for 2000 GPs in the NHS disclosed a cyber attack, and in August 2025, the criminal group, known as Cl0p, stole files from Barts Health NHS Trust's database, including names, addresses, and invoices of patients and staff who had paid for treatment or services over several years. In 2023 the Cyber Security Strategy for Health and Social Care was published and sets out a plan to promote cyber resilience across the sector by 2030. AI is increasing the scale, speed and volume of cyber attacks - making existing threats such as phishing and ransomware more frequent and effective. Barriers to entry are falling, enabling less-skilled actors to carry out more sophisticated attacks and expanding the overall threat landscape. Social engineering is becoming harder to detect, as AI-generated messages remove traditional warning signs and increase the likelihood of users falling victim to well-crafted attacks. AI is accelerating the discovery and exploitation of vulnerabilities, reducing the time organisations have to respond. The widespread adoption of AI is also expanding the attack surface and systemic risk, particularly through complex systems and emerging "agentic AI", where autonomy, access, and unclear ownership can significantly amplify the impact of failure.

Scenario

The reasonable worst-case scenario would involve widespread disruption to the health and care sector due to systemic ransomware attack. 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.

Key assumptions for this scenario

The ransomware is expected to spread rapidly from the initial infected organisation to other organisations. All data systems, services and points across the sectors outlined, including critical national infrastructure systems, are within scope of this scenario.

Variations

Localised disruption to the health and care sector due to a ransomware attack against a limited number of NHS Trust(s). Targeted attack against emergency services sectors (Police, Fire, Ambulance, Coastguard) to cause national disruption.

Response capability requirements

Government and Agencies. At the local level, additional staff will be required to handle paper records and rearrange appointments. Clinical support will be required to provide advice due to loss of care records and services (e.g. 111). At the national level, Cyber Incident Response Retainer (CIRR) has been established to cover key national systems and address the immediate impacts, and specialist communications should be engaged quickly to provide key information to patients and media.

CNI and Wider Private Sector. Private companies involved would be those who regularly provide the NHS specialist IT support. They may be drawn upon to help address the immediate impacts of the incident.

Voluntary, Community and Faith Sector. Given the strain of the health and social care system, volunteers would assist by supporting impacted vulnerable people. This will aid recovery.

Recovery

There is likely to be a significant recovery time across the whole health and social care system. Return to normal service use is characterised by a phased return of priority service functions over several months. This is dependent on the type of attack and the different levels of resilience across the cyber system.

Impact on vulnerable people

As health and care provision becomes strained, the main vulnerable people impacted include those with long term sickness, elderly people, those who are pregnant, children and young people and those with mental health challenges. Principally the disruption to prescriptions is likely to impact the sick and elderly. Whilst, the disruption to appointments is likely to impact those with mental health challenges, pregnant people and children.

Common consequences:

The exact consequences will be dependent on the nature of the cyber attack; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, government services, health)
- disruption to cyber services
- disruption to security
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).

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. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the transport sector will continue to monitor how current and emerging AI influences this risk.

Scenario

The reasonable worst-case scenario for a cyber attack targeting one mode of transport. This may be maritime, aviation or land transport such as rail or road. All of these risks would have different consequences. For illustrative purposes, an attack on the rail network has been used as the reasonable worst-case scenario. This scenario is a significant ransomware attack targeted directly at a rail operator, undertaken by a sophisticated actor, which compromises and results in loss of critical systems. This would result in cumulative disruption that could last for at least a week following systems becoming operational again as backlogs are cleared. There could also be a significant impact to domestic movement, disruption to public services and economic impact in the UK until services can be restored.

Key assumptions for this scenario

The scenario assumes that the attack will lead to disruption to rail passenger movements and freight and cargo facilitation at multiple key transport CNI sites in the UK for at least a week. Knock-on impacts to other modes of transport as passengers and cargo switch may be a possibility.

Variations

The threat or risk to rail is not assessed as any more likely than a similar attack against road, maritime or aviation. Equally plausible scenarios could include cyber attacks targeting other modes of transport such as aviation or maritime that would result in delayed and cancelled services.

Response capability requirements

Government and Agencies. The government incident response will be managed by DfT and the National Cyber Security Centre and other Lead Government Departments where needed; with Cabinet Office coordination if required. This may require a surge in cyber security, policy/operations and communications staff drawn from across government. Locally, emergency transport options may be required for stranded passengers with LRFs required to manage local impacts.

CNI and Wider Private Sector. Transport operators affected would lead the operational response to the incident including service updates to passengers.

Voluntary, Community and Faith Sector. Organisations could support by providing transportation support to those with physical and mobility impairments.

Recovery

The immediate systems recovery could take weeks to months depending on the nature of the attack. Any impacts on critical goods supply chains could require a bespoke response to ensure effective movement of goods. The cost of recovery of cyber incidents can run into the billions, which may have long-term commercial viability impacts. LRFs may be required to support with disruption to passengers.

Impact on vulnerable people

This may include those who require rail travel to attend health or social care appointments; those with physical and mobility impairments (including those who cannot drive); children, young people and those in education who rely on rail services; digitally excluded and minority speakers or those with other communication needs; carers may not be able to fulfil their caring role and tourists who are less able to make alternative arrangements. This could be exacerbated the longer the disruption continues.

Common consequences

The exact consequences will depend on the nature of the cyber attack; this could include some of the following:

- disruption to essential services (including transport, food, health)
- disruption to security
- disruption to cyber services
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).

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. 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. Artificial intelligence may affect the nature and delivery of cyber threats, for example by enabling aspects of cyber activity to be conducted faster, at greater scale, or both. The government will continue to monitor how current and emerging uses of AI could influence this risk.

Scenario

A disruptive and sophisticated cyber attack against a third-party Managed Service Provider (MSP) used by many UK telecommunication operators, would affect millions of customers. 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. It is expected that most customers will be reconnected in 24 hours, but depending on the nature of the attack, disruption could last for up to 72 hours, but could extend into weeks or months.

Key assumptions for this scenario

The cause and extent of network disruption may not be known immediately. Certain actors have displayed capabilities to attack telecoms networks, and would likely conduct offensive cyber activity during periods of heightened political tension or conflict.

Variations

There are numerous variations of this risk in terms of attack vectors, scale, services and sectors impacted, and length of disruptions.

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Telecommunications 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.

Voluntary, Community and Faith Sector. Voluntary sector support to vulnerable people would aid recovery.

Recovery

It is expected that most customers would be reconnected within 24 hours, although disruption could last for up to 72 hours. Communications recovery timeframes are expected to be longer for other impacted CNI sectors.

Impact on vulnerable people

Disruption to telecommunications services would prevent vulnerable people (e.g. the elderly or those with pre-existing health conditions) from contacting 999/112 or other forms of support. During disruption vulnerable people will need additional support.

Common consequences

The exact consequences will dependent on the nature of the cyber attack; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including government services, food, education, health, water supply, sewage management, energy, transport, communications)
- disruption to security
- disruption to business
- disruption to cyber services
- disruption to financial services
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Cyber attack: data infrastructure

Data centres host and support the digital infrastructure that underpins modern life, from patient records and emails to product data and financial systems. Data centres were designated as a critical national infrastructure sub-sector in 2024, putting data centres on an equal footing as water, energy and emergency services systems. Under the UK's Cyber Security and Resilience Bill, data centres will be regulated as essential services, providing government and the regulator with the necessary levers to oversee and support the sector, ensuring consistent protection and enabling secure growth. Emergent AI Models can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government will continue to monitor how current and emerging AI influences this risk.

Scenario

A disruptive and sophisticated cyber attack against one or more colocation UK data centres, allowing the exfiltration of data, customer information, intellectual property, or operational details held in the data centres, with the potential to impact millions of customers. As data centres host, store and transfer data to multiple organisations there would be significant downstream impacts. Data held could include personal data, such as bank information, health records, and addresses, or host essential services for one or multiple critical national infrastructure sectors. This could also lead to Cloud service providers being offline as they rely on colocation data centres. Depending on the nature of the attack, the attack itself may last 2-7 days, but disruption would last months, and it may take years for full service to resume.

Key assumptions

A successful cyber attack can occur at any time, and is not limited to a specific location, and effects will be felt across all regions of the UK.

Variations

There are numerous variations of this risk in terms of attack vectors, scale, services and sectors impacted, and length of disruptions. Similar disruptions could also occur from issues other than a cyber attack, such as a national state attack during conflict, accidental disruption, power outage, heatwaves or domestic attack by protestors.

Response capability requirements

Government and Agencies. The Department for Science, Innovation and Technology and the National Cyber Security Centre will lead the response. The overall handling process is underpinned by the Cabinet Office Cyber Incident Management Plan in conjunction with NCSC and DSIT cyber incident processes. Local authorities are also likely to be involved.

CNI and Wider Private Sector. Since most data centres are owned by private entities, the responsibility is ultimately on firms, though the government can support in a crisis. Firms are encouraged to improve their cyber security and resilience as prevention measures and ensure robust response and business continuity plans are in place.

Voluntary, Community and Faith Sector. Generalist, and welfare and communications support could assist recovery.

Recovery

Disaster recovery would take several days to weeks before restoration could commence. Services operated by customers would start whenever they felt it was necessary and safe to do so. If the attack has a ransomware component, then recovering information may not be feasible as recent incidents show that the information is deleted or sold on the dark web. It will take years for information to be restored if data is compromised or destroyed.

Impact on vulnerable people

The effects of the successful cyber-attack could indirectly harm vulnerable people depending on the nature of services hosted at the data centre, and vulnerable individuals may be disproportionately affected, due to their reliance on digital systems for essential services.

Common consequences

The exact consequences will be dependent on the specific nature of the cyber attack; this could include some of the following:

- disruption to essential services (including education)
- disruption to security
- disruption to cyber services

We expect this risk to link to other planning assumptions. We are developing our knowledge of the risk impacts as it is a new CNI sub-sector.

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Cyber attack: water infrastructure

The water sector is increasingly reliant on digital systems, known as Operational Technology (OT), to manage the treatment and distribution of water. While this connectivity improves efficiency, it introduces the risk of disruptive cyber attacks. A successful attack on these systems could disrupt water supplies and wastewater services, mirroring the impact of physical infrastructure failures. OT has been affected by cyber incidents before, with recent examples being a compromise of OT in the energy sector in Poland in December 2025 and the disruption to waterworks in Denmark in 2024. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry.

Scenario

The reasonable worst-case scenario assumes an advanced cyber actor infiltrates the OT systems of a water company. The attacker deploys malware that erases critical data and disables key components controlling essential operational functions. This results in the water company losing visibility and control of its systems, causing a major disruption to water supply and wastewater services for a large population.

Key assumptions

The scenario assumes the event takes place in London and impacts a population of over 1 million people.

Variations

The following variations have been considered as part of this scenario: scale of organisation impacted; actor responsible; motivations for the attack; time of year; changes to water quality; scale of impact across the company.

Response capability requirements

Government and Agencies. A significant logistical operation is needed to manage the shortage, potentially requiring military assistance to supplement resources. Security personnel are required to protect water bowsers and tankers from theft and misuse.

CNI and Wider Private Sector. The water industry mobilises Alternative Water Supplies (AWS) and additional tankers, as part of their contingency plans for disruptive scenarios. However, maintaining an alternative water supply at this scale would present significant logistical challenges, requiring infrastructure and personnel resources beyond standard operational capabilities. Operators lead the complex technical recovery to replace or reconfigure compromised digital systems.

Voluntary, Community and Faith Sector. Volunteers are required to support a significant logistical operation, specifically assisting with the distribution of supplies at large numbers of bottled water stations.

Recovery

A return to full functionality could take several months. Unlike physical repairs, recovery involves complex digital challenges: many OT components are specific to the facility and may require full replacement or reconfiguration. Furthermore, the water company would need assurance that the attacker has been completely removed from the network, requiring rigorous isolation and testing of all systems before services can be safely restored.

Impact on vulnerable people

Priority for Alternative Water Supplies would be given to those on the Priority Services Register (PSR) and essential institutions. Hospitals, prisons, and care homes would be treated as top priorities for tanker deliveries. However, due to the scale of the incident, demand for water is expected to outstrip the available supply, significantly increasing the risk to vulnerable populations.

Common consequences

Bespoke planning for these risks is done at a national level due to the catastrophic scale of impacts. Bespoke planning will draw on national and local generic capabilities.

The exact consequences will be dependent on the nature of the attack, but this could include some of the following:

- human health impacts, which may include physical casualties, mental health casualties and fatalities
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, government services, communications, education)
- public behaviour and social cohesion – pro-social and anti-social behaviours

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Cyber attack: police systems

Policing systems are seen as high value targets for malicious actors, with the potential to cause disruption to emergency services in the UK. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the police will continue to monitor how current and emerging AI influences this risk.

Scenario

A cyber-attack targeting critical policing systems, which may result in: compromised investigations/prosecutions; risk to staff safety; reputational damage; reduction in police access to intelligence and operationally critical information; and a reduction in the effectiveness of frontline policing – resulting in the risk to life, and property. There may be a requirement to withdraw from critical systems until security can be restored. The most severe impacts are likely to last several days, whilst ongoing disruption could last months.

Key assumptions

Policing has been subject to significant attacks in recent years including attacks against national systems, local IT infrastructure, and third-party suppliers.

Variations

Variations include data breach, third-party supplier attack, mis/disinformation attack, or exploitation of legacy technology systems.

Response capability requirements

Government and Agencies. Police Digital Service (PDS) National Management Centre (NMC) coordinates the policing response in line with the National Police Chiefs' Council (NPCC) cyber response strategy as agreed by the Digital, Data and Technology Coordination Committee, and supported by the Home Office, National Cyber Security Centre and Cabinet Office.

CNI and Wider Private Sector. Specialist IT support may be beneficial to aid recovery.

Voluntary, Community and Faith Sector. Given there will be some expected disruption to police service provision, victim support provided by VCFS will be essential to support those in need.

Recovery

Recovery rates will be dependent upon the sophistication of the attack and scale of impact. In some cases, it is highly likely that the technical recovery could take months, in some instances, up to 18 months, and could be costly.

Impact on vulnerable people

Vulnerable people can be at higher risk of crime (this may be based on ethnicity, disability, or sexual orientation) and depend on the policing response capabilities, and would be disproportionately impacted by a reduction in the services provided.

Common consequences

The exact consequences will be dependent on the nature of the cyber-attack. This could include some of the following:

- disruption to essential services (including emergency services, education, energy and government)
- disruption to cyber services
- disruption to security

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).



State threats

Malicious attack: civil nuclear

The civil nuclear sector is of strategic importance to the UK's national security, energy resilience and clean energy transition. The UK's civil nuclear industry covers a broad spectrum of the nuclear fuel cycle, including fuel enrichment and fabrication, electricity production, transportation of nuclear materials and nuclear waste management. Given increasing digitisation and interconnectedness alongside geopolitical instability and increasingly capable adversaries, the sector must remain vigilant to national security threats facing UK CNI, such as hybrid security threats, to maintain its defence posture.

Security in the UK civil nuclear sector is managed through a combination of safety and security regulatory frameworks, a defence-in-depth approach and proactive, sector-wide collaboration under the 2022-27 Civil Nuclear Cyber Security Strategy. This drives a holistic and resilient approach to managing safety and security risks in the sector. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. The government and the civil nuclear sector will continue to monitor how current and emerging AI influences this risk.

Scenario

This scenario assumes a cyber attack enabled by an insider is detected at a civil nuclear power plant. Operators subsequently decide to shutdown the reactor as a precaution. This results in a disruption to normal operations until investigations have demonstrated nuclear safety and security critical systems remain unaffected. Whilst the disruption is not a direct result of the attack, the incident erodes public confidence in the safety and security of the sector and undermines future expansion of the sector, potentially leading to the early decommissioning of sites. The ramifications impede the UK's net-zero and energy security objectives.

Key assumptions

Defence in depth, inherent protections and functional diversity prevent an offsite radiological release.

Response capability requirements

Government and Agencies. Local Resilience Forums' partners have a collective responsibility to plan, prepare and communicate in a multi-agency environment. Interagency coordination must be exercised to minimise the impact of incidents on local communities and dovetail with national incident management objectives. A robust communication strategy will be required to minimise misinformation and disinformation.

CNI and Wider Private Sector. Operators must establish and regularly test their arrangements for preparing for, responding to and recovering from security incidents.

Voluntary, Community and Faith Sector. Mental health support may be required to assist those suffering from anxiety or distress caused by the incident.

Recovery

Normal operations will resume following investigations and assurance activities to demonstrate nuclear safety systems are unaffected. Long-term recovery would focus on rebuilding trust in the operator and the wider sector.

Impact on vulnerable people

Misinformation and disinformation about the safety and security posture of the site may lead to increased anxiety among local residents. In addition, vulnerable or stigmatised communities may be deliberately targeted by mis/disinformation campaigns online, particularly via social media, increasing the public's exposure to harmful narratives. Timely, coordinated, and accurate information through public channels is crucial to responding to this.

Common consequences

The exact consequences will depend on the nature of the incident, but this could include:

- potential human health impacts, which could include mental health casualties
- disruption to essential services (including energy)
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Malicious attack: 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. 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 which 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 state 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. Impacted banks and customers will also face heightened operational losses and fraud risks. 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.

Key assumptions for this scenario

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. For example, attacks on the SWIFT messaging system, Visa and Bacs retail payments and Real Time Gross Settlement (RTGS).

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. 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, which reached its initial implementation milestone in spring 2025, requires regulated firms to set impact tolerances and remain within these.

Recovery

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

Impact on vulnerable people

Depending on the FMI impacted, this could impact those on lower incomes, weekly payments, living in poverty, or in receipt of benefit payments.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include disruption to financial services, disruption to cyber services, disruption to government services and potential changes in public behaviour.

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘cyber attacks on infrastructure’ category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Malicious 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). 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 actor. The attack 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. Following the outage, some customers will be able to access the bank's IT networks but a large number of customers will continue to experience some level of disruption for several weeks as backlogs are cleared. The bank will also likely face heightened fraud and operational losses.

Key assumptions for this scenario

The scenario is based on past cyber incidents and the increasing cyber threat. The assumption would be that the cyber attack directly impacts the IT operations of the bank.

Response capability requirements

Government and Agencies. Collective incident response capability is managed under the UK's Authorities' Response Framework.

CNI and Wider Private Sector. 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, which reached its initial implementation milestone in spring 2025, requires regulated firms to set impact tolerances and remain within these.

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.

Impact on vulnerable people

The most significant impact would be felt by vulnerable customers with only a single bank account. This scenario could also disproportionately impact older people, those on lower incomes, people with disabilities, those living on weekly payments, living in poverty, or in receipt of benefit payments.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include disruption to financial services, disruption to cyber services and potential changes in public behaviour.

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the 'cyber attacks on infrastructure' category is 3 (moderate) and the average likelihood score is 4 (5-25%).

Major disruption to international subsea telecoms cables

The UK is highly reliant on international digital connectivity for everyday services, economic activity, and public administration. Subsea telecoms cables provide this connectivity, carrying around 99% of internet and data traffic to and from the UK, including voice calls, online services, and data exchange. Major disruption to international subsea telecoms cables would have widespread adverse effects in the UK and beyond.

Scenario

The reasonable worst-case scenario assumes the majority of transatlantic subsea fibre optic cables connecting the UK directly to North America would be damaged over a number of hours, rendering them inoperable. This would cause considerable disruption to UK internet connectivity, with members of the public experiencing slow or unreliable internet-based services for up to three days. Consequently, essential services that rely upon international connectivity and offshore data services – including communications, finance, transport, government and defence – would be adversely affected, as well as some supply chain management and payment systems. Emergency services are expected to continue operating, although pressure on supporting systems may increase.

Key assumptions

The most severe impacts to communications would be during the first 24-72 hours following the cable damage. Impacts to low latency connectivity between the UK and North America could last for a month, depending on cable repair times. Alternative communications methods exist (like satellite communications) but cannot fully replace the capacity of subsea cables in the short term. Disruption could also have knock-on effects beyond the UK, particularly in other European countries, where slower-running border processes may delay passengers and freight, further impacting services used by UK businesses and citizens.

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.

Response capability requirements

The response would rely on coordinated action across sectors to sustain essential connectivity and restore essential services.

Government and Agencies. The government would support coordination of the operation to restore connectivity, including provision of mutual aid and assistance where necessary. It would also assist with the coordination of activity to manage the impacts in the UK of the disruption to international connectivity, including impacts on essential services.

CNI and Wider Private Sector. Communications service providers would lead the restoration of critical traffic flows to the UK. The cable repair industry maintains repair capabilities to respond if an incident occurs.

Voluntary, Community and Faith Sector. Given general communications will be disrupted there may be a role for this sector to support government messaging and communications.

Recovery

The most severe impacts to internet communications would recover by up to three days, as networks are reconfigured. Digitally intensive sectors could face longer-lasting impacts as lost access to digital systems reduces productivity, forces reliance on manual workaround, and in some cases requires operations to pause. Full 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.

Impact on vulnerable people

The scenario would disproportionately affect short-term visitors to the UK, younger people, and those reliant on digital connectivity for health, care, safeguarding, and access to information. The most severe impacts would be limited to the first 24-72 hours of disruption.

Common consequences

The exact consequences will be dependent on the specific nature of the failure and could include some of the following:

- disruption to essential services (including transport, communications)
- disruption to security
- disruption to financial services
- disruption to business
- potential change in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘conventional attacks on infrastructure’ category is 4 (significant) and the average likelihood score is 3 (1-5%).



Geopolitical and diplomatic risks

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. Recent events in the middle east demonstrate the impact of the disruption of global oil trade routes. The government will look to embed learning from current events in future NRR editions.

Scenario

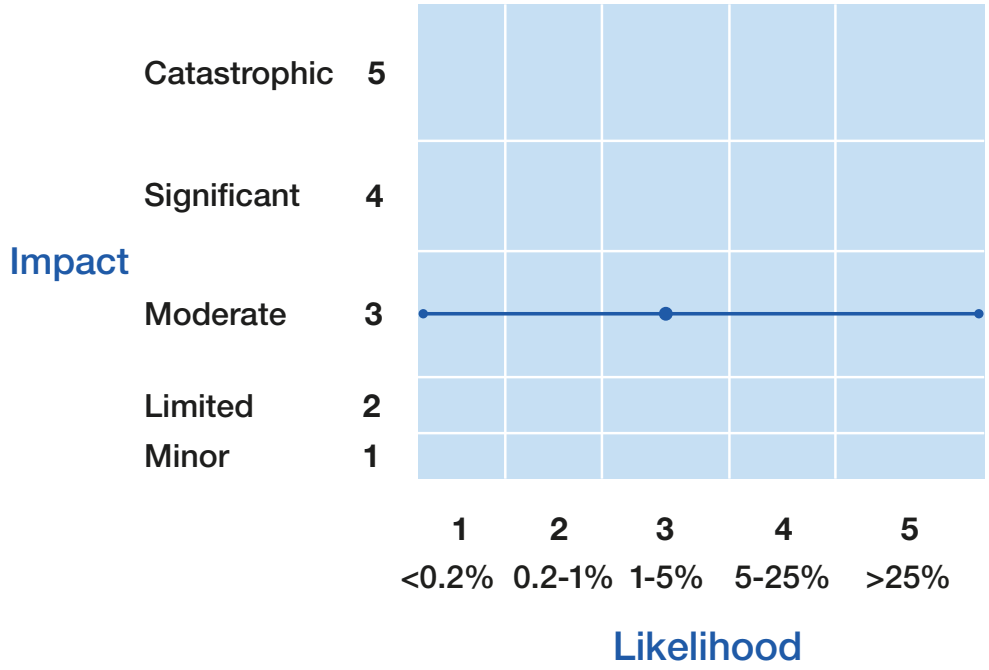
The reasonable worst-case scenario assumes that war, political upheaval or a more benign cause would significantly disrupt global oil supply, resulting in much higher global prices. This has a knock-on effect on the global economy, given its reliance on oil as an energy source (particularly for transport).

Key assumptions

The oil market is globally integrated and a disruption anywhere will affect the UK by increasing global competition for remaining supply.

Variations

The level of disruption to global oil supply could vary substantially and would affect how impactful this was on global supply and the UK.



Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. CNI owners and operators, as well as the wider private sector are heavily reliant on oil, contingencies should be in place for an event of reduced access to oil and higher prices. There also may be some impact on key supply chains as a result, companies involved in these supply chains are encouraged to ensure resilience within the system for an event such as this.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

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.

Impact on vulnerable people

The increase in oil prices is likely to disproportionately impact people from lower socioeconomic backgrounds given they tend to spend a higher proportion of their total income on fuel and food both of which will be impacted. The elderly, children and the immunocompromised are also likely to be adversely impacted as there may be a reluctance to utilise fuel as much as previous which may result in second order health impacts.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, health, food, energy and transport)
- disruption to financial services
- potential changes in public behaviour

Interference in UK democratic process

This government is committed to restoring trust in our political system, by strengthening our democracy and encouraging full participation in our elections. MHCLG set out their vision in Restoring trust in our democracy: Our strategy for modern and secure elections. Within this, it is a key priority, to identify and assess threats to democracy and potential interference. MHCLG and CO work jointly to identify and assess the threat.

Scenario

Interference in UK democratic processes could take a variety of forms. This could include one or more of the following: attacks on election infrastructure, deterioration of the online information space, harassment and intimidation towards candidates or voters, the hack and leak of sensitive information relating to a party or a prominent individual, and any element of foreign interference in any of these.

Key assumptions

Elements of this scenario may occur amid heightened tensions between the UK and other state actors.

Variations

The scenario could vary substantially. The exact nature of the interference would affect the resultant impacts.

Response capability requirements

Government and Agencies. The UK has established structures (including monitoring and incident response capabilities) in place to protect and secure UK democratic processes. Central government would lead the response and key activities include intelligence gathering, monitoring, incident response coordination, system penetration testing, integration of cybersecurity with electoral expertise, and effective communication with local authorities, the Electoral Commission, and across government. Where appropriate, the government will work with political parties and candidates, in partnership with the Electoral Commission.

CNI and Wider Private Sector. Organisations who act as the sites for local elections should ensure they have effective processes in place to minimise the potential for interference.

Recovery

If this risk materialised there would be an erosion of public confidence in the resilience and integrity of UK democratic processes and this may lead to long-term implications, reduced engagement in the electoral process and questions around the legitimacy of results.

Impact on vulnerable people

Candidates in areas where there has been significant disruption may face increased levels of intimidation and harassment. If this risk were to materialise candidates with certain characteristics may be dissuaded from standing in an election or being able to campaign to the full extent. Were this risk to materialise, there may be a cascading impact where people are less likely to engage with the democratic process as certain groups may be less likely to vote if there is reduced diversity in candidates.

Common consequences

The exact consequences will be dependent on the nature of the interference. It is expected that there will be disruption to security and changes in public behaviour.



Accidents and systems failures

Major adult social care provider failure

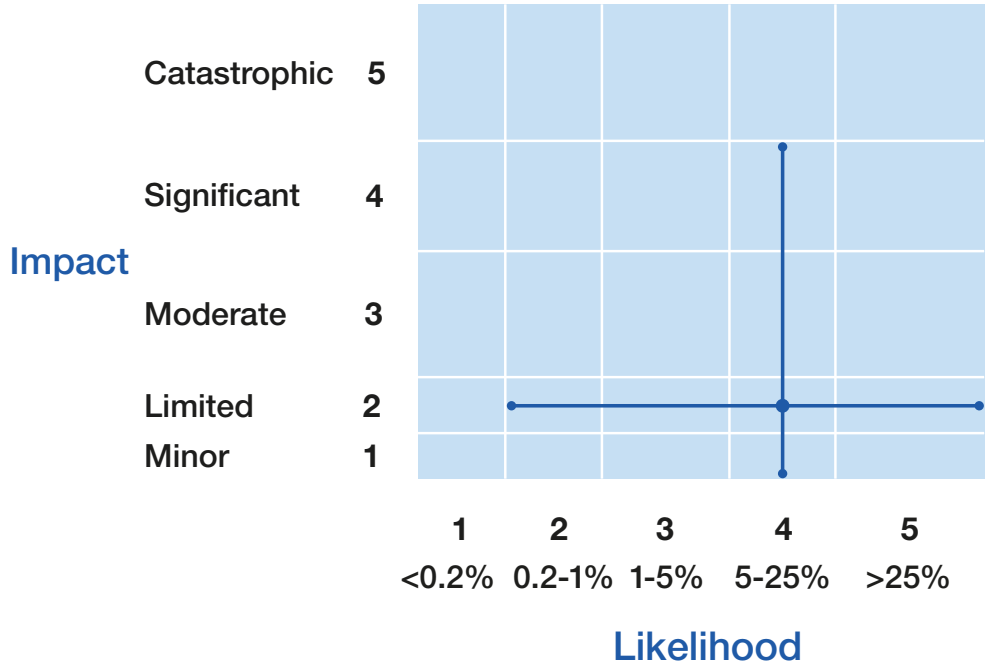
A complex major adult social care provider failure (MPF) could occur for a number of reasons, such as cost pressures or over-indebtedness. If unmitigated, there is a real risk to continuity of care for people with significant health, care and support needs. The Care Quality Commission's (CQC) Market Oversight Scheme is designed to monitor the financial health of major providers that are difficult to replace, and ensure local commissioners are given some advanced 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 health and care commissioners to protect continuity of care.

Scenario

A complex MPF occurring with limited prior warning, leading to sudden service cessation, and impacting a significant number of local authorities, Integrated Care Boards (ICBs), and people with care and support needs (either in their own homes or dedicated care spaces). In this scenario, the scale and complexity of the failure may make it difficult for affected local authorities to discharge their temporary duty under Section 48 of the Care Act 2014 to ensure continuity of care, putting the welfare of people with care and support needs at risk.

Key assumptions

The scenario assumes a complex MPF that involves a significant number of local health and care systems 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 and ICBs are in the process of rolling out their contingency plans.



Response capability requirements

Government and Agencies. This scenario is likely to place significant pressure on local authority resources – including social workers and adult social care commissioners – and local NHS services. To support local authorities in discharging their temporary duty, DHSC will 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.

CNI and Wider Private Sector. Providers of adult social care are responsible for monitoring their own financial health. The largest and most 'difficult to replace' providers – major providers of adult social care – are subject to CQC's Market Oversight Scheme. The scenario reflects 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 mitigate the impacts. Where applicable, providers should work with CQC to ensure awareness of any changes in their circumstances.

Voluntary, Community and Faith Sector. As part of their contingency plans, local authorities and ICBs may work with the VCFS, informal carers, and the private sector, to ensure that people who may find themselves in a vulnerable position have appropriate support in place.

Recovery

Recovery time would depend on national and local market conditions.

Impact on vulnerable people

A complex MPF may result in disruption to the services provided to adults in receipt of social care and have a serious impact on their health and wellbeing. There is evidence that indicates moving those with complex health and care needs, e.g. dementia, mental health and learning disabilities, in an unplanned way can increase the risk of serious harm and risks potential fatalities. In this scenario, where a local authority is unable to discharge its temporary duty to secure continuity of care, there may be an interim period where the level of care and/or support is reduced. This could have a significant impact on the lives of individuals and their carers, and mitigations are needed to ensure that disruption is minimised as far as possible.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- health and wellbeing impacts on those needing care services
- increased demand on other essential services – including the NHS – and on the voluntary sector and informal carers and families
- loss of confidence in the wider adult social care market
- potential economic impacts, which may include increased costs for continuity arrangements, financial pressures on local authorities, and wider market effects

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. 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 impact and likelihood 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

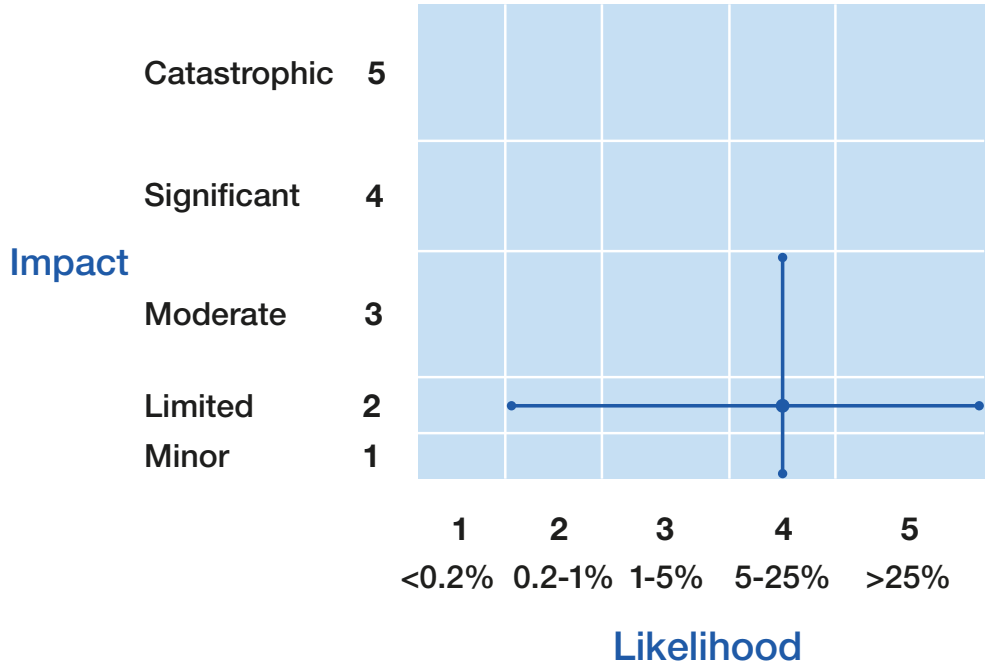
The reasonable worst-case scenario is based on the insolvency of a supplier of critical IT services supporting operational systems or back office processes integral to critical national services across the country. Potential significant impact upon critical service operational delivery, such as lack 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. Impact dependent on the nature, size and geography of service and supplier.

Key assumptions

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

The scenario could vary in the sector where the insolvency occurs and the number of insolvencies at once. More insolvencies at once will likely have a larger impact.



Response capability requirements

Government and Agencies. Central capability in corporate finance (restructuring, insolvency) 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.

CNI and Wider Private Sector. Specialist capability is required to manage distress and contingency plans, such as back-up operations.

Voluntary, Community and Faith Sector. If the secondary impacts disproportionately affect vulnerable people, support to these people would aid recovery.

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.

Impact on vulnerable people

If the secondary impact was felt in sectors where vulnerable people would be disproportionately affected (healthcare, care sector, social services) this dimension would present specific challenges. For instance, disruption to IT systems in healthcare could prevent access to critical patient records or disrupt care coordination. Loss of service in social services could directly affect the delivery of support packages, leaving individuals without essential help. The complexity of these issues is amplified by the potential for vulnerable individuals to have less resilience or alternative means to cope with service outages.

Common consequences

The exact consequences will be dependent on the specific event; this could include some of the following:

- disruption to essential services (including emergency services, education, government services, health, energy, transport, communications)
- disruption to financial services
- disruption to security
- potential changes in public behaviour

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 or sale as a going concern of the site, enabling the uninterrupted supply of fuel to customers.

Scenario

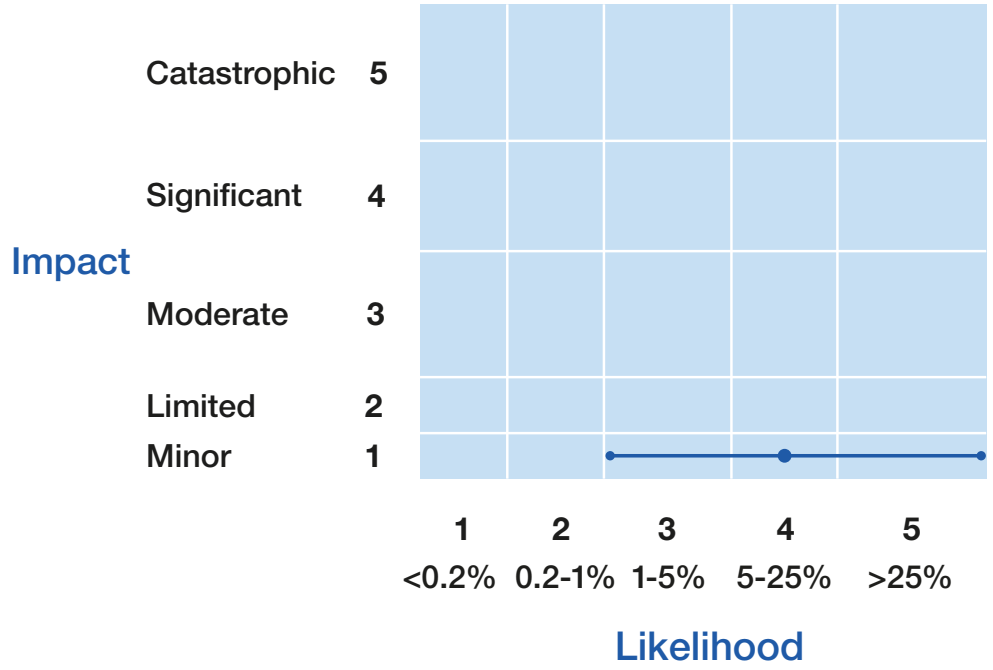
The reasonable worst-case scenario for this risk concerns an oil refinery, importation, storage or distribution company becoming insolvent. This could cause regional disruption to the production and supply of refined fuels, impacting road transport, aviation and domestic heating fuel. The loss of fuel 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.

Key assumptions

This risk focuses on a managed insolvency, without adaptive purchasing. However, in a worst-case scenario there could be a sudden insolvency accompanied by adaptive purchasing which does not allow the government and industry sufficient time to bring in mitigations and activate contingency plans, which could result in temporary fuel shortages.

Variations

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 and Agencies. 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.

CNI and Wider Private Sector. The emphasis is for industry to ensure they have contingency plans and effective mitigations in place for an incident such as this, and to mitigate issues as much as possible without government intervention. As seen in the Prax Lindsey Oil Refinery insolvency in summer 2025, the UK's downstream oil sector is flexible and largely able to adapt supply chains to make up shortfalls without government intervention.

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.

Impact on vulnerable people

If there is disruption to fuel supply in this scenario, those that rely on fuel to heat their homes and/or are reliant on cars to receive medical care would likely be adversely affected. This is likely to be disproportionate towards rural and elderly members of the public, but DESNZ will put in mitigations to limit the scale of this.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- disruption to essential services (including transport)
- potential changes in public behaviour

Rail accident

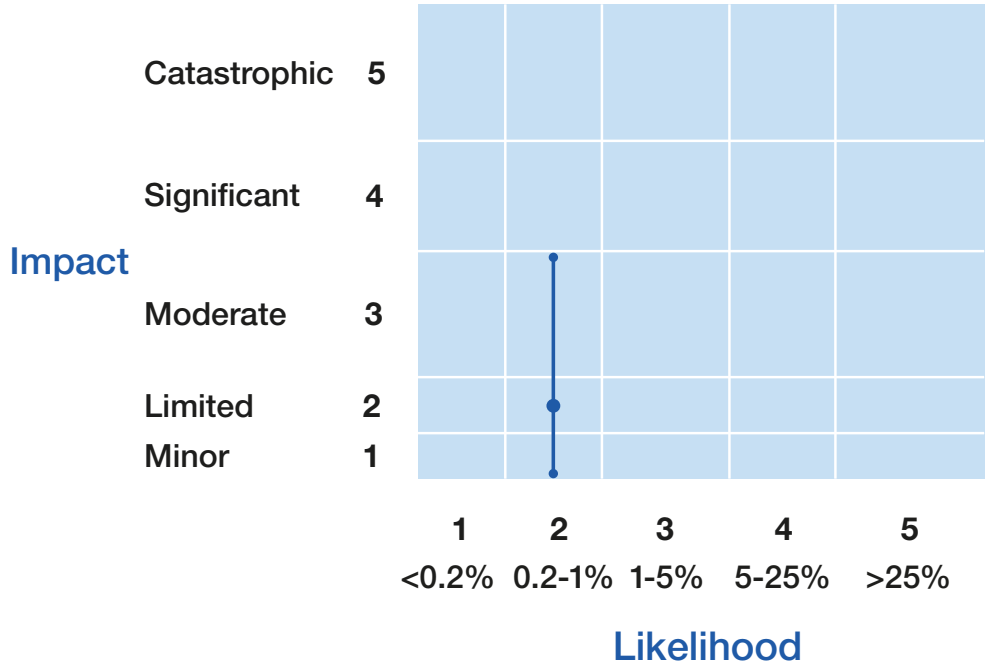
Although UK railways are among the safest in Europe, there is still a risk that a rail accident could occur. A recent example is the Shap derailment in November 2025, when a passenger train ran into a landslide in rural Cumbria following a period of heavy rainfall, which resulted in the train derailing for 560 metres, with 4 injured and significant damage to overhead lines, track, and signalling. A robust safety framework, with an independent safety regulator and accident investigation body, is central to mitigating this risk. Key to a safe system is having strong legal requirements setting clear responsibilities and duties for bodies operating in and around the railway, supported by a strong culture of enforcement and compliance.

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.

Key assumptions

The current legal framework that assigns roles and responsibilities to identify, mitigate and control risk is maintained. Robust safety and technical standards are in place to ensure trains operate safely on the network. This extends to specifications for the design of trains, infrastructure, and operational procedures.



Variations

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

Government and Agencies. A quick coordinated response between rail operators, Network Rail, the Office of Rail and Road, the Rail Accident Investigation Branch, local authorities and emergency services (including police, fire and rescue and ambulance services) would be required to mitigate the impacts of a rail accident and reduce potential for subsequent harm.

CNI and Wider Private Sector. Industry has experience of managing rail accidents and has procedures and processes in place to effectively respond and run rail replacement services where required. Where dangerous materials are involved, emergency procedures would need to be rapidly implemented. Companies working in critical supply chains should ensure there are effective mitigations in place for disruption caused by a rail accident. Local authorities have agreements and call-off contracts with providers who may need access to a range of supplies as the need arises, e.g. food, accommodation, and transport.

Voluntary, Community and Faith Sector. Voluntary organisations provide post-incident victim assistance for casualties and people nearby, including psychological treatment and support.

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 based on harm/economic damage). 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.

Impact on vulnerable people

Those with mobility or visual impairments, and those living in rural areas are likely to be disproportionately impacted by services being suspended, due to inaccessibility and difficulty leaving the affected area.

Common consequences

The exact consequences will be dependent on the specific event; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for people to be evacuated
- contaminated environment or the presence of potentially hazardous materials
- disruption to essential services (including transport and emergency services)
- potential changes in public behaviour

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. The UK has extensive experience managing large passenger vessels and cruise ships and has an exemplary safety record.

Scenario

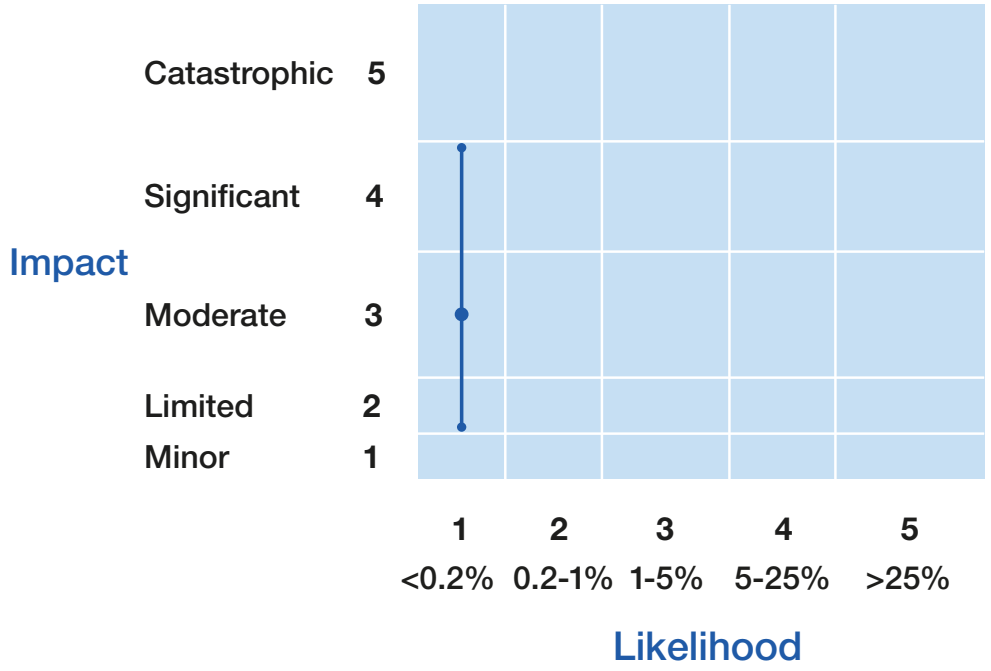
The reasonable worst-case scenario is based on a large passenger vessel (for example, cruise ship or ferry) sinking, potentially caused by a collision with another vessel, fire or grounding. Significant numbers of people are aboard, who rapidly abandon the vessel. There would be no-notice fatalities 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

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

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

Government and Agencies. 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. A robust capability to count and track casualties and survivors is required.

CNI and Wider Private Sector. Where passengers are landed at ports, port security may need to be considered and communication capabilities between agencies landside and seaside at the landing point need to be strong.

Voluntary, Community and Faith Sector. Local, regional and national charity, voluntary and faith organisations will likely support the response. The RNLI and other independent lifeboat charities would have significant involvement through their 24/7 maritime rescue service coordinated by HMCG. Local faith and community groups would potentially provide casualty and family support, such as opening public buildings for a place of temporary shelter, or the supply of clothing, food and drink, phone charging etc. Where these capabilities exist, they are referenced within local landing point plans managed by the LRF.

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 where the incident may leave a lasting impact on the community. Recovery of the vessel and any pollution are managed through the National Contingency Plan and commercial salvage routes.

Impact on vulnerable people

Depending on the demographics, background and experiences of those on the ship there may be some people who are more adversely affected by the event than others. For example, those who are less mobile, elderly or children may struggle more with the evacuation and will need support.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- search and rescue
- potential human health impacts, which may include physical casualties, mental health casualties and fatalities
- evacuation from the vessel; shelter required
- disruption to essential services (including emergency services, health, transport and government)
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to security
- potential changes in public behaviour

Major maritime pollution incident

There is a risk of major maritime pollution in UK waters, which could result from the accidental spillage of a pollutant, for example, oil from tankers or leakage from pipelines or offshore oil wells. These incidents are infrequent but do occur on occasion. For example, 72,000 tonnes of crude oil were spilled due to the Sea Empress grounding in Milford Haven in 1996. The UK has plans and procedures in place, the National Contingency Plan, to deal with pollution at sea in order to quickly respond, limit and reduce impacts on the environment and local coastal communities, working with local authorities and emergency services to communicate and plan for such eventualities.

Scenario

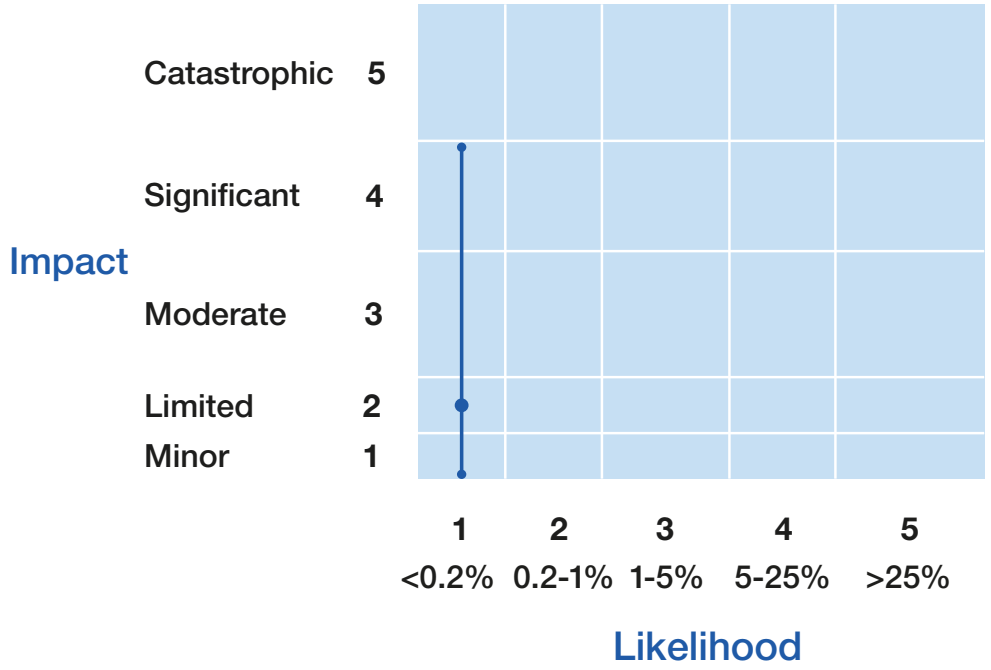
This scenario involves the spillage of 100,000 tonnes of crude oil into UK coastal waters. The cause could be vessel collision, fire or grounding. The spillage results in up to 200km of UK coastline being contaminated. Depending on the type of pollutant and extent of the contamination, there could be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

Key assumptions

The scenario assumes that the vessel would not sink or prevent access to liquified natural gas terminals or port infrastructure.

Variations

The scenario could vary in a range of ways including location, the type and volume of pollutant and where the pollutant could come from. Closer proximity to a densely populated area would increase the impact but is less likely to occur. A less likely, but more impactful, scenario would occur if the ship were to sink or oil to ignite and put lives in danger. The pollutant type could also vary, for example, non-oil-based types of pollution such as plastic nurdles or more persistent oil types.



Response capability requirements

Government and Agencies. Local authorities, the Environment 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.

CNI and Wider Private Sector. 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 for Maritime Salvage and Intervention (SOSREP), salvors, and ship insurers to organise the removal of the vessel (if safe to do so).

Voluntary, Community and Faith Sector. The VCFS would engage with local authorities to support the coastal communities and assist in clean-up efforts. Seafarer welfare charities would also potentially be engaged to support those onboard the vessel.

Recovery

Recovery may take several years. Satellites and aerial assets 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 Prevention of Cruelty to Animals and Royal Society for the Protection of Birds would assist in wildlife aid and recovery. The MCA would be responsible for managing stand-by response vessels. An investigation by the Marine Accident Investigation Branch (MAIB) would be required.

Impact on vulnerable people

There are likely to be significant impacts on responders, the vessel crew and the surrounding coastal communities. Responders will be given protective equipment and will follow best practice to reduce the impact. Support will be targeted to impacted coastal communities.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated or closure of public areas
- disruption to essential services (including emergency services, health, energy and transport)
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- potential changes in public behaviour

Vessel blocking a major UK port

There is a risk that an accident involving a vessel could block a major UK port, disrupting key imports and exports. 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 and had significant impacts on trade and global supply chains.

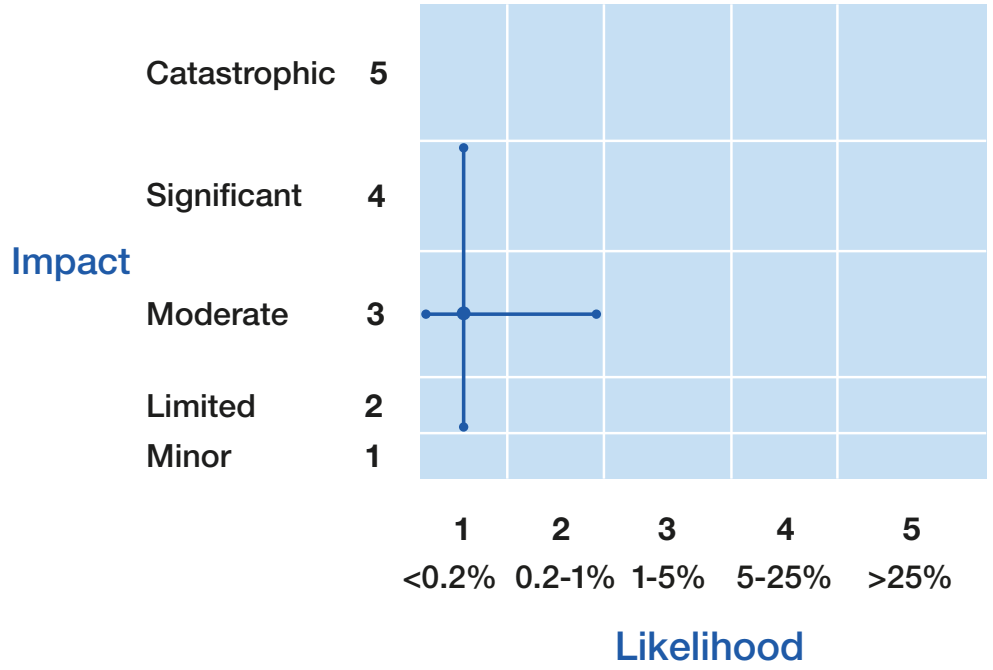
Ports and harbour authorities maintain responsibility for ensuring plans are in place to manage incidents that could impact port operations. National support is provided through the UK's National Contingency Plan for Responding to Maritime Pollution Incidents, which sets out the framework for coordinating and delivering salvage and pollution-response activity.

Scenario

A large container vessel grounds or sinks in a major UK Port, restricting some or all access into the port for vessels. The movement of critical goods into the UK, including energy supply, may be impacted for several weeks to months depending on the nature and location of the incident. It would likely take at least three months for a full salvage operation to be carried out in the port to re-open the channel. Cargo would no longer be able to transit through the port to enter or exit the UK, potentially impacting critical supply chains. Ships would need to be rerouted as far as possible, which would be challenging due to their size and the port infrastructure required to accommodate them and their cargo.

Key assumptions

The incident is not the result of malicious intent but rather human or technological error, or an extreme weather event leading to an accident. The port would be closed to all marine traffic initially but limited activity may be able to resume in the short term.



Variations

This severity of any incident will be dependent on the port impacted, as well as the vessel type and its cargo. The length of disruption to the UK will depend on the port's ability to continue operating and any alternatives which may be available.

Response capability requirements

Government and Agencies. Department for Transport, Maritime and Coastguard Agency (MCA) and Secretary of State's Representative for Maritime Salvage and Intervention (SOSREP) would oversee and inform. Generic emergency response capabilities such as search and rescue and

policing would be required, alongside specialist environmental support where needed. If an uninsured vessel is involved, the government may need to provide financial assistance.

Government intervention would be critical in managing national impacts, including setting priorities for the movement of essential goods. This could be to meet requirements for food, medical supplies or industrial materials. Government intervention would also be critical to meet any deficit created by the loss of energy supply.

CNI and Wider Private Sector. The salvage and recovery operation would mostly be actioned through the private sector with specialised resources and personnel. Many of these responders would have to come from abroad at very short notice.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people. Seafarer welfare charities would also potentially be engaged to support those coming off the vessel.

Recovery

Recovery length would depend on the nature of the incident, the location, weather conditions, accessibility to the wreck and availability of specialists to conduct the wreck removal. A vessel may be able to be refloated or partially removed to enable the port to operate but a fully disruptive wreck removal could potentially hinder port operation for months. Insurance would likely protect the facility from financial hardship during this time, but returning to business would be the port's priority.

Impact on vulnerable people

Those on the vessel itself will become vulnerable in the event and will be prioritised in the response. There will also be some disruption to supply chains and potentially higher fuel prices, which may adversely impact some people, for example those in lower socioeconomic groups, those in rural areas and those who purchase larger volumes of fuel and energy regularly.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, energy and transport)
- potential changes in public behaviour
- potential contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials

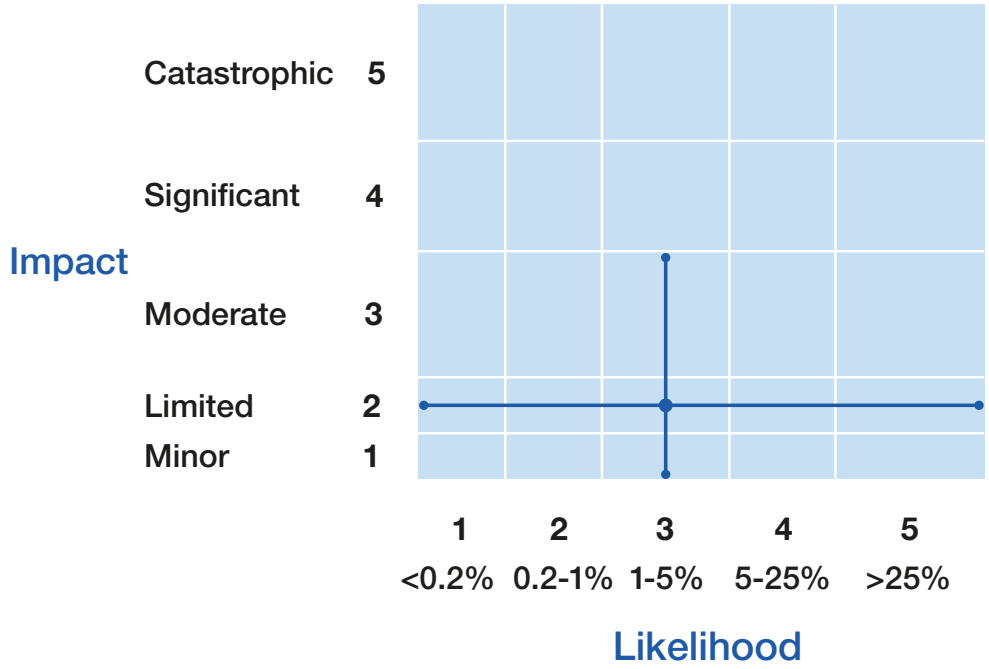
Accident involving high-consequence dangerous goods

High-consequence dangerous goods are materials that pose significant risks to health, safety or the environment and have the potential for misuse in terrorist events, requiring strict regulatory and security measures. However, there are regulations in place (the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009) as well as international regulations (ADR) to ensure that these substances are transported safely and securely so that accidents 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 could result in casualties and would likely lead to road closures for several days, significant local infrastructure damage, 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. The types of substances that could be involved include flammable gases or liquids, substances liable to spontaneous combustion, corrosive substances, and nuclear material or any other dangerous goods.



Key assumptions

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.

Variations

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

Response capability requirements

Government and Agencies. Depending on the substance carried, 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.

CNI and Wider Private Sector. Companies who transport dangerous goods should adhere to regulations which will decrease the likelihood of the risk occurring.

Recovery

It may take a few months to rebuild and repair the damage to building and infrastructure, the exact time would depend on the extent of the damage and nature of the substance.

Impact on vulnerable people

Those in the surrounding area would become vulnerable, requiring targeted support. The road closures in the aftermath of this incident, will disproportionately impact those reliant on driving for transportation.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties and injuries, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services and transport)
- potential changes in public behaviour
- regulatory changes are likely to be made

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 UK State Safety Programme for aviation. 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 all the UK aviation authorities, including the UK Civil Aviation Authority and other key partners.

Scenario

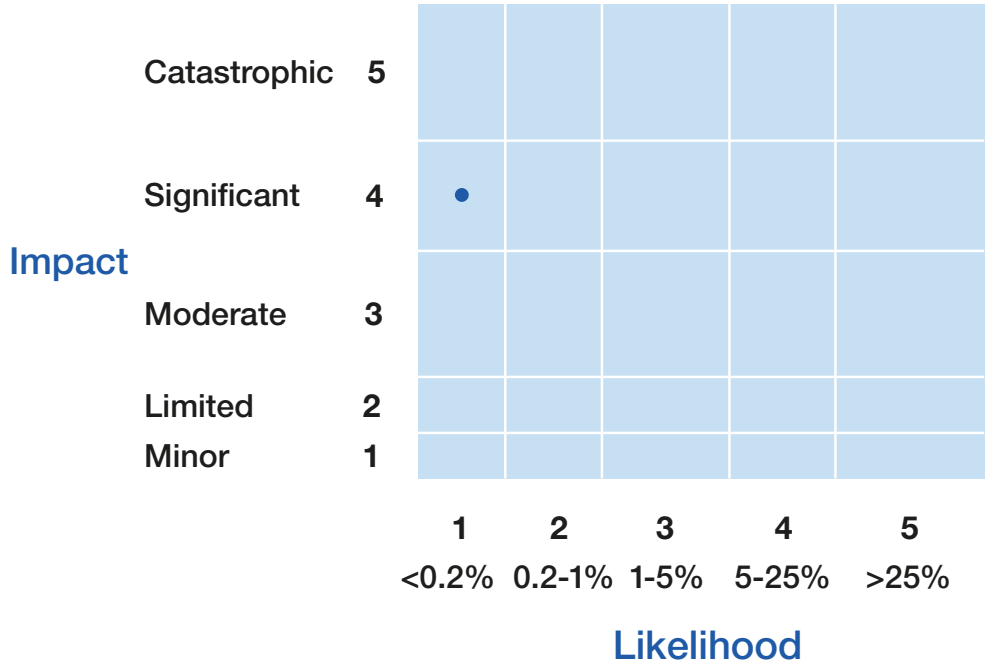
The reasonable worst-case scenario is based on an airborne collision involving one or more commercial aircraft over a major urban area in the UK. This results in fatalities of the passengers and crew on board the aircraft, with significant fatalities and casualties on the ground due to falling debris. Debris would also cause damage in the affected area. This would require decontamination services to clean up aircraft fuel that is spread over a wide area.

Key assumptions

Robust safety and technical controls are in place to ensure aircraft operate safely, and 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 UK Civil Aviation Authority (CAA) iteratively, and any changes to baseline effectiveness will be reflected in future updates.

Variations

Other plausible scenarios include a collision with a general aviation light aircraft, business jet or remotely piloted aircraft.



Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. There would be a need for decontamination services to clean up aircraft fuel, debris and other remains. 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 Air Accidents Investigation Branch (AAIB) would assess the cause of the collision and make recommendations for immediate actions required to improve aviation safety.

Voluntary, Community and Faith Sector. 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.

Impact on vulnerable people

Those from lower socio-economic backgrounds may not be able to pay for repairs to damaged properties, and individuals with disabilities and mobility impairments may experience additional challenges in ensuring their needs are catered for. The trauma experienced by observers could lead to mental health issues or exacerbate existing mental health issues.

Common consequences

The exact consequences will be dependent on the specific event, this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, transport)
- contaminated environment or the presence of potentially hazardous materials
- disruption to security
- potential changes in public behaviour

Malicious drone incident

The use of drones has increased significantly in recent years, both for business and pleasure purposes. UK law 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. The government, working with the CAA, industry, and the police, maintains risk analysis and continually strengthens mitigations against malicious drone incidents.

Scenario

One planning scenario is based on the malicious use of a drone at an airport, aimed at causing disruption and safety concerns. However, we actively plan for all types of potential disruption and other adverse outcomes that may result from negligent, criminal, or terrorist use of drones, not just that of airport disruption.

Key assumptions

Assumptions vary by scenario, however, for the airport disruption scenario described above, the risk would not occur at the same time as another major event and the perpetrator is assumed to have malicious intent.

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Airports and airlines are responsible for ensuring the safety and security of their operations and taking appropriate measures to protect the public. This includes maintaining up-to-date risk assessments and regularly reviewing any changes to the threat picture.

Recovery

Recovery would depend on the exact nature of the scenario. For the above, full airport operations may take days to return to normal due to flight disruption, which would affect thousands of passengers.

Impact on vulnerable people

Those in the airport would be particularly vulnerable. There may be elderly people, those with mobility challenges and children in the airport all of whom may need support should the airport need to be evacuated.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential need for the site to be evacuated
- disruption to essential services (including emergency services, health, food, government services and transport)
- disruption to security
- potential changes in public behaviour

Disruption to space-based services

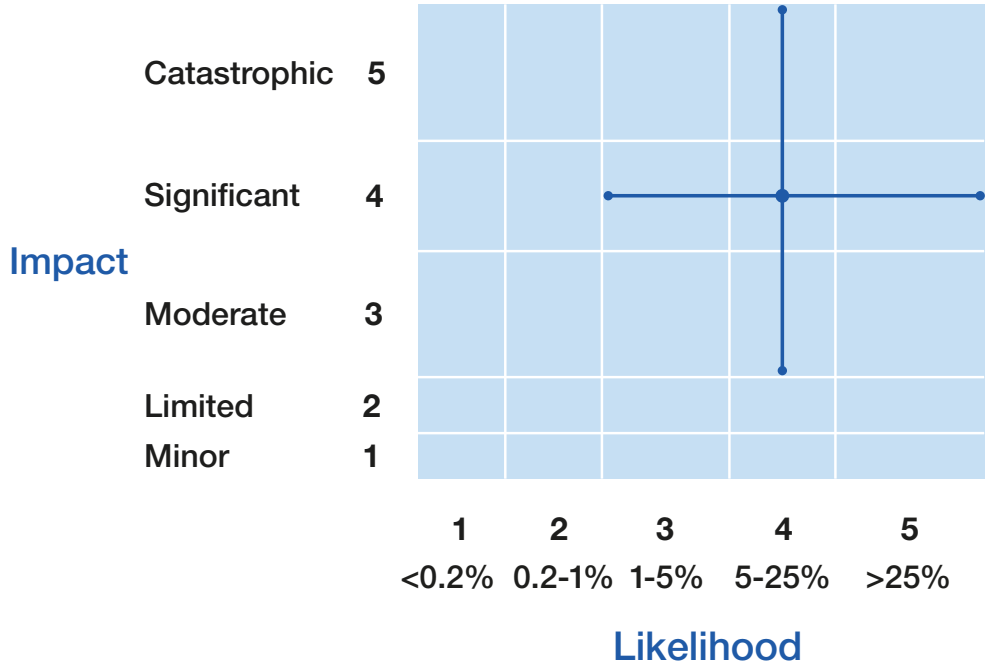
Space-based services, including satellite communications and remote-sensing systems, are integral to the United Kingdom's critical national infrastructure. Rising orbital congestion and increasing national reliance have significantly elevated the assessed likelihood and impact of disruption. Loss or degradation of these capabilities would have substantial cross-sector implications. Mitigation requires strengthened debris-removal activity, resilient terrestrial alternatives and enhanced space-situational awareness. DSIT will continue to explore how current and emerging AI will impact space based services, both positively and negatively, in future risk analysis.

Scenario

The reasonable worst-case scenario assumes a major orbital collision creates a fast-growing debris field that disables multiple satellites across affected orbits. This triggers widespread disruption to communications, navigation and Earth-observation services, with outages lasting from days to months depending on severity and replacement capacity. The resulting impacts cascade across critical sectors, including finance, transport, energy and emergency services, creating significant disruption.

Key assumptions

It is assumed that the likelihood of debris fragments re-entering and causing direct physical damage within the UK remains extremely low, based on historical re-entry data and the predominance of ocean and sparsely populated land areas on Earth's surface. However, this assumption does not reduce the overall risk because the primary impacts derive from the loss of satellite capability rather than debris re-entry. It is further assumed that collision and debris modelling provided by international partners remains reliable and that the UK will have timely access to and analysis capabilities of space surveillance data.



Variations

Variations include severe space weather, near-Earth objects, technical failures and malicious interference. Although they differ in likelihood and impact, all stem from reliance on space-based services. Rising concerns of space weather and deliberate interference have contributed to the higher likelihood score, their impacts on critical infrastructure are similar.

Response capability requirements

Government and Agencies. Reliance on space services needs to be better understood with redundancy systems in place in the event of disruption. The UK needs stronger space-situational awareness to inform response activities.

CNI and Wider Private Sector. Better international data-sharing and interoperability are essential, alongside tighter coordination across government, regulators and operators.

Voluntary, Community and Faith Sector. Voluntary and community groups will be important in supporting those with limited connectivity who would be impacted by a disruption.

Recovery

Recovery timelines depend on the orbit affected, debris spread and availability of replacement satellites. Short-term recovery focuses on restoring essential services using terrestrial backups; medium-term recovery may involve launching replacements and clearing high-risk debris; and long-term recovery could require redesigning or relocating satellite constellations. Some impacts on orbital safety and future launch windows may last for years.

Impact on vulnerable people

Disruption to space-based services would disproportionately affect vulnerable people, especially in remote areas that rely on satellite connectivity. Interruptions to navigation, logistics and emergency response would have a greater effect on population with complex health needs, making targeted support and alternative communications essential.

Common consequences

The exact consequences will be dependent on the specific event; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, food, finance, government services, education, water supply, sewage, energy, communications, transport)
- disruption to security
- loss of or disruption to Global Navigation Satellite Systems
- overseas response
- potential changes in public behaviour

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 location and navigation and providing precise timing for a range of critical systems. A long-term loss of PNT services, either due to technological failures or malicious activity, such as jamming, would have catastrophic and cascading effects across the UK and globally. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. DSIT will continue to monitor how current and emerging AI impacts the variations of this risk.

Scenario

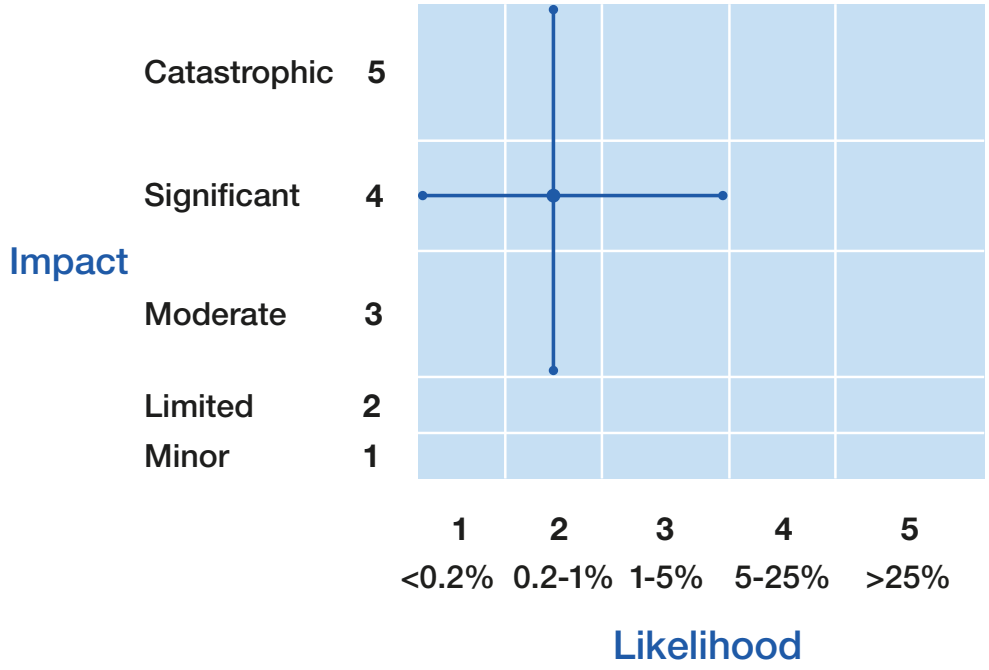
The reasonable worst-case scenario is based on a severe technical failure, due to either hardware failure or human error, in a Global Navigation Satellite System (GNSS) constellation leading to data corruption of that service. This would result in inaccurate position and timing data being delivered to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

Key assumptions

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

Variations

Variations include serious and organised crime jamming and spoofing activities leading to a loss of PNT services; state threats 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 recovery times.



Response capability requirements

Government and Agencies. DSIT is developing UK resilience to PNT loss, by implementing the October 2023 Government Policy Framework for Greater PNT Resilience and is committed to building infrastructure to mitigate the loss of GNSS services. This includes the establishment of the National Timing Centre (NTC) programme, to provide resilient, terrestrial, sovereign, and high-quality timing for the UK, including sovereign components, and the Enhanced Long Range Navigation (eLoran) programme, to provide a resilient, terrestrial, and sovereign system to provide backup position and navigation and distribute the timing signal from the NTC. Local Resilience Forums will play a role throughout the RWCS event to provide support and coordinate response and identify key essential services which require additional support or advice to recover.

CNI and Wider Private Sector. Given GNSS services are used by private companies they would be crucial in the response. To mitigate impacts, companies need to have resilient backup systems, such as atomic clocks to holdover time, in place and have plans on how to transition from back up services to GNSS once services are re-operational.

Voluntary, Community and Faith Sector. Support from the VCFS to those adversely impacted will be crucial to recovery.

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.

Impact on vulnerable people

Given the wide-ranging disruption due to the loss of PNT everyone would become vulnerable to some degree but some people would be more impacted than others. For example, delays to emergency services would impact individuals requiring medical attention potentially leading to loss of life, those travelling in an unfamiliar area during the period of disruption are at greater risk of getting lost, people who live alone may be adversely impacted by the loss of communications, people from lower socioeconomic backgrounds who are heavily reliant on public transport who may be less able to get to work as well as individuals who receive regular homecare whose carers travel may be disrupted.

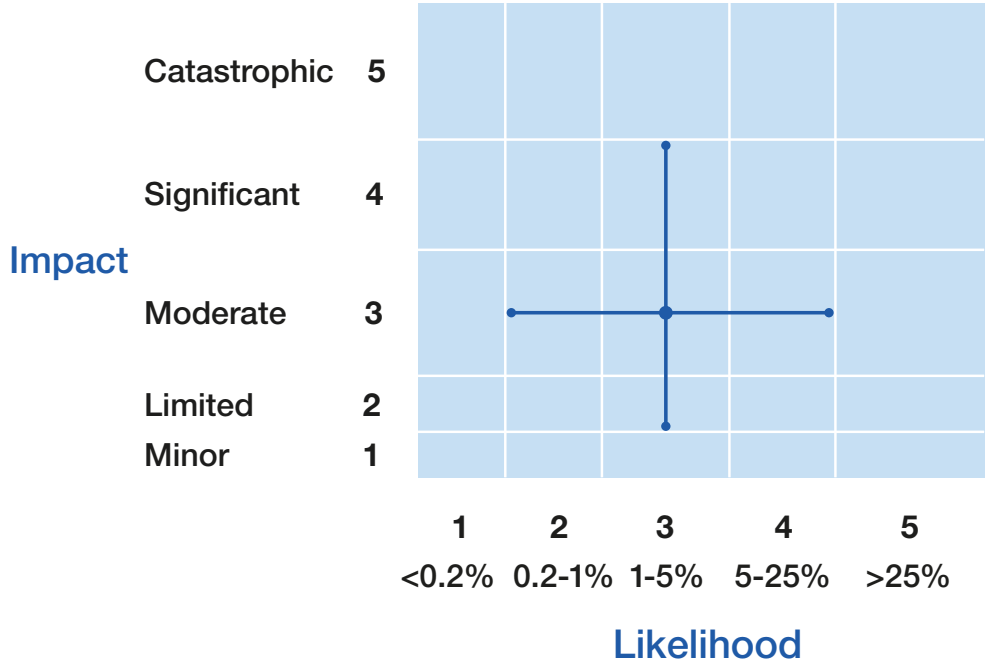
Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, health, food, communications, energy, water supply, sewage management, education, government services and transport)
- disruption to security
- disruption to business
- disruption to financial services
- potential changes in public behaviour

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

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

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

Government and Agencies. All affected customers would be unable to call 999/112, requiring a full response from Local Resilience Forums' partners and their devolved government 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.

CNI and Wider Private Sector. Telecommunications sector should ensure contingency measures are in place and should respond quickly if an incident occurs, working with government and local authorities.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people who may be more isolated due to a lack of communications.

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.

Impact on vulnerable people

Given all forms of communication would be unavailable, the affected customers may be less able to call support services. LRFs, government and local authorities would seek to mitigate against this. Proactive checks would be encouraged for the most vulnerable, working closely with the telecommunication providers.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, energy, health, food, government services, water supply, sewage management, communications, education and transport)
- disruption to security
- disruption to business
- disruption to financial services
- potential changes in public behaviour

National power outage

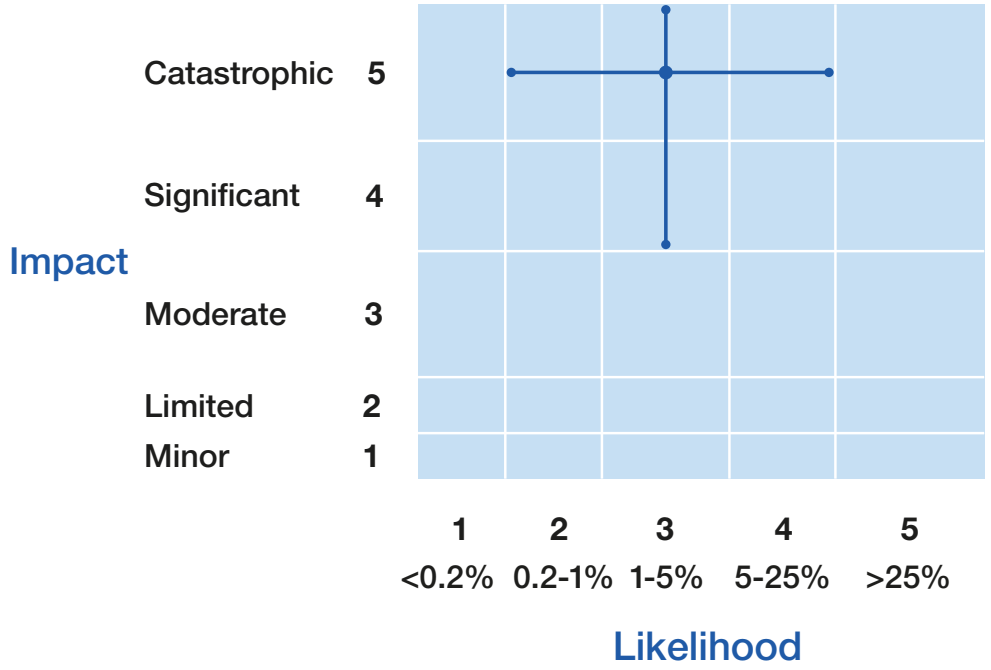
The National Electricity Transmission System (NETS) transports electricity across Great Britain. A failure of this system has the potential to severely disrupt all other critical systems, resulting in greater consequences than typical utilities failures. Great Britain has never experienced a nationwide loss of power and the likelihood is low, however, similar events have occurred internationally. In 2025, a rare cascading voltage surge caused a major power outage across Spain and Portugal leaving millions without power, demonstrating the severe impact of such events on modern infrastructure and society.

Scenario

The reasonable worst-case scenario is based on the failure of the NETS leading to 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.

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, and would worsen impacts on society.



Variations

The scenario could change depending on the number of available supply points, for example, generator sites, which could impact the time for complete restoration.

The scenario occurs during summer, which presents different impacts, particularly coupled with an NPO occurring during a hot day where air conditioning is required. Impacts could be similar to the Iberian outage in April 2025 however for a longer timescale.

Response capability requirements

Government and Agencies. Government bodies and emergency services will endeavor to maintain resilient communications systems to coordinate the response and support the immediate aftermath. The Department for Energy Security and Net Zero would enact the National Emergency Plan for Downstream Gas and Electricity.

CNI and Wider Private Sector. The National Energy System Operator (NESO) is legally required to have a plan to restore the electricity network within 5 days in the event of a National Power Outage, with a new Electricity Restoration Standard that will come in at the end of 2026.

Voluntary, Community and Faith Sector. Organisations assist by providing humanitarian assistance and victim support to help communities cope in the immediate aftermath of the incident.

Recovery

Within a few hours, some consumers would gradually be reconnected, with a significant proportion of demand (approximately 60%) being reconnected within 2 days. Restoration will increase from Days 3 and 4 and by Day 5 and 6, all customers will be re-connected however controlled demand disconnections will occur at peak times, for example, during evenings. Beyond 7 days we expect full and stable power restored to all of Great Britain. Residual recovery will impact critical sectors as they return to normal operations.

Impact on vulnerable people

It is not possible for any domestic customer's electricity supply to be prioritised during a National Power Outage. Although individual support capabilities will be limited by the scale of disruption, Local Resilience Forums (LRFs) and Local Resilience Partners (LRPs) will seek to target support using the Priority Service Register where possible. From Day 5 some pre-determined critical sites, such as some major hospitals, will have their power supply maintained, somewhat mitigating the impacts to essential services and therefore society.

Common consequences

Bespoke planning for these risks is done at a national level due to the catastrophic scale of impacts. Bespoke planning will draw on national and local generic capabilities. The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including health, food, transport, communications, water supply and sewage, cyber)
- disruption to security
- disruption to financial services
- potential changes in public behaviour

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. In recent years, Great Britain has experienced smaller-scale regional electricity failures, including by storm Darragh in winter 2024-25 where over 2 million homes were left without power, with disruption lasting up to a week for hundreds of customers. Government continues to work with industry to mitigate the impacts of severe weather, and industry have taken several steps to improve the electricity sector's resilience, as well as the protections and support available to consumers. These actions will aid in mitigating against larger-scale regional electricity failures.

Scenario

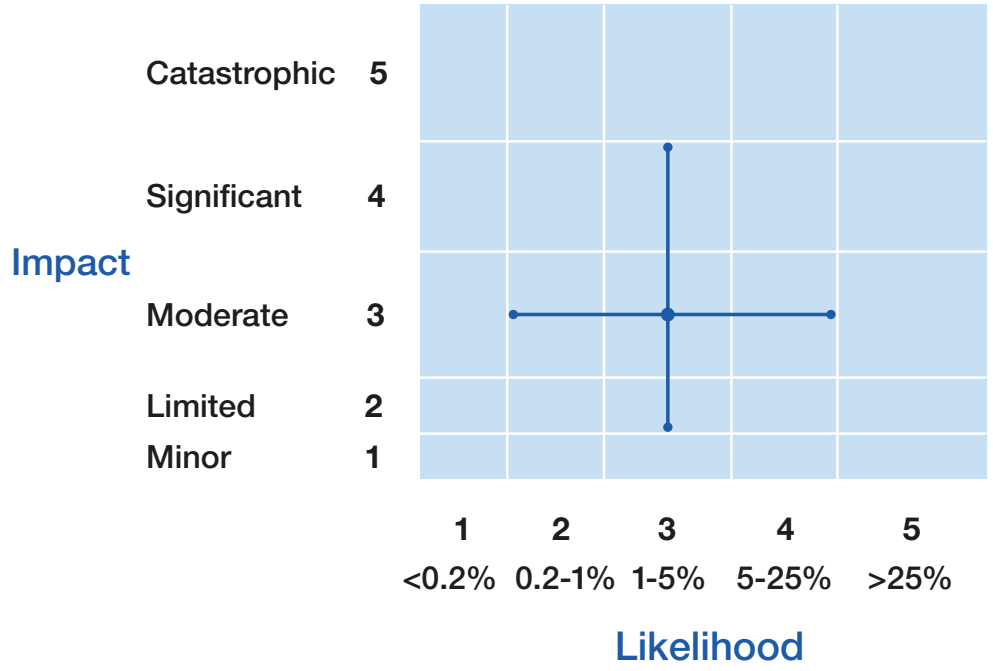
The reasonable worst-case scenario is based on a significant failure of the electricity network across several regions of Great Britain leading to the loss of power of up to 3.5 million customers for up to 24 hours, up to 350,000 still off supply for up to 48 hours and 20,000 for up to a week across the affected regions. Impacts would vary depending on which regions are affected (including rural regions which are likely to be worst impacted) 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 would be disrupted.

Key assumptions

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

Variations

Variations depend upon the cause and region impacted, and levels of resilience in these areas. There are a range of other potential causes of the damage including ground movement, over-pressurisation, mechanical failure or a malicious attack.



Response capability requirements

Government and Agencies. If caused by storms, weather forecasting would allow government, industry and local authorities to prepare. The response to an incident of this scale would require multi-agency coordination across Local Resilience Forums, with Strategic Coordinating Groups (SCGs) and Tactical Coordinating Groups (TCGs). Additional coordination from the central government would also take place. The government would activate established response plans to manage wider recovery.

CNI and Wider Private Sector. There would need to be preparations in place to support wider recovery and the continued operation of critical infrastructure, including those in health, such as hospitals, and fuel distribution, potentially utilising backup generators to maintain services to critical sites.

Voluntary, Community and Faith Sector. The VCFS organisations should work alongside local authorities to provide welfare support to vulnerable people, particularly those on the Priority Service Register who may be impacted by power cuts.

Recovery

Most customers would be reconnected on a staggered basis within hours. However, when damage is widespread, or impacts more remote locations, it could take up to 2 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.

Impact on vulnerable people

Customers on the Priority Services Register will receive additional support to help cope with cascading impacts, including welfare provisions to support vulnerable people who have lost power, such as food vouchers, accommodation and tailored support to meet their needs. The Energy Networks Association (ENA) has a free-to-dial 105 service which connects consumers experiencing power outages to their local network operator and the GOV.UK Prepare website has a dedicated sector for power outage preparation.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- contaminated environment or the presence of potentially hazardous materials
- potential need for some people to be evacuated
- disruption to essential services (including health, food, transport, communications, water supply and sewage)
- potential changes in public behaviour

National gas and electricity shortfall

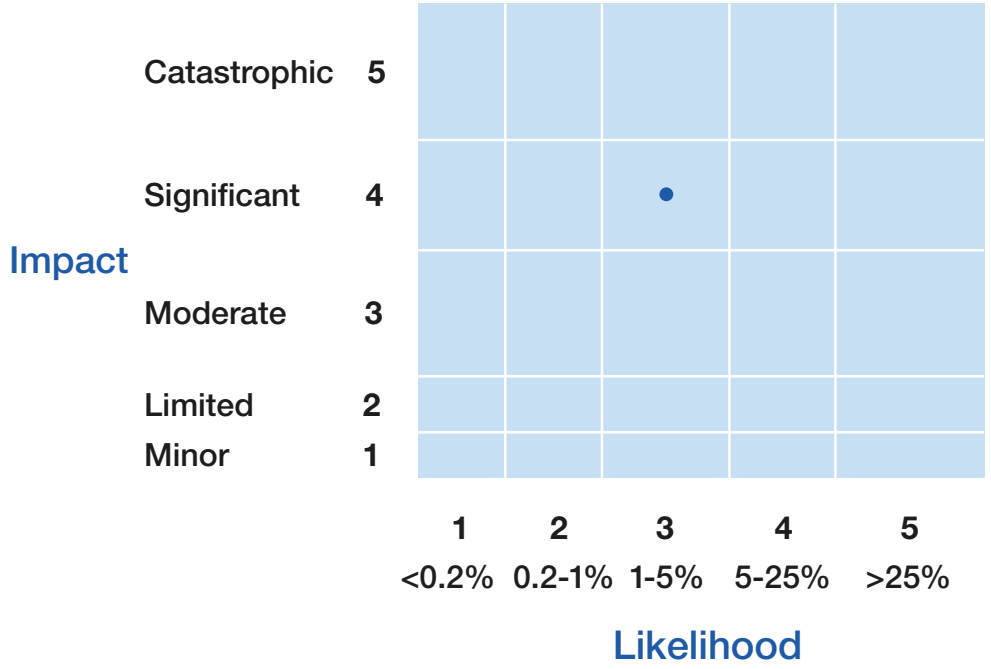
Natural gas is a crucial fuel source that is used to heat homes and businesses, generate electricity, or act as a feedstock for industrial processes across the UK. Great Britain has diverse and highly resilient gas and electricity networks and a National Gas shortfall has never occurred in Great Britain. Industry works to continuously minimise the risk of unplanned disruption while taking the risk of such outages into account in forward planning.

Scenario

The reasonable worst-case scenario is based on a technical failure which results in a significant loss of gas supply capacity to Great Britain. This would cause a national shortfall of gas supply, requiring emergency measures to balance the gas network. While domestic gas customers and some critical users are prioritised from gas disconnection, the majority of industrial gas users, including electricity generators, will be instructed to cease taking gas, causing significant cascading impacts. 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 may be required to balance supply and demand. This could affect between 1 and 11 million customers for a period of over two months. While domestic gas supply is maintained, widespread power cuts would pose significant risks to public health and welfare, particularly for those reliant on electrically powered medical equipment or heating controls. Within this process, some critical sites would be protected from electricity 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.

Key assumptions for this scenario

The scenario assumes that impacts would be greatest during a severe winter that sees high consumer demand where there is more reliance on gas supplies for heating.



Variations

Electricity shortfall occurs independently of gas supply issues. This could be from high electricity demand leading to a national electricity shortfall, however, impacts to electricity supply will occur for a shorter period of time (up to a week).

Response capability requirements

Government and Agencies. The government activates the National Emergency Plan for Downstream Gas and Electricity. The Secretary of State for Energy Security and Net Zero initiates the Electricity Supply Emergency Code (ESEC) to manage demand disconnections. The National Energy System Operator (NESO) will publish rolling out rotas up to 7 days in advance to enable households and businesses to prepare for power outages using block letters, which can be found on energy bills and the Powercut 105 website. This is to ensure the electricity system remains in balance.

CNI and Wider Private Sector. There would need to be preparations in place to support wider recovery and the continued operation of CNI, including those in health, such as hospitals, and fuel distribution, would ensure continued operation, potentially utilising backup generators to maintain services to critical sites.

Voluntary, Community and Faith Sector. Organisations may assist by supporting vulnerable households, particularly those struggling with the lack of heating or access to necessary medical treatment due to rolling power cuts.

Recovery

Restoration of the affected gas infrastructure could take approximately 3 months. However, rolling power cuts would likely end sooner than this, once the gas shortfall is resolved through other supply points. It would take a further week for industrial gas customers to be fully restored and weeks or months for some industrial sites to return to normal service.

Impact on vulnerable people

No domestic gas customers will lose supply, but all domestic customers are at risk of being disconnected from electricity supply. Customers will receive advanced notice of any rolling outages to ensure preparations can be made. During outages, customers on the Priority Service Register, including those reliant on continuous electricity supply for medical needs, will receive tailored support from their energy network providers and Local Resilience Forums' partners. The provision of additional welfare provisions such as hot meals and alternative accommodation during the rolling outages (approximately 3-hours at a time) will be assessed based on customer needs, but will also be limited by the widespread nature of the disruption.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including health, transport, food, communications, water supply and sewage, energy, education)
- contaminated environment or the presence of potentially hazardous materials
- potential changes in public behaviour

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

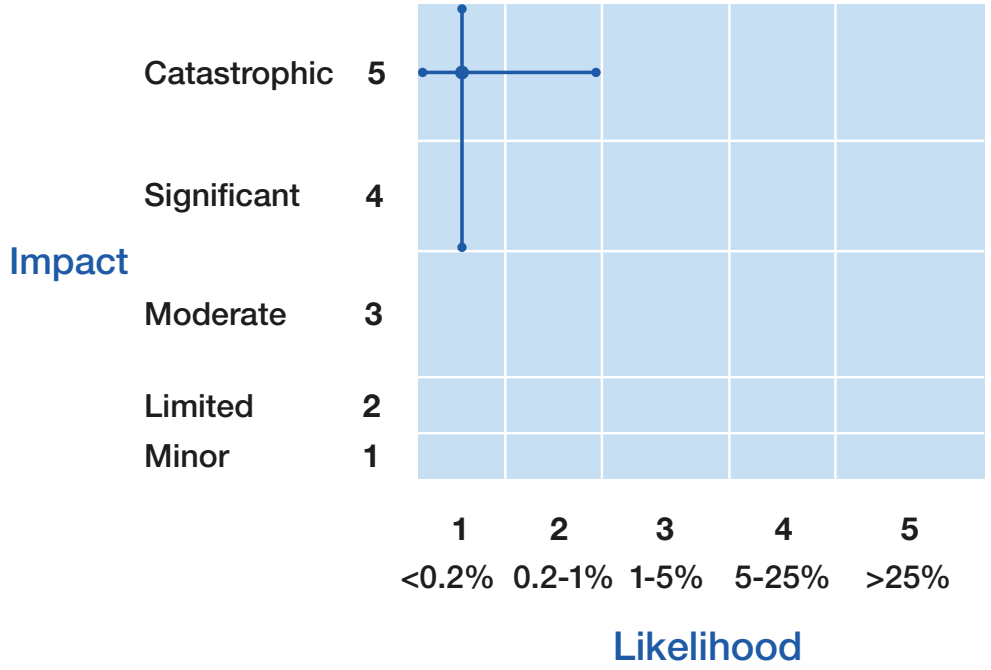
In line with international good practice, the UK's domestic legislation requires planning for a range of scenarios. This scenario is based on an accident occurring at a civil nuclear site that results in a release of radiological material that extends beyond the boundary of the site. Onsite casualties 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

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

Variations

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



Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Nuclear sites should continue to adhere to UK regulations to reduce the likelihood of an accident and should ensure effective mitigations are in place.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people.

Recovery

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

Impact on vulnerable people

Vulnerable people and those with pre-existing medical conditions may be more vulnerable to effects of exposure and they may need extra support with public protective actions.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of hazardous materials
- disruption to essential services (including emergency services, energy, health, food, government services, water supply, communications, education and transport)
- disruption to security of electricity supply
- disruption to financial services
- potential changes in public behaviour

Radiation release from overseas nuclear site

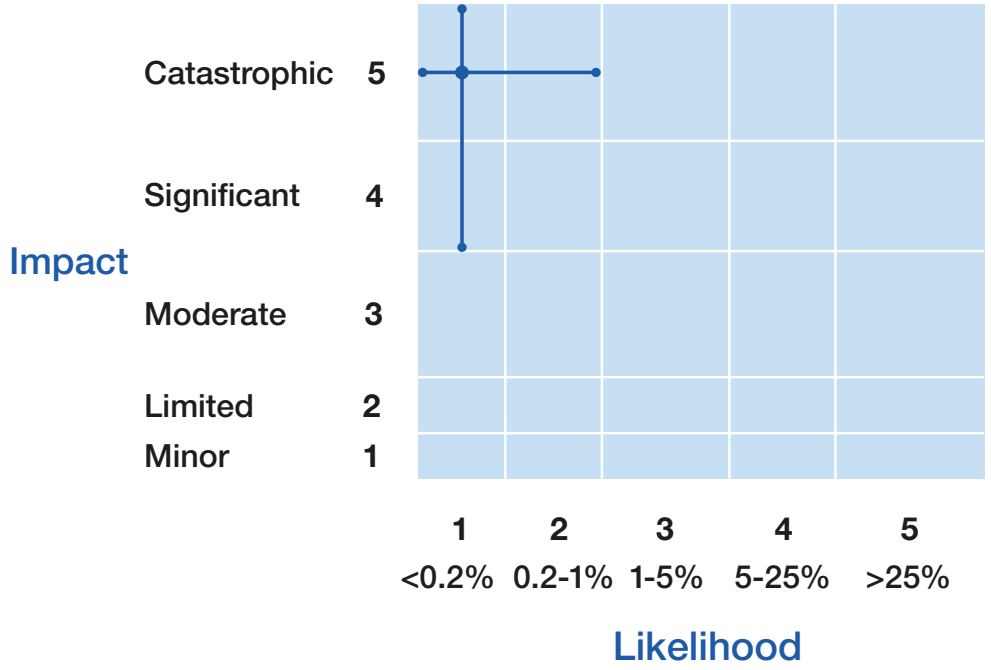
Another risk that the government is planning for is an accident at an overseas nuclear site that results in the release of radiation. Impacts on the UK homeland would most likely be felt if the accident occurred at a site in a country close to the UK as opposed to a geographically distant location. For 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. This scenario 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, site type 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

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



Variations

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

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Humanitarian assistance for foreign nationals and refugees in the UK, alongside international aid for those in the affected country would support recovery.

Recovery

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

Impact on vulnerable people

British nationals in the country where the incident occurs would be vulnerable to the health effects of the radiation.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- overseas response
- contaminated environment resulting from the release of hazardous materials
- disruption to essential services (including health, food, water supply, and transport)
- potential changes in public behaviour

Radiation exposure from transported, stolen or lost goods

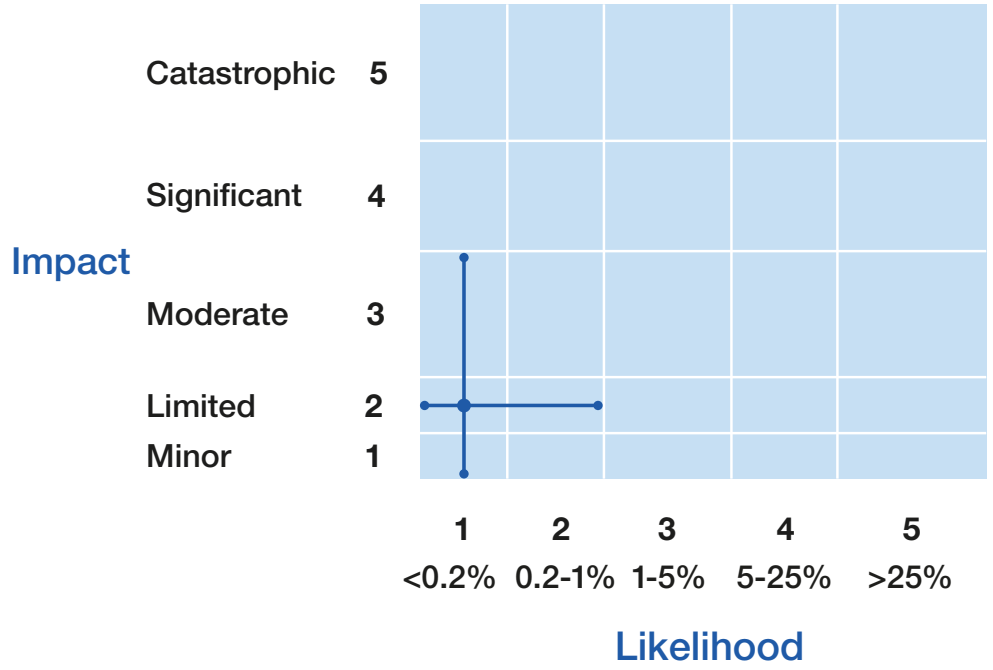
There is a low likelihood that radiation could be released from goods being transported within or into the UK. When these goods are handled correctly by trained professionals, the risk of radiation release is extremely low. However, there is a risk as individuals handling transported, stolen or lost goods are unlikely to have the appropriate training. The scenario used 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.

Key assumptions

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.



Variations

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.

Response capability requirements

Government and Agencies. 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 and waste management capability would also be impacted. DESNZ has an arrangement with UKHSA who conduct radiological effects modelling on our behalf. We can obtain data from regulators on source holder compliance and from the Orphan source arrangements which can inform historic and current frequency of incidents to inform likelihood.

CNI and Wider Private Sector. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Recovery

Health impacts among the affected workers would be expected for a number of years, with a requirement for long-term medical supervision. Decontamination would take several weeks and require extensive resources.

Impact on vulnerable people

Those in close proximity would be most vulnerable to the radiation's effects, including workers. Workers with pre-existing medical conditions may be disproportionately impacted.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including education) and to security
- potential changes in public behaviour

Technological failure at a systemically important retail bank

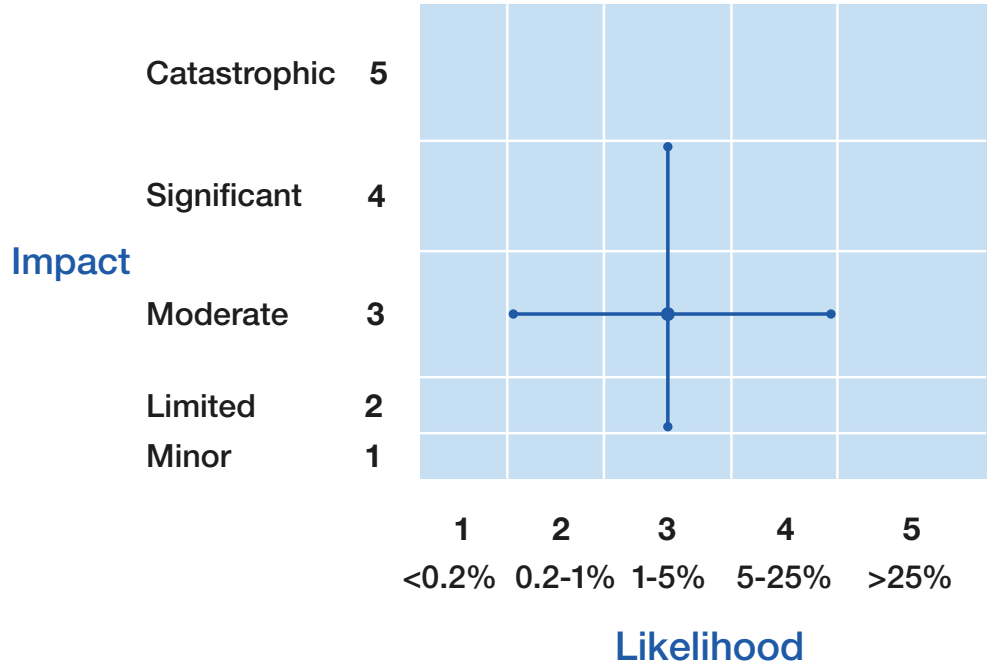
The increasing digitisation of financial services means that a technological failure of IT systems could result in customers being unable to access key account functions and important information, including online banking. The financial regulators' operational resilience policy requires finance sector 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 for at least 2 days, 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.



Key assumptions

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.

Variations

Technological failure of a UK critical financial market infrastructure.

Response capability requirements

Government and Agencies. 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).

CNI and Wider Private Sector. 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, which reached its initial implementation milestone in spring 2025, requires regulated firms to set impact tolerances and remain within these.

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.

Impact on vulnerable people

The most significant impact would be felt by vulnerable customers with only a single bank account. This scenario could also disproportionately impact older people, those on lower incomes, people with disabilities, those living on weekly payments, living in poverty, or in receipt of benefit payments.

Common consequences

The exact consequences will be dependent on the nature of the incident, but could include disruption to financial services, disruption to government services and potential changes in public behaviour.

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.

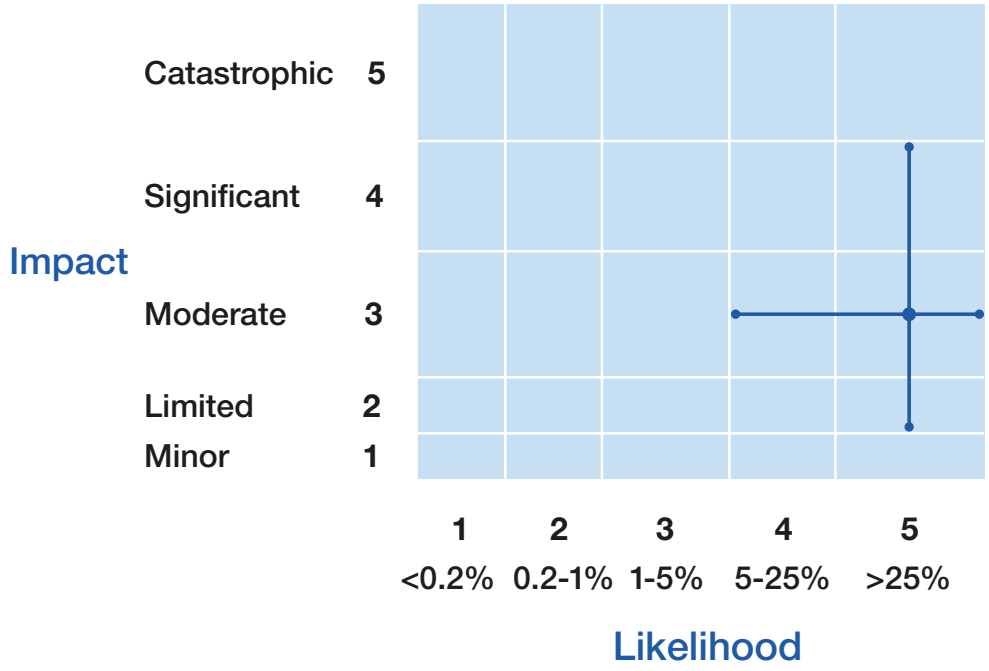
This supervisory framework covers FMIs and other systemically important institutions (O-SIIs), critical to the UK's financial stability, who must also consider their risks in relation to harm their institution may cause to the real economy and financial services sector as a whole.

Scenario

This scenario is based on a technological systems failure causing an outage of a systemically important UK financial market infrastructure (FMI) for at least 5 days. 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

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

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

Response capability requirements

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

CNI and Wider Private Sector. 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, which reached its initial implementation milestone in spring 2025, requires regulated firms to set impact tolerances and remain within these.

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.

Impact on vulnerable people

Depending on the exact nature of the incident and the FMI impacted, this could impact those on lower incomes, weekly payments, living in poverty, or in receipt of benefit payments.

Common consequences

The exact consequences will be dependent on the nature of the incident, but could include disruption to financial services, disruption to government services and potential changes in public behaviour.

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

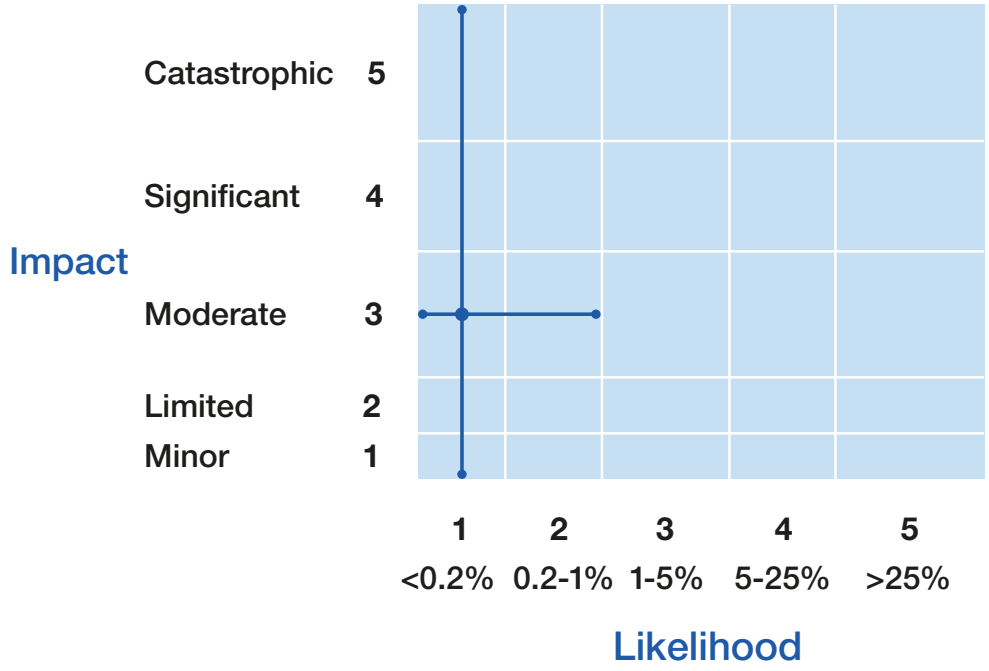
The reasonable worst-case scenario for this risk concerns a major fire and/or explosion occurring at an onshore COMAH site, potentially causing building damage and possible collapse close to the site. The fire would generate a visible plume of smoke that may travel to nearby areas. The accident could 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

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

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

Government and Agencies. 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 involve search and rescue teams.

CNI and Wider Private Sector. Operators of COMAH sites should follow the legal duty to prevent accidents from occurring and to mitigate their consequences.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people.

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.

Impact on vulnerable people

Those with pre-existing health conditions, such as reduced lung function or heart conditions will be more severely affected by exposure to respiratory irritants such as smoke. Whilst those will mobility challenges may be less able to self-evacuate.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services, energy, health, education and transport)
- potential changes in public behaviour

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

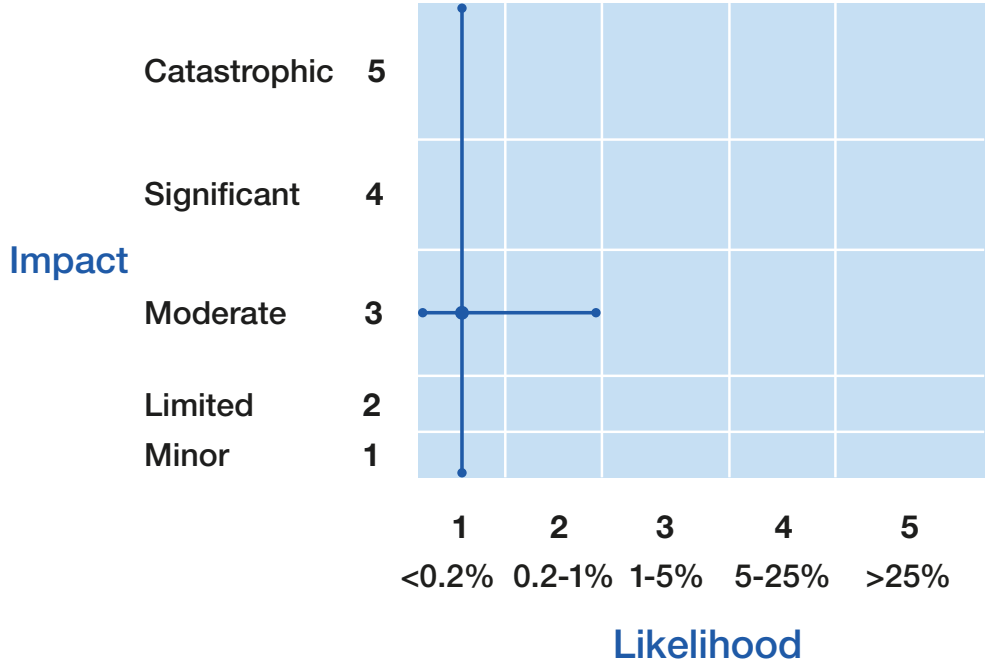
This risk is concerning an incident in which a toxic gas is accidentally released from a Control of Major Accident Hazards (COMAH) site in the UK. There are two types (tiers) of establishment that are subject to COMAH regulations, known as 'Upper Tier' and 'Lower Tier'. Upper Tier establishments hold 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 people disproportionately affected.

Key assumptions

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

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 but larger impacts, or a lower-scale release of toxic gas with smaller impacts.

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Operators of COMAH sites should follow the legal duty to prevent accidents from occurring and to mitigate their consequences.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people.

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.

Impact on vulnerable people

Those with pre-existing health conditions, such as reduced lung function or heart conditions will be more severely affected by exposure to respiratory irritants such as chlorine or ammonia. Whilst those will mobility challenges may be less able to self-evacuate.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services, health, food, water supply, sewage management, education and transport)
- potential changes in public behaviour

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

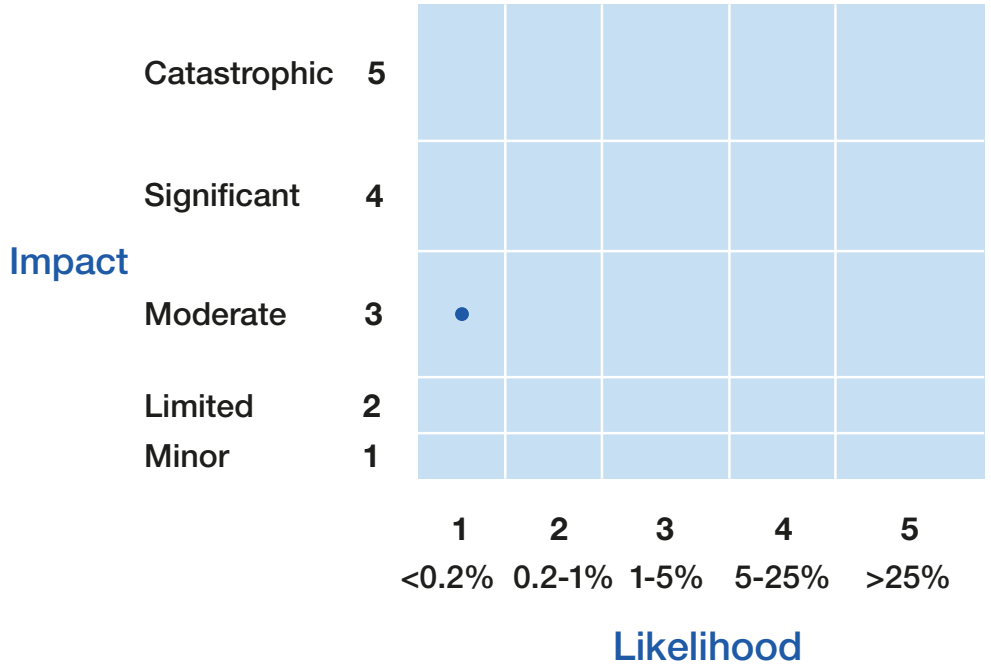
The reasonable worst-case scenario for this risk is a fire or explosion occurring on an offshore oil or gas installation. The incident would be local to the site resulting in casualties and fatalities. There could also be environmental damage. The incident may cause supply issues depending on the type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

Key assumptions

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

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

Government and Agencies. Government and Local Resilience Forums' partners (LRFs) would coordinate with installation to support where needed. For example, onshore the NHS will play a key role receiving any evacuated casualties and fatalities.

CNI and Wider Private Sector. 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.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support those who may become vulnerable following the incident.

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.

Impact on vulnerable people

All offshore personnel have to be medically assessed and certified as fit to work in this type of environment and therefore are unlikely to have pre-existing conditions or additional support requirements. However, the incident and exposure to the fire may cause new forms of vulnerability which may need longer-term support.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services, health and energy)
- potential changes in public behaviour

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 1 km 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.

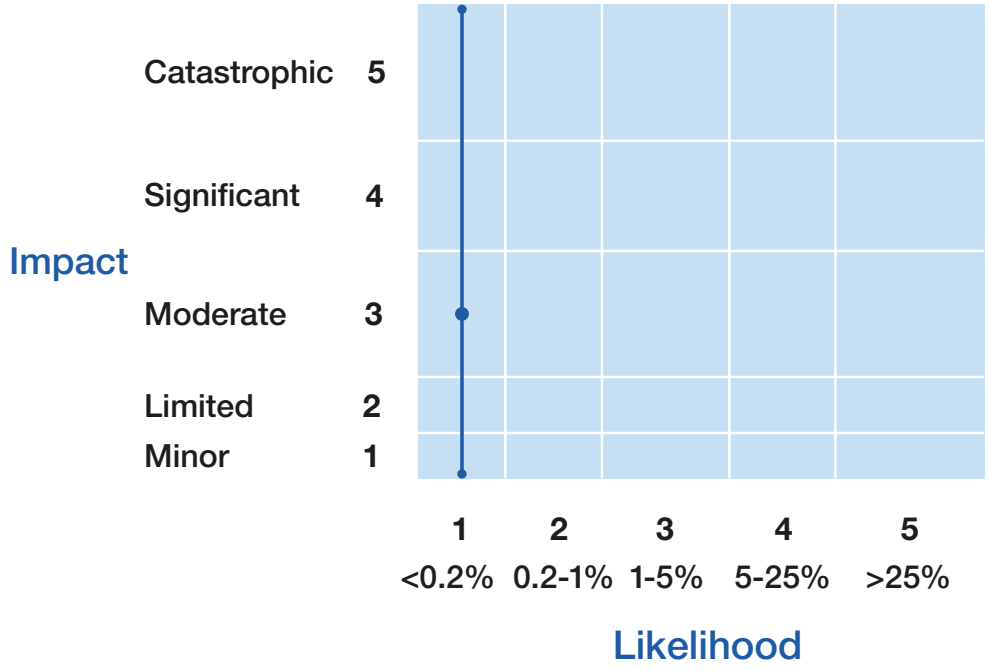
Key assumptions

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

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

Government and Agencies. 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.

CNI and Wider Private Sector. 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.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support those who are vulnerable.

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.

Impact on vulnerable people

Some chemicals may have potential to compromise the health of vulnerable members of the population, for example, by increasing the decline of lung function for those with existing bronchial problems. Evacuation may result in the need for additional support to help manage people's pre-existing medical conditions.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services, health, energy, education and transport)
- potential changes in public behaviour

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

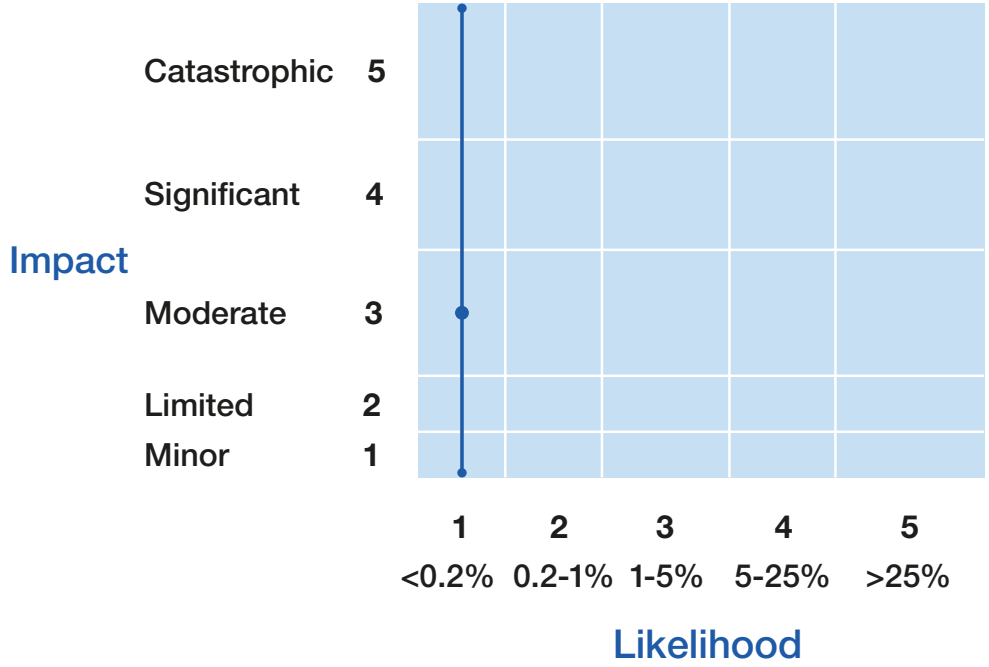
The reasonable worst-case scenario is based on an accidental fire or explosion occurring at a MAHP situated close to an urban area. The ignition of flammable gas or liquids under high pressure would result in a loud explosion, which could cause a crater, building damage and require evacuation from homes. 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

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

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

Government and Agencies. The Pipelines Safety Regulations 1996 (PSR) require a local authority to prepare emergency plans for pipelines which have the potential to cause a major accident (known as MAHPs). The pipeline operators' emergency procedures then inform capability requirements locally.

CNI and Wider Private Sector. The Regulations also require a pipeline operator 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. Temporary evacuation and shelter for displaced people, site clearance plans and infrastructure repair may be required.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support those who are vulnerable.

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.

Impact on vulnerable people

Any impacts may be affected by the weather conditions e.g. if the incident occurs during a period of very cold weather then people may feel the effects of the lack of heating sooner if the incident results in localised disruption to domestic supply. Those particularly vulnerable to these impacts would include the very young, the elderly and those with pre-existing medical conditions. There may be long lasting effects for some people, for example continued respiratory issues in those with pre-existing medical conditions. Evacuation may result in the need for additional support to help manage people's pre-existing medical conditions.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- disruption to essential services (including emergency services, health, energy, education and transport)
- potential changes in public behaviour

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

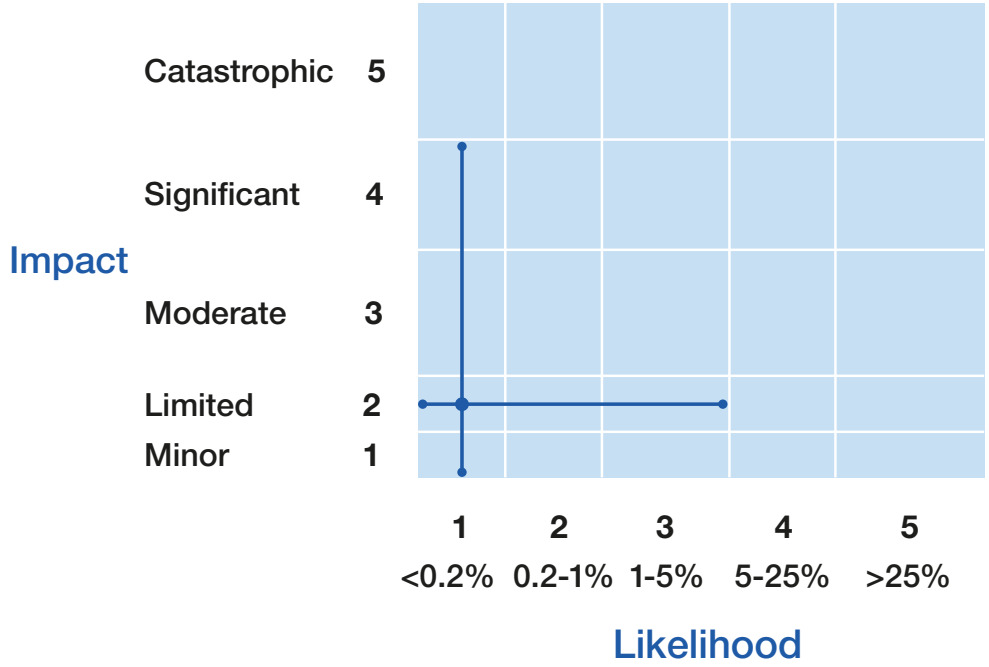
This risk involves the accidental release of a hazardous pathogen from a laboratory in the UK. Operators of these sites must meet strict containment and safety requirements to work with these types of pathogens and develop emergency procedures to mitigate this risk. The UK has a well-established regulatory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

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

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

Government and Agencies. 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.

CNI and Wider Private Sector. Operators of these sites must meet strict containment and safety requirements to reduce the likelihood of the risk occurring and robust mitigations measures should also be in place.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support those who are vulnerable.

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.

Impact on vulnerable people

It is unknown if this particular type of influenza would be more virulent in certain people; however, generally, the elderly, the very young, those with compromised immune systems (including pregnant women) and those with pre-existing respiratory conditions are more affected by seasonal influenza, leading to more severe infections, longer periods of hospitalisation and increased risk of mortality.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- potential changes in public behaviour

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

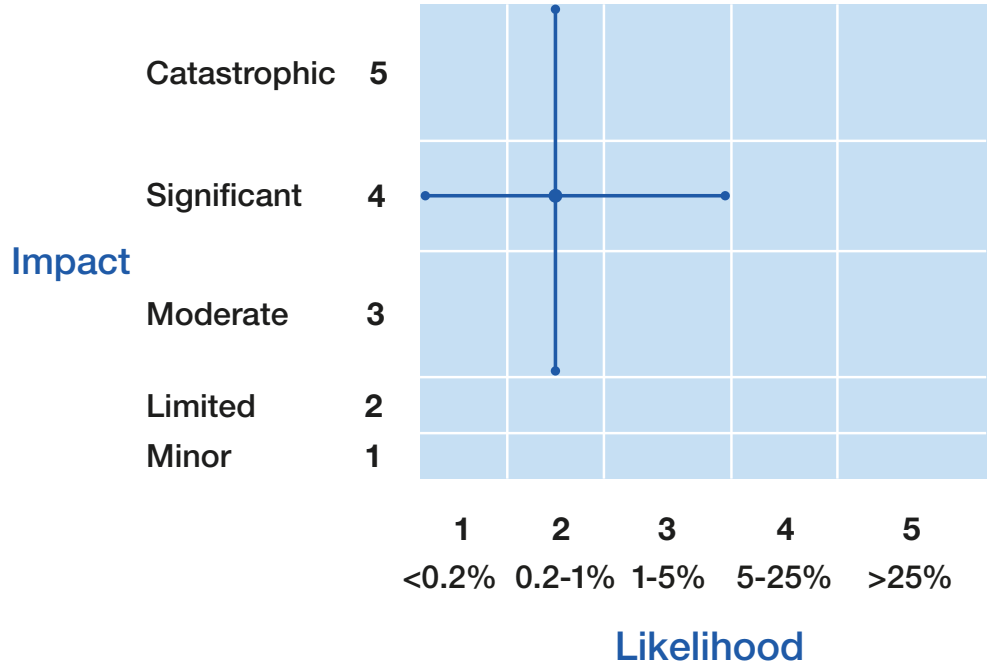
The reasonable worst-case scenario is based on a sudden collapse of a dam without warning. This would result in flooding, with a substantial quantity of water moving at high speed. There would be casualties, fatalities and significant mental health impacts. Utilities to nearby homes and businesses would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

Key assumptions

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

Variations

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



Response capability requirements

Government and Agencies. Reservoir owners and Local Resilience Forums' partners 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 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 across the country. The joint Department for Environment, Food and Rural Affairs (Defra)/ Cabinet Office National Flood Response Centre would coordinate the national UK response to the incident.

CNI and Wider Private Sector. Since 2020, Defra has made it a legal requirement for all owners of large raised reservoirs to have on-site emergency flood plans.

Voluntary, Community and Faith Sector. The VCFS would be encouraged to engage with local authorities to support vulnerable people and communities.

Recovery

There would be major economic, environmental, infrastructure and humanitarian implications of the collapse. Key aspects of immediate recovery would involve searching for missing people buried by rubble and sediment, evacuation and shelter of populations, temporary accommodation and clean-up of contaminated urban and agricultural land and large-scale environmental damage. There would also need to be repairs to damaged infrastructure over the longer term.

Impact on vulnerable people

Those with mobility challenges, people affected by physical or mental illness, children and the elderly are all likely to be disproportionately impacted.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- properties affected by flooding
- potential need for some people to be evacuated
- potential human and animal health impacts, which may include physical casualties, impacts on mental health and fatalities – saving lives and protecting communities from the dangers of flooding will be a top strategic priority
- disruption to essential services (including emergency services, health, food, energy, communications, water supply, sewage management, education and transport)
- disruption to security
- disruption to financial services in the affected area
- potential changes in public behaviour

Water infrastructure failure or loss of drinking water

The failure of critical water infrastructure serving a large urban area would result in the loss of drinking water supply to a large population. An incident of this magnitude is likely to overwhelm the capacity of the water sector to provide alternative water via tankers or bottles and require evacuation of households and closure of businesses in the affected area.

Scenario

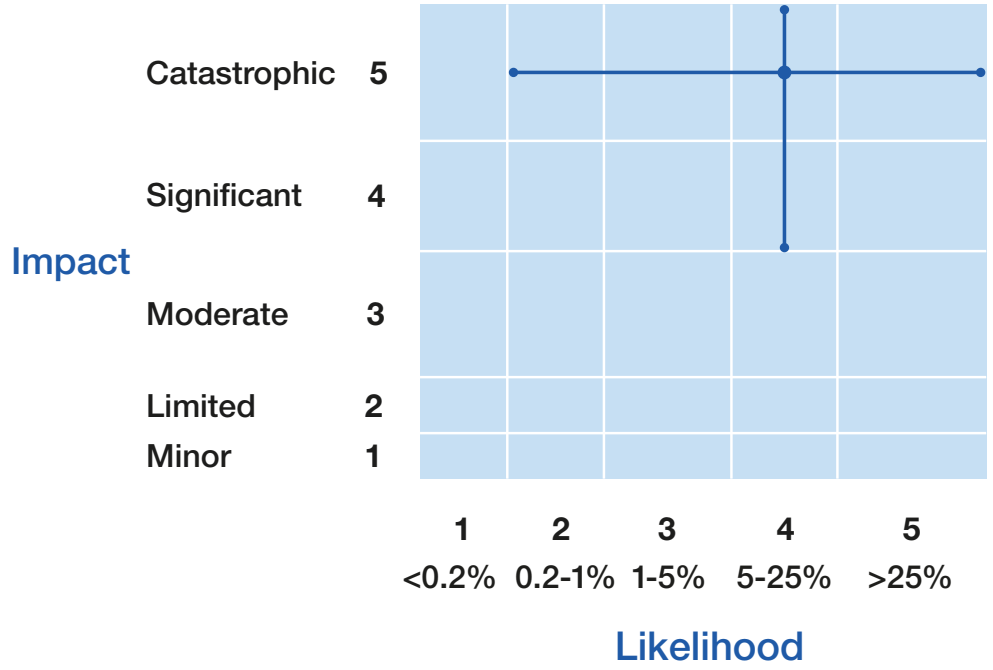
Significant damage to water infrastructure that supplies a large urban area, resulting in the loss of piped drinking water and impact to wastewater services for over one million people. This would have knock-on consequences to the functioning of essential services such as schools, hospitals, care homes and prisons until alternative water supplies are provided or supply is restored. Due to the impact on health and sanitation, residents would likely have to leave the area, and some may require evacuation. It is likely that repair of the infrastructure could take months.

Key assumptions for this scenario

This would be a regional event. There would be limited capability in the water network to reroute supplies from elsewhere through the pipe network.

Variations of this scenario

There are different scenarios that could result in the loss of water supply of this magnitude, including power failure, supply shocks and extreme weather incidents, however the capabilities required to respond to the impacts would remain broadly the same.



Response capability requirements

Government and Agencies. The response may necessitate government intervention to manage large-scale evacuation to unaffected areas as well as shelter arrangements if standard operational capabilities are exceeded. Water is a devolved matter and Wales, Northern Ireland and Scotland have equivalent requirements in place.

CNI and Wider Private Sector. Water companies in England are required to maintain contingency plans for disruptive scenarios. However, maintaining an alternative water supply for a population of this magnitude in situ would present significant logistical challenges, requiring infrastructure and personnel resources beyond standard operational capabilities.

Voluntary, Community and Faith Sector. Organisations may assist in supporting large-scale evacuation and shelter arrangements necessary to relocate affected residents to unaffected areas and support them for the duration of the incident.

Recovery

Infrastructure repair could take several months. Consumers are likely to be gradually brought back on to supply in stages as their area is reconnected. Piped supply would be restored as soon as possible but would be dependent on the extent of the damage to the water infrastructure.

Impact on vulnerable people

Water companies are required to provide water to all domestic customers whilst prioritising provision of alternative water to those 'at risk'. However, transient vulnerabilities would inevitably emerge among the populations unable or unwilling to evacuate. Within days the numbers of people classed as vulnerable – given the fact that everyone needs drinking water – would rapidly rise. An incident of this scale may therefore rapidly overcome the capacity of providing alternative water.

Common consequences

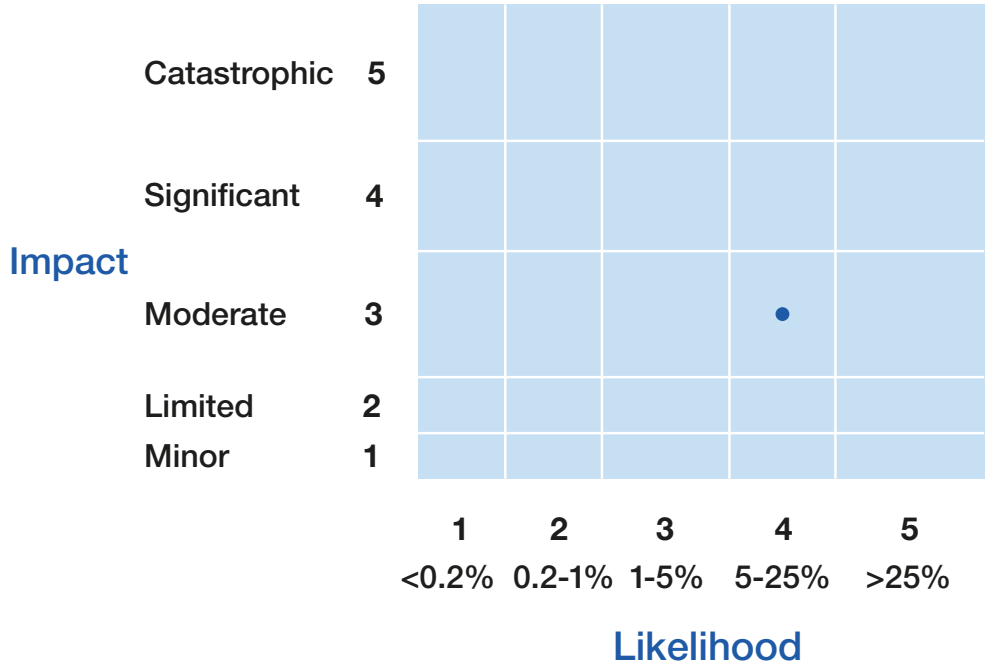
- Human health impacts, which may include physical casualties, mental health casualties and fatalities
- Disruption to essential services (including health, transport, food, government services, communications, education)
- Public behaviour and societal cohesion – pro-social and anti-social behaviours, impacts from displacement of communities

Food supply contamination

The contamination of food products with pathogens such as Salmonella, Listeria or Shiga toxin-producing Escherichia Coli (STEC) represents a significant threat to public health. Contamination may result from processing failures, cross-contamination, poor hygiene, inappropriate storage or contamination with animal waste. The Food Standards Agency (FSA) estimates that foodborne pathogens are responsible for 2.4 million cases of disease in the UK each year, at a cost of £11.9 billion. The FSA and FSS prioritises keeping the level of foodborne disease low through inspecting, auditing, and assuring businesses in England, Wales, Northern Ireland and Scotland 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 or the production of toxins from pathogens that cause harm 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, dairies, livestock production areas). Trust in the food system will be impacted, and consumer confidence might also be affected, leading to lost markets and, where staple products are affected, adaptive purchasing behaviours.



Key assumptions

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

This type of pathogen, or the toxin it produces, could be present in other products at different levels resulting in a range of severities of illness. A different pathogen may also be present in similar products.

Response capability requirements

Government and Agencies. Response capabilities to effectively manage such a scenario would include close liaison between the FSA, other government departments, public health agencies and local authorities, possible decontamination services to clear up the site of the incident and mitigation of the risk e.g. consumer advice/guidance, of widespread loss of consumer confidence in food. The response should ensure food security and continued supply of safe food, particularly for vulnerable people for example. infants dependent on infant formula.

CNI and Wider Private Sector. Private sector companies and those involved in key supply chains in the UK need to ensure effective mitigations are in place for potential incidents of contamination to enable collaboration with key partners and effective decontamination.

Voluntary, Community and Faith Sector. Transport and management of resources (acquisition, storage, transportation and distribution of 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. Re-establishing trust in the food system through public communication and guidance.

Impact on vulnerable people

The impact of infection for young children, the elderly and the immunocompromised may be more severe, especially if staple products are affected, or products commonly utilised e.g., infant formula.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including food where certain products could be depleted from shelves)
- contaminated environment resulting from the release of chemical, biological or radiological material, or the presence of potentially hazardous materials
- potential changes in public behaviour and loss of trust in the food system

Major fire

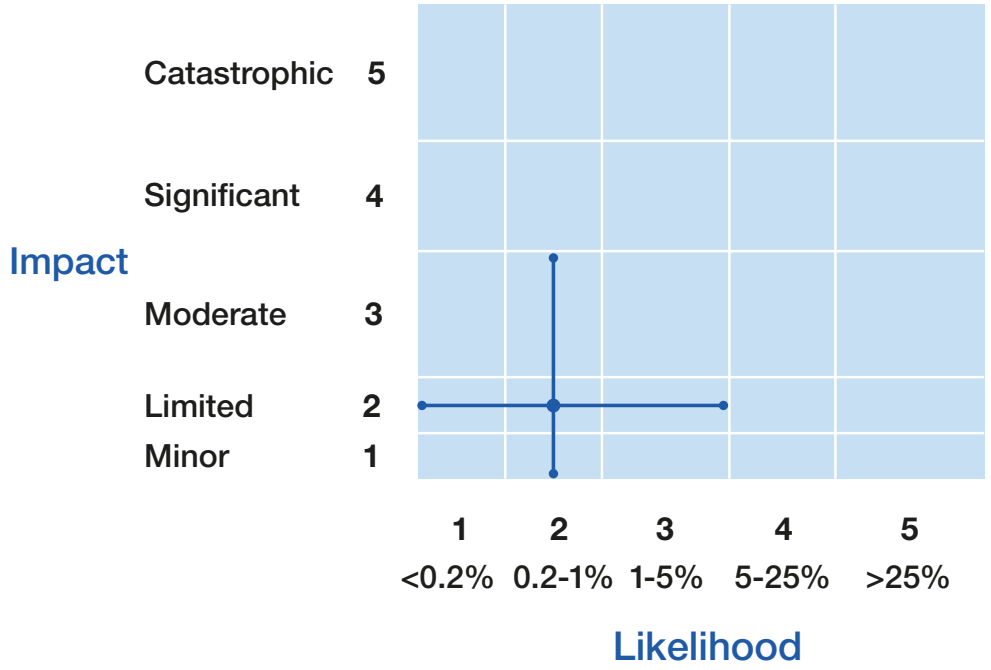
This risk concerns a major fire occurring in the UK. Major fires can start for a variety of reasons, including accidents (for example, electrical faults), human activity that combines ignition sources and fuel, malicious activity (for example, arson), infrastructure incidents (for example, sparks from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

Government and Agencies. Fire and rescue services would lead on the response, including putting out the fire as well as the emergency evacuation and rescue of residents. There could be 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. Disaster Victim Identification (DVI) capabilities are also likely to be required to support identification.

CNI and Wider Private Sector. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Coordinate with local authorities to support the evacuation of those with mobility challenges. Consideration of Residential Personal Emergency Evacuation Plans (rPEEPs) would also be necessary to support the safe evacuation of disabled residents in high-rise settings.

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.

Impact on vulnerable people

The elderly or those with disability are more likely to reside in a care-home; additionally given challenges in mobility likely to be associated with these individuals they may be less likely to self-evacuate than younger or able-bodied persons.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, energy, education and transport)
- disruption to security
- potential changes in public behaviour

National disruption to data infrastructure

In 2025, prolonged power outages in Spain and Portugal led to widespread disruption of digital services, with several data centres experiencing outages and Cloud-based services becoming inaccessible, demonstrating how regional infrastructure shocks can cascade into digital failure.

Data centres were designated as critical national infrastructure in 2024. Under the UK's Cyber Security and Resilience Bill, data centres will be regulated as essential services, providing government and the regulator with the necessary levers to oversee and support the sector, ensuring consistent protection and enabling secure growth. DSIT and the AI Security Institute are continuing to explore how current and emerging AI will continue to influence this risk going forward.

Scenario

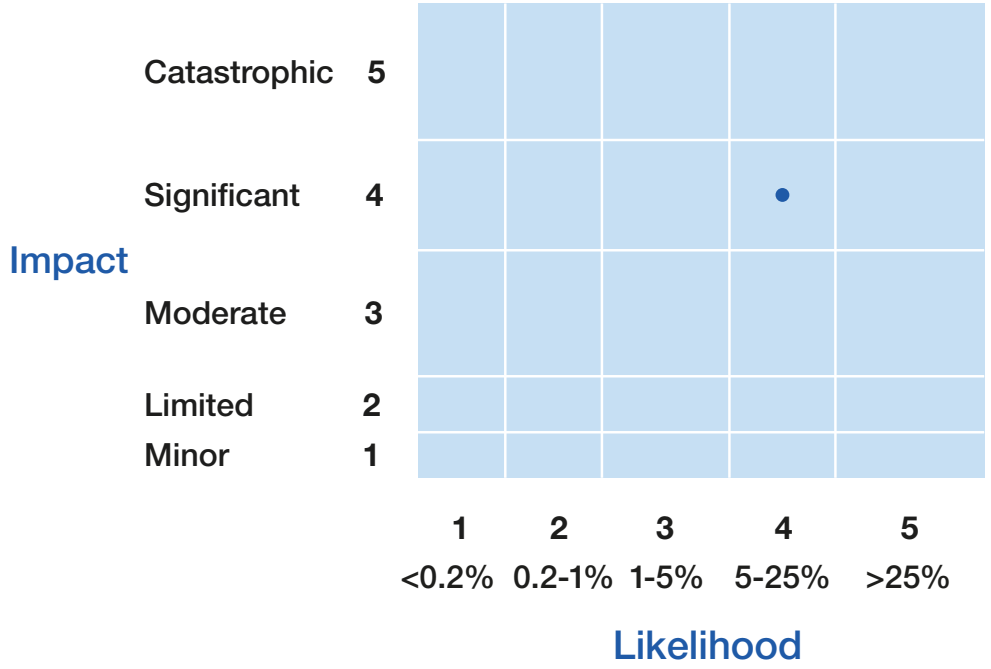
A national disruption affecting UK data centres could cause widespread outages across critical digital infrastructure. This would compromise access to essential public services, disrupt government operations, and undermine national resilience. The impact would be systemic and far-reaching, extending across cloud platforms, core network services, identity and access systems, and data storage environments. The immediate disruption could last from several days to over a week, while full restoration—particularly where physical infrastructure is damaged or where cloud service providers are affected globally—could take months or even years.

Key assumptions

The assessment assumes that disruptions could have major nationwide effects.

Variations

National disruption to data infrastructure could occur from power outages, extreme weather conditions (e.g. flooding or extreme heat) or solar flares, particularly geomagnetic storms.



Response capability requirements

Government and Agencies. A coordinated and multi-agency response would be essential to manage the consequences effectively. The Department for Science, Innovation and Technology (DSIT) will lead the response in central government, and local authorities would also play a critical role, particularly where local services are disrupted. In a widespread power disruption, fuel delivery routes may be compromised. Government, fuel suppliers, and emergency logistics providers would be essential to ensure continuity of power and cooling systems.

CNI and Wider Private Sector. Since most data centres are owned by private entities, the responsibility is ultimately on firms, though the government can support in a crisis. Firms are encouraged to ensure robust response and business continuity plans are in place and should consider backup generation as a critical contingency measure.

Voluntary, Community and Faith Sector. Generalist, and welfare and communications support would greatly assist recovery.

Recovery

Initial efforts would focus on restoring utilities and stabilising systems but face challenges like fuel shortages and physical damage. Such events often cause cascading failures that complicate recovery. Reactivating services must be carefully phased to avoid data loss, with critical functions prioritised. Long-term recovery may involve equipment replacement, regulatory changes, and rebuilding public trust, with full stability taking months or longer.

Impact on vulnerable people

A national-level disruption to data infrastructure would significantly impact vulnerable people by interrupting access to essential services that rely on data centres, such as healthcare, government support and utilities. Under widespread disruption, vulnerable people could face prolonged loss of critical information, services, and communications on which they disproportionately depend.

Common consequences

The exact consequences will be dependent on the specific nature of the disruption; this could include disruption to essential services (including education), disruption to security, and disruption to cyber services.

We expect this risk to link to other planning assumptions. We are developing our knowledge of the risk impacts as it is a new CNI sub-sector.

Digital resilience failure

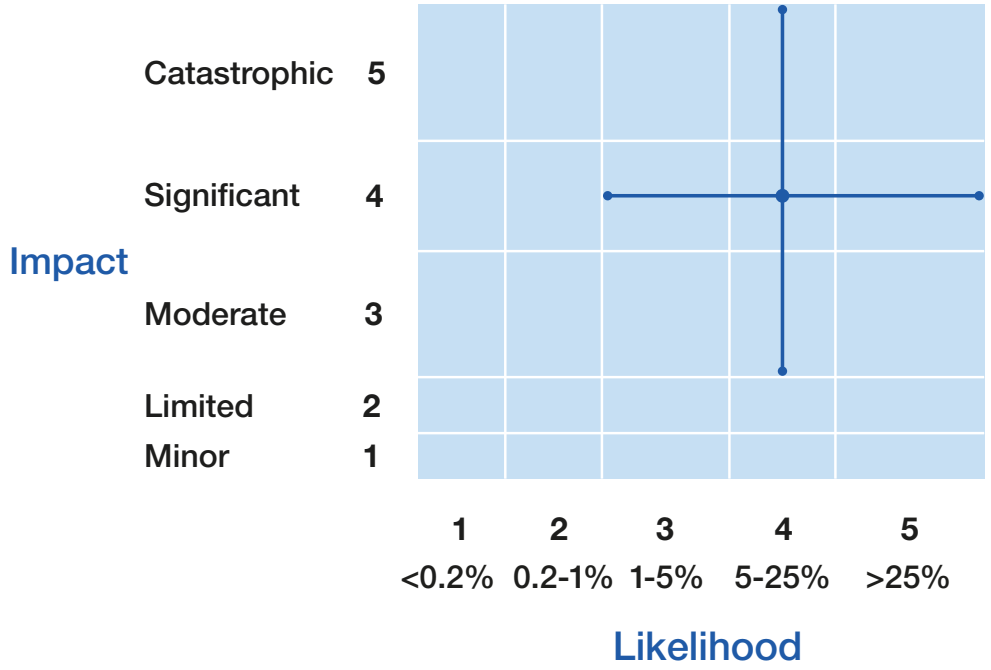
Digital resilience failures are becoming more common. Most instances are small-scale in impact, but there are examples where there is disruption at a national scale. Reasonable worst-case scenarios can range from those that are high in likelihood and low in impact, to low in likelihood but extremely high impact across all sectors. Disruption to critical digital infrastructure for days or weeks can become a national crisis. In 2024, a major IT outage caused by a CrowdStrike software update disrupted thousands of services across the UK, potentially costing the UK economy between £1.7 and £2.3 billion. Despite not being a malicious attack it exposed the risk and the need for a coordinated cross-government response. It showed how a single supplier dependency can create widespread disruption across the public sector and the economy at large.

Scenario

A reasonable scenario for this risk could be a faulty software update that crashes critical servers, relied on across the UK and globally, causing a sudden and widespread digital outage. Key impacts would include shutdown of communications, emergency services, transport, border control, financial systems, and broadcasting, alongside widespread failure of smart devices and smartphones.

Key assumptions

This scenario was not the result of hostile intent, but instead an issue introduced in error to a key dependency. Whilst hostile actors may try and take advantage of the situation, they are not the cause, and damage is not specifically targeted. This is one scenario for digital resilience risk, there are a number of other risks, including supply chain and reliance on large/hyperscale providers risks, that could impact online systems and services at scale.



Variations

We have identified three variations on the risk: a creeping error unnoticed initially but compounded over time, a more limited outage of systems that takes critical systems offline, and a catastrophic loss of data and systems with widespread disruption lasting weeks or months and damage that cannot be restored.

Response capability requirements

Government and Agencies. Government is responsible for managing risks to public systems and services and capabilities to detect, respond to, and recover from outages at national and government levels. Management of this risk is supported by governance, risk management processes and standards for prevention, protection and preparedness. Local Resilience Forums' partners need local contingency planning and testing in case national communications systems fail. Cooperation across governments and agencies would likely be required in the event of global disruptions.

CNI and Wider Private Sector. The private sector plays a key role and has responsibilities to mitigate risks for greater resilience of systems and services. This is supported by standards (codes of practice), and the government is exploring further resilience efforts via policy, the Cyber Security and Resilience Bill and separate, specific CNI regulations.

Voluntary, Community and Faith Sector. The VCFS will play a key role in providing generalist and welfare support to those in need.

Recovery

Time to recover varies, some systems and services could be back online within a few hours, while others could take days, weeks or longer. Regional or global outages take longer to resolve due to the sheer number of affected devices, systems or services and the need for prioritised, phased recovery, across a complex connected landscape with limited information on dependencies and, a high concentration of outdated, legacy technology across the UK and public sector.

Impact on vulnerable people

This could affect those who rely on digital systems for safety, communication and financial support, including young, elderly, disabled individuals, asylum seekers, victims of domestic violence or, those seeking support. Those without access to emergency or support services, essential provisions or, living in isolated areas, may face severe consequences, including injury, hunger, or even death.

Common consequences

The exact consequences will be dependent on the specific nature of the failure; this could include some of the following:

- disruption to essential services (including emergency services, health, transport, communications)
- disruption to security
- disruption to online services including financial and communications services

We expect this risk to link to other planning assumptions. We are developing our knowledge of the risk impacts.

Accidental damage on the National Gas Transmission Network

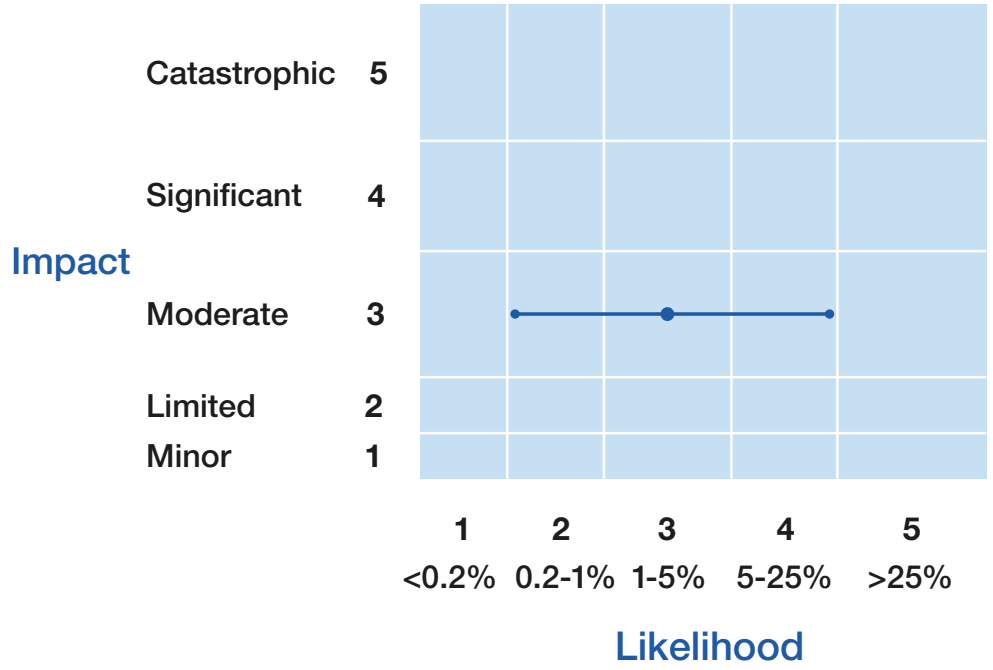
Natural gas is a crucial fuel source that is used to heat homes and businesses, generate electricity or act as a feedstock for industrial processes across the UK. The UK has a diverse and highly resilient gas network. Industry works to continuously minimise the risk of unplanned disruption while taking the risk of such outages into account in forward planning. Accidental damage on the National Gas Transmission Network leading to a regional gas constraint incident has never occurred in the UK at this scale and the likelihood of the risk materialising remains low.

Scenario

On a cold winter day, non-malicious agricultural digging from a third party strikes the National Transmission System (NTS) infrastructure. The accidental damage on NTS infrastructure results in an explosion. A jet flame will emanate from the ruptured infrastructure until the gas is stopped from flowing through the infrastructure, which may take around 12 hours to stop completely due to the high pressure. This may lead to casualties and fatalities for those in the immediate vicinity. Transport routes in the region would be closed and some buildings in the vicinity could catch fire. As a result of the rupture, there is a loss of gas supply to all areas downstream covering surrounding towns. This results in approximately 250,000 domestic and industrial customers, including essential services such as hospitals, losing gas supply for 3 weeks while repairs on the damaged infrastructure takes place. This incident would not, however, lead to a GB-wide gas supply shortfall.

Key assumptions

This reasonable worst-case scenario takes place in winter when it is cold and demand is highest. It is not possible for any customers' gas supply to be restored until repairs are made to the damaged infrastructure.



Variations

Variations depend upon the cause, seasons (for example, summer) and region impacted, and levels of resilience in these areas which may lessen the impact on Great Britain. There are a range of other potential causes of the damage including ground movement, over-pressurisation, mechanical failure or a malicious attack. Any delays to repairs or restoration efforts (for example, if engineers are required to visit all impacted properties to restore supplies) would prolong and worsen impacts.

Response capability requirements

Government and Agencies. The response to an incident of this scale would require multi-agency coordination across Local Resilience Forums, with Strategic Coordinating Groups and Tactical Coordinating Groups. Additional coordination from the central government would also take place.

CNI and Wider Private Sector. National Gas would coordinate the repair of damaged infrastructure. Gas Distribution Networks should also work with The VCFS to support impacted customers. Mutual aid agreements with other distribution networks would be enacted to provide additional welfare provisions, engineers and additional staff to aid in the safe isolation and restoration of customers.

Voluntary, Community and Faith Sector. The VCFS should work with local authorities and GDNs to provide welfare support including heaters, hot plates, warm packs would be provided to impacted customers.

Recovery

It would take approximately 3 weeks to repair the damaged infrastructure. All downstream properties would be isolated until the repair has been completed and gas can safely flow. Once repairs have been made on the NTS infrastructure, homes and businesses can have their supplies restored. Once the Gas Distribution Network board has approved, the GDN Operator will initiate Self Isolation and Restoration and provide customers with details on how to restore supplies back to their properties with vulnerable customers being offered additional support such as house visits to safely restore supplies as quickly as possible.

Impact on vulnerable people

There may be disproportionate impacts on medically dependent customers who are reliant on heating, showers and bathing – for example, keeping wounds clean. There are also risks to the provision of medicine due to closure of sites such as pharmacies. Whilst there will be disruption to some essential services including (hospitals, schools, prisons, care homes etc.) this risk is likely to adversely impact the physical and mental health of those who are reliant on these services.

Common consequences

The exact consequences will be dependent on the nature of the incident; this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, energy, education and transport)
- disruption to security
- potential changes in public behaviour



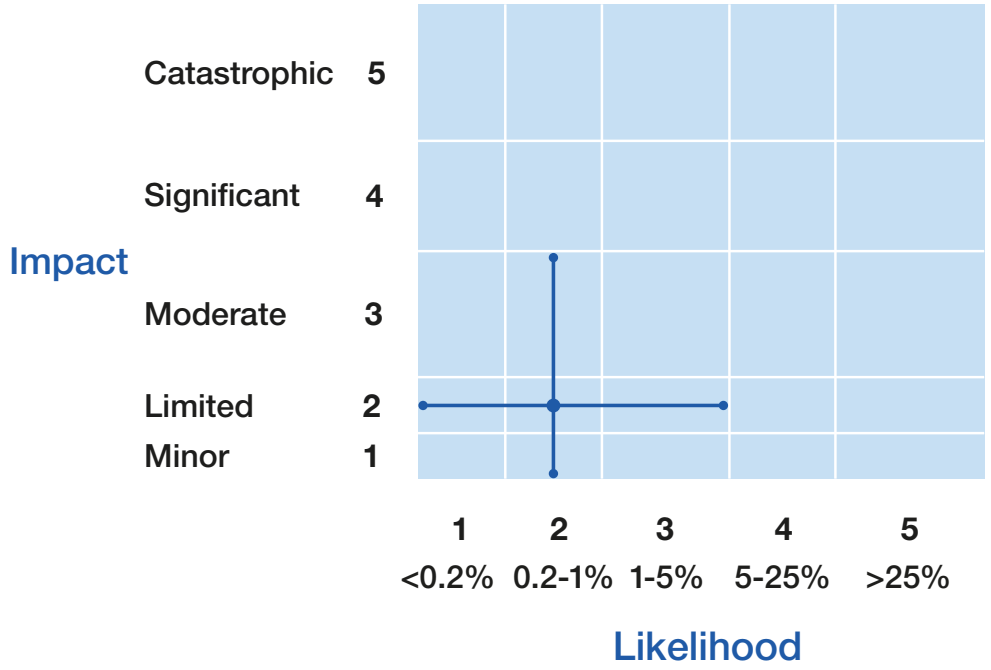
Natural and environmental hazards

Wildfire

A wildfire is an uncontrolled fire that burns vegetation, such as grass, heather, woodland, crops and scrubland. Climate change is leading to changes in the weather patterns that affect the UK, with longer drier summers becoming more common. This leads to drier vegetation and more frequent, larger wildfires – increasing risks to communities and property, disruption to infrastructure and services, as well as environmental impacts including habitat loss, the release of stored carbon and, in some areas, significant effects on vulnerable species. Fire and Rescue Authorities (FRAs) are required to plan for the foreseeable risks in their area, such as wildfires through their Community Risk Management Plan (CRMP). Based on their CRMPs, FRAs determine how best to respond to identified risks. In England, following a Machinery of Government change, the Ministry of Housing, Communities and Local Government (MHCLG) is now the lead government department for wildfire, working across departments and stakeholders, including Defra, to coordinate activity. Fire is a fully devolved matter in Scotland, Wales and Northern Ireland.

Scenario

The reasonable worst-case scenario is based on a sustained and widespread extreme wildfire requiring protracted multi-agency attendance. The peak impacts would likely be during an acute phase of several days, but the entire response may require attendance over weeks or months, 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 property, including homes located at the boundary between rural land and residential areas, as well as critical infrastructure, transport networks, utilities and the environment.



Key assumptions

Wildfires typically occur between February and October, though they can occur year round. There are differences in nature, scale and timing of the risk across the UK. Almost all wildfires in the UK are caused by humans, either deliberately or accidentally.

Variations

Multiple wildfires could take place at the same time as a result of a prolonged period of heat and dry spells. This would impact multiple Fire and Rescue Services (FRS) which would impact mutual aid support.

Response capability requirements

Government and Agencies. Fire and Rescue Services (FRS) would lead on the response putting out the fire and emergency evacuation and rescue of residents. Broader evacuation of 'at risk' areas/population will require support of police and other agencies. FRS response could include utilisation of national capabilities, for example the National Resilience capabilities for wildfire, high-volume water pumps, and Urban Search and Rescue (USAR) assets to help move equipment. Mutual aid from unaffected fire and rescue services would be requested. Other emergency services and agencies are likely to play a role in the response and be coordinated through Local Resilience Forum arrangements (LRFs). Military assistance may be requested if this capacity and/or capability becomes exhausted.

Voluntary Community and Faith Sector. Humanitarian organisations could provide additional assistance for evacuating older populations and those with reduced mobility. Also for volunteering roles in fire prone areas during periods of heightened risk.

CNI and Wider Private Sector. Companies involved in key supply chains are encouraged to ensure they have effective contingency plans in place as wildfires can affect availability of some commodities and transport can be disrupted. Response activity may also involve cooperation with landowners, land managers and environmental organisations. This may involve providing local knowledge and facilitating response activity.

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. Significant wildfires may require sustained recovery activity across affected communities. This could include repairing or rebuilding damaged property, restoration of utilities and transport infrastructure, and support to displaced residents. There may also be health and wellbeing impacts, including from smoke exposure and the psychological effects of evacuation, property loss, or sustained disruption.

Impact on vulnerable people

This risk would disproportionately affect vulnerable people such as those with respiratory conditions like asthma, and those with reduced mobility either due to additional challenges evacuating or due to potential risks of being caught out by a fast-moving wildfire.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for evacuations
- disruption to essential services (including emergency services, transport, energy and water supply)
- disruption to security
- disruption to business
- potential changes in public behaviour
- damage to the natural environment, including natural habitats, water courses and productive land uses such as farming and forestry
- release of stored carbon to the atmosphere
- destruction of property
- potential impacts to critical national infrastructure
- potential impacts on local health services
- wildfire smoke can contain pollutants that are known to be hazardous to human health

Volcanic eruption

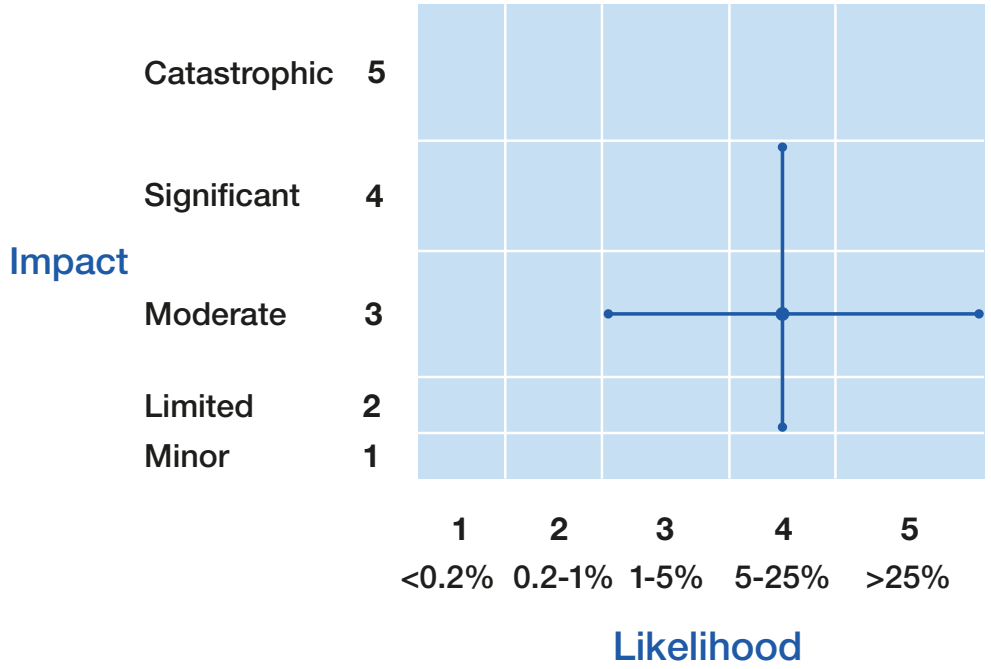
There are several volcanoes across Europe that could affect the UK, such as Santorini in the Aegean Sea and Vesuvius in Italy. However, volcanoes in Iceland (such as Bárðarbunga and Eyjafjallajökull) are of most concern because they are close to the UK and could impact a high volume of air traffic across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

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, 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. 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

Volcanic eruptions are unpredictable in nature and their severity and impact can be vastly different depending on the type. 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 before a full eruption occurs, including volcanic earthquakes, seismic tremor (vibration), ground deformation (changes in elevation), gas emissions or meltwater from glaciers.



Variations

A gas-rich volcanic eruption is a less likely, less impactful manifestation of the risk. The risk to aircraft is likely to be limited but could lead to short-term disruption. A lower-impact, higher-probability scenario could see a volcanic eruption with explosive phases over a 2-week period but with smaller ash plumes or winds that carry the ash away from the UK. This would result in ash concentrations in the UK not being sufficient to cause significant travel disruption, but concerns could lead to people postponing 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 scenario. The eruption could lead to an international humanitarian crisis and include major disruption to supply chains, international displacement, and hazardous weather

Response capability requirements

Government and Agencies. 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.

Voluntary Community and Faith Sector. Humanitarian organisations with a presence abroad could provide additional assistance evacuating older populations and those with reduced mobility in the area at risk of eruption.

CNI and Wider Private Sector. Airlines should follow London Volcanic Ash Advisory Centre guidance. Some airlines already have safety cases in place, and are allowed to operate if they are satisfied that no high-density ash is present at the actual time of flight.

Recovery

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

Impact on vulnerable people

British nationals stranded overseas may be disproportionately impacted if they are elderly, have underlying health conditions or are children. It is unlikely that there would be serious health risks to aircraft occupants in or near UK airspace, but respiratory irritation is likely for large eruptions. Asthmatics in the UK are particularly vulnerable, and even a relatively low and short exposure can be potentially severe.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- overseas response
- disruption to essential services (including health and transport)
- disruption to security
- potential changes in public behaviour

Earthquake

Significant earthquakes in the UK are rare, and an earthquake powerful enough to inflict severe damage is unlikely. Each year, the UK experiences around 200-300 earthquakes but only 10% of these are powerful enough to be noticed by people even slightly. There is an increased chance of damage occurring and of that damage being severe, in historical buildings.

Scenario

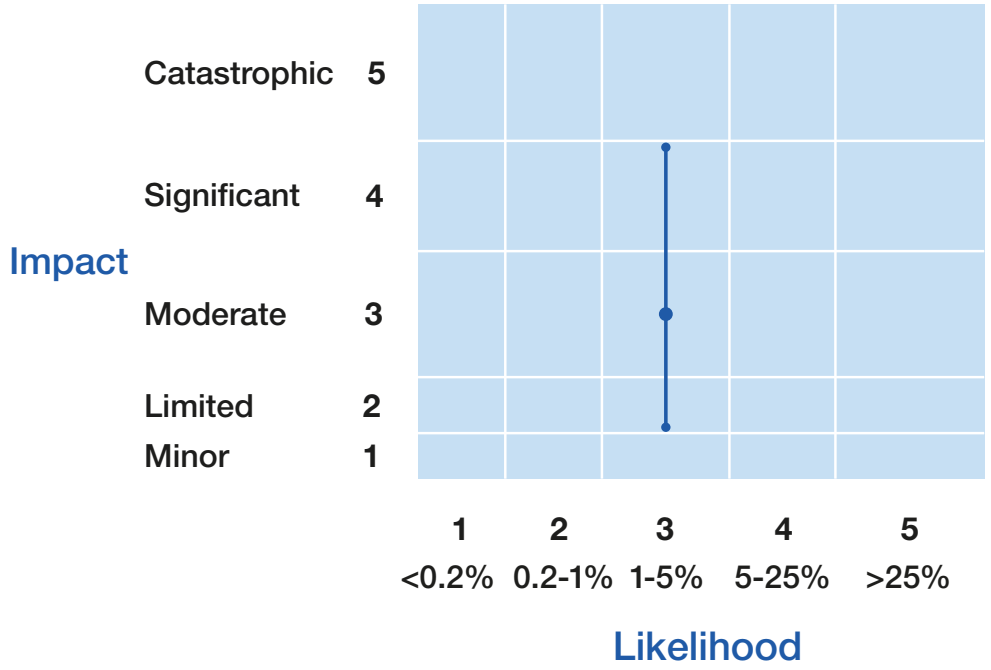
The reasonable worst-case scenario is based on earthquake activity in the UK that results in the ground shaking with an intensity up to 8 on the EMS,[2] which may cause damage to buildings and infrastructure and could result in a small number of fatalities and casualties due to falling masonry or interior damage. Damage to buildings would range from moderate to severe, for example from extensive cracks in walls to complete collapse of chimneys. Such an earthquake may cause short-term but significant disruption to power, infrastructure, transport and communications, even if the physical damage is comparatively minor.

Key assumptions

The risk assumes that no critical infrastructure is damaged to an extent that overwhelms existing emergency plans.

Variations

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



2 The European Macroseismic Scale (EMS) is an assessment tool of scale of an earthquake's impact, incorporating the magnitude, local geology, and vulnerability of buildings as part of its measurements.

Response capability requirements

Government and Agencies. Capabilities required to deal with the aftermath from an earthquake are largely covered by plans put in place by government departments and Local Resilience Forums (LRFs), e.g. Site Clearance, Evacuation and Shelter and restoration of essential services and will be determined by the actual impacts in each case. Additional support could be provided via mutual aid agreements with neighbouring local authorities and partners – supplemented as necessary by national support.

CNI and Wider Private Sector. Damage to infrastructure such as power or communications networks will require specialist intervention. Impacts on supply chains, services and CNI will be dealt with in line with organisational and local planning arrangements and private companies' insurance cover.

Voluntary, Community and Faith Sector. VCFS partners will coordinate with local authorities and LRFs to ensure support packages are in place for impacted people, to include both initial longer-term support. This could include provision of evacuation support, emergency shelter or temporary accommodation and practical support such as food, water, clothing and medicines.

Recovery

Temporary or permanent rehousing may be necessary where residential properties are unsafe or uninhabitable. 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. Short-term closures of bridges, roads, and rail lines may be necessary to carry out safety inspections and repairs and there may be disruption to services, power and communications networks whilst repairs are made.

Impact on vulnerable people

The UK population could be considered more vulnerable to earthquake impacts due to a general lack of awareness of the risk, and consequently, lack of personal preparedness. 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.

Common consequences

The exact consequences will be dependent on the specific nature of the earthquake, but could include potential human health impacts, such as physical casualties, mental health casualties and fatalities, the need for some people to be evacuated and disruption to essential services (including water supply, sewage, education, health, transport, energy, communications).

Humanitarian crisis overseas: natural hazard event

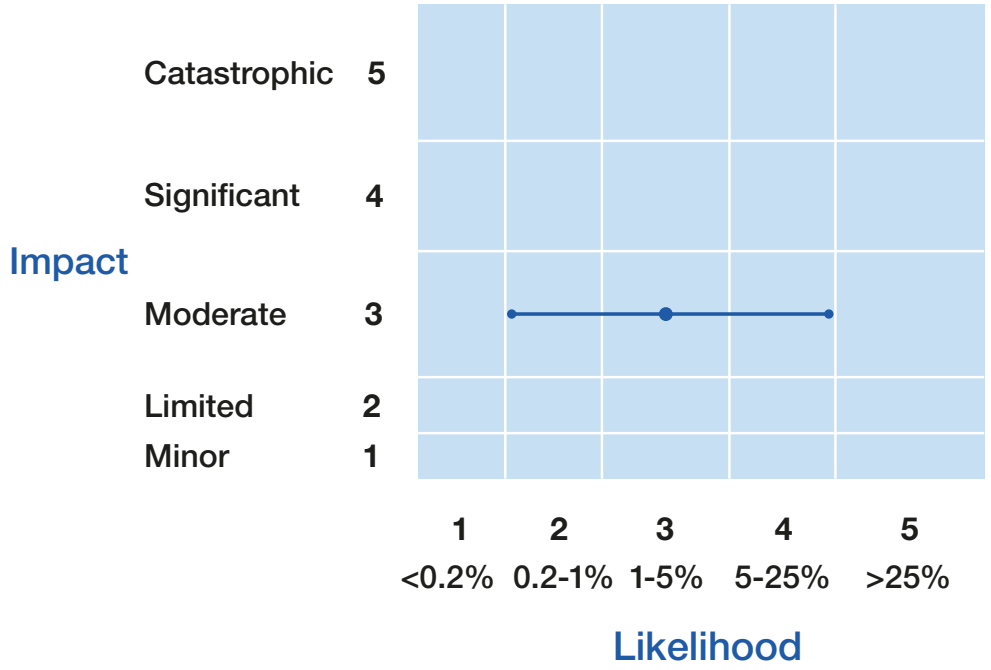
A natural hazard event such as an earthquake, hurricane or tsunami may result in a humanitarian crisis overseas that directly impacts UK interests or citizens. The UK regularly responds to major humanitarian crises overseas such as Hurricane Melissa in the Caribbean and the Myanmar Earthquake last year. This can include financial support, humanitarian expertise, medical services, search and rescue teams and relief 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 north-east 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

Government and Agencies. A UK response would be through ODA-funded capabilities including international search and rescue, operational infrastructure support and humanitarian assistance led by the FCDO in coordination with other government departments such as the MOD and DHSC. Consular assistance would be provided to British nationals directly affected by crisis. There may be additional migration considerations, particularly for people with family based in the UK.

CNI and Wider Private Sector. The private sector contributes to recovery by maintaining and restoring essential services, supply chains, and assets and by providing technical, operational and logistical capabilities. Disruption to infrastructure would hinder response operations, limit access to vital services, and slow overall recovery by affecting power, communications, transport and supply chains.

Voluntary, Community and Faith Sector. VCFS organisations would work alongside government to provide a range of services, with local organisations often acting as first responders and international NGOs contributing additional technical, operational and logistical support.

Recovery

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

Impact on vulnerable people

Natural disasters disproportionately affect vulnerable people by exacerbating existing vulnerabilities and causing sudden loss of shelter, access to healthcare, safe water, communications and mobility, and increasing exposure to injury and displacement.

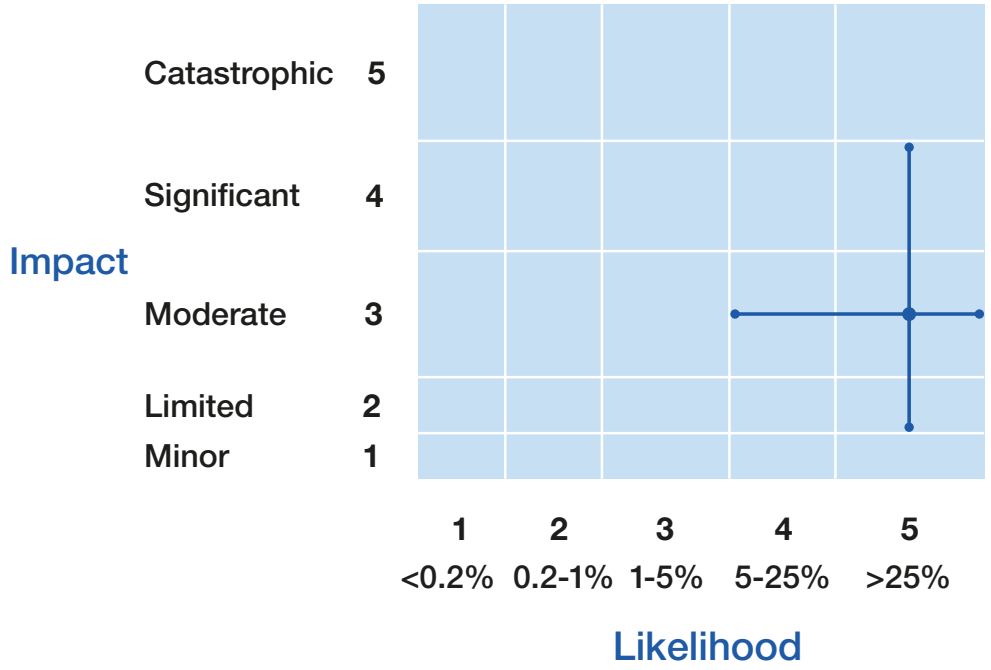
Common consequences

- Coastal inundation causing widespread damage to homes, infrastructure and transport links
- High casualties and displacement, especially in low-lying and densely populated areas
- Major disruption to essential services, including power, health, water and communications
- Severe economic impacts on coastal livelihoods, ports and fisheries across the region

Disaster affecting a UK Overseas Territory

As an inalienable part of the UK homeland, the UK bears responsibility for the security of the Overseas Territories (OTs). Any major disaster or issue in an OT would require a rapid and major response from the UK after assistance has been requested by the relevant OT government, and considerable political and public pressure. This has been seen before as per the Montserrat volcanic eruption (1995), various hurricanes, and historical military intervention over the Falklands. More recently, Hurricanes Irma and Maria in 2017 caused catastrophic damage across BVI, Anguilla and TCI, including widespread looting and prison breakouts, demonstrating the scale of security and stabilisation challenges that can arise. There is also sustained UK parliamentary interest in the OTs, alongside expectations from a large OT diaspora living in the UK, which increases political pressure in times of crisis.

The OTs are particularly vulnerable to high-impact natural hazards (hurricanes, volcanoes, earthquakes). For example, a hurricane in one of the Caribbean OTs may exceed local response capacity, requiring significant UK support in the short-term (humanitarian aid and emergency services) and long-term (relief and recovery). These natural hazards pose significant risks to British nationals and local economies. They also bring major security risks where local law enforcement and infrastructure become overwhelmed.



Scenario

A major hurricane or successive hurricanes simultaneously impact up to 3 OTs in the Caribbean, exceeding local response capacity and requiring significant short-term support (humanitarian aid and emergency services) and long-term UK response (relief and recovery). Impacts could include fatalities and casualties, damage to infrastructure, disruption of transport and critical services and serious security consequences. There would also be a significant impact on the economy and wider society, some of these issues may last for several years. There is also a risk to the UK Government's reputation during the recovery operation. Parliamentary, media and diaspora scrutiny would be immediate, increasing expectations for rapid UK intervention.

Key assumptions

The scenario assumes that the small government structures in the OTs do not have the capability to provide adequate crisis management or maintain internal security after a severe event.

Variations of this scenario

The 14 inhabited OTs are spread across the globe and are susceptible to different disasters. 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 and UK-led security stabilisation.

Response capability requirements

Government and Agencies. 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. UK military, policing and security support may be needed early to re-establish order and protect critical national infrastructure.

CNI and Wider Private Sector. Airline companies may be involved in supporting the flying of supplies out to OTs. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Humanitarian assistance for refugees and aid for those in need in the OT would support recovery. Safeguarding would be an important consideration in both relief and recovery.

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 UK response 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. Stabilising security and law-and-order may remain an ongoing requirement throughout recovery. A diverse range of UK government departments are likely to be involved in offering support on recovery.

Impact on vulnerable people

Vulnerable people are likely to be disproportionately affected if basic critical national infrastructure and front-line services fail. These include the elderly, disabled, low-income individuals, children left unsupervised, transient workers in the tourism sector, and undocumented migrants. Breakdowns in security further increase risks.

Common consequences

The exact consequences will be dependent on the specific disaster event, this would include an overseas response and potential disruption to essential services in the impacted OTs (including communications, food, education, health, water supply, sewage). There may also be disruption to financial services, businesses and security and justice. If multiple OTs are affected simultaneously, both local and UK response capacity could be overwhelmed quickly, intensifying political and public pressure.

Severe space weather

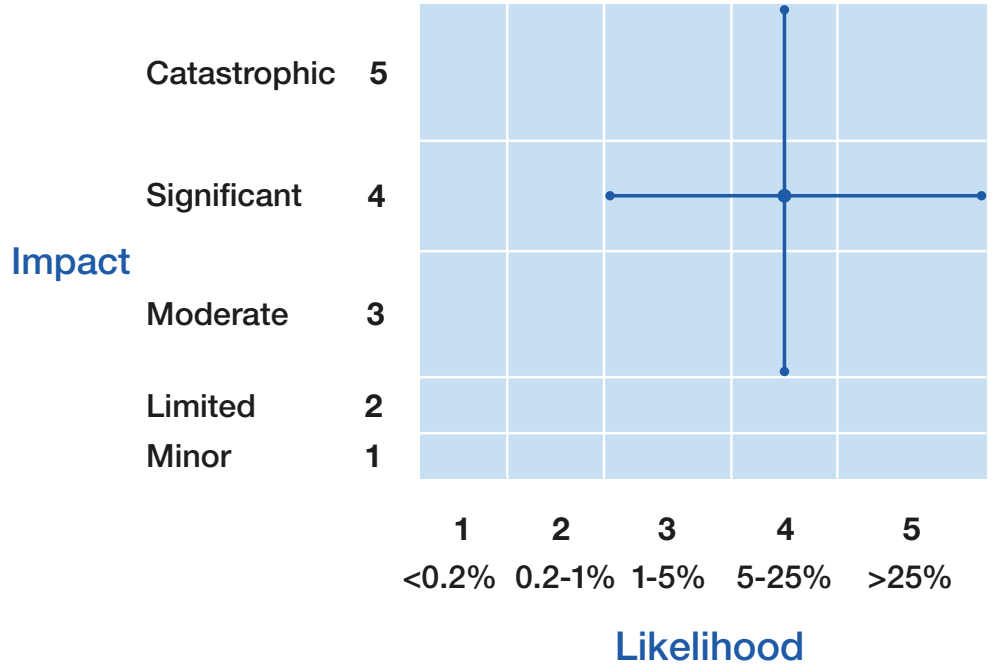
The term ‘space weather’ describes a series of phenomena originating from the sun, which include solar flares, solar energetic particles and coronal mass ejections. Day-to-day space weather causes little more than the Aurora Borealis in polar regions, but strong space weather events can bring disruption 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 in 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

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

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.

Response capability requirements

Government and Agencies. Emergency services and government bodies coordinate to support wider recovery and maintain resilient communications systems to manage the response effectively.

CNI and Wider Private Sector. 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.

Voluntary, Community and Faith Sector. Organisations assist by providing support to vulnerable people, particularly those with disabilities, the old and young who may be adversely impacted by losses to heating, water, transport and communications.

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.

Impact on vulnerable people

Severe space weather leading to localised loss of power and impacts on GNSS would likely impact already vulnerable populations e.g. those with medical equipment or that require additional support at home (home visits). Specifically, you may expect that there would be disproportionate impacts on the old and young, and the disabled who could become more vulnerable if loss of power leads to loss of heating, water, transport and communications.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, government services, food, transport, energy, education, communications, water supply and sewage)
- loss of or disruption to Global Positioning Systems
- disruption to financial services
- potential changes in public behaviour

Storms

Windstorms – associated with Atlantic low-pressure systems – affect the UK every year, mainly during autumn and winter. Met Office climate change projections indicate that the frequency and intensity of winter windstorms may well increase over the coming decades. The UK has experienced some severe storms over the last few years, such as Storm Eowyn (January 2025). Impacts of such storms can include disruption to power, communications and transport networks, school closures, and injuries and fatalities due to falling trees or flying debris. Disruption due to flooding or snowfall is also possible in some cases.

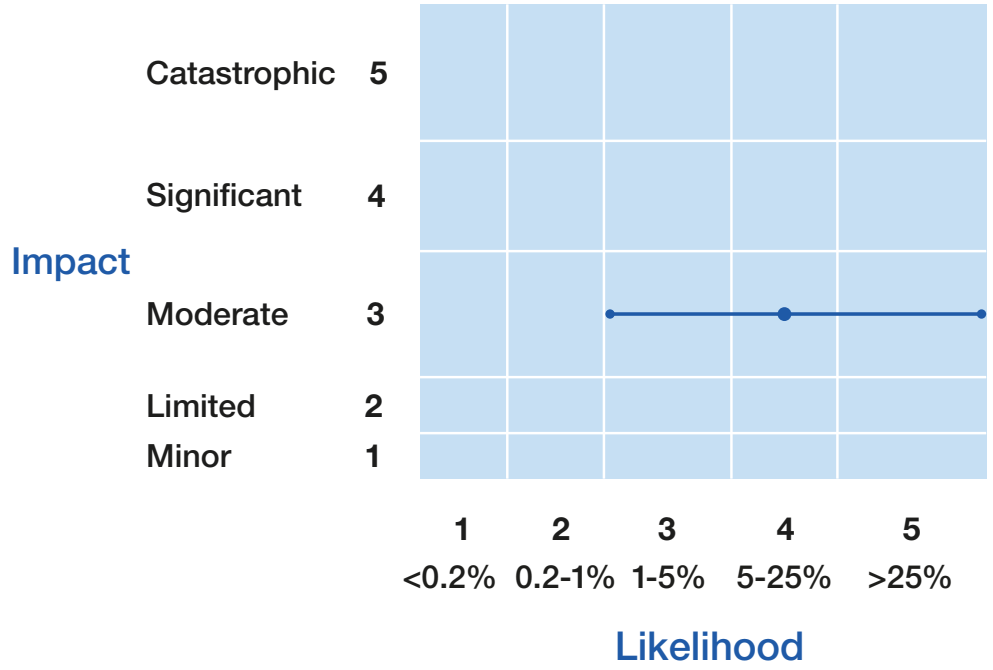
Scenario

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 55 mph, with gusts in excess of 85 mph. 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 environmental and economic impact would also be expected, due to fallen trees and disruption to transport networks.

Key assumptions

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



Variations

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

Government and Agencies. 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.

CNI and Wider Private Sector. Companies involved in key supply chains are encouraged to ensure they have effective contingency plans in place as damage from wind can affect availability of some commodities and transport can be disrupted.

Voluntary, Community and Faith Sector. Organisations assist by providing support to those disproportionately impacted by the cold 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.

Impact on vulnerable people

This risk would disproportionately affect those with low incomes and homeless. There may be differential impacts across rural and urban communities and the type of housing that people live in will affect how susceptible to the impacts of the risk.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, government services, food, transport, energy, education, communications, water supply and sewage)
- some properties may be affected by flooding
- disruption to security
- disruption to businesses
- disruption to financial services
- potential changes in public behaviour

High temperatures and heatwaves

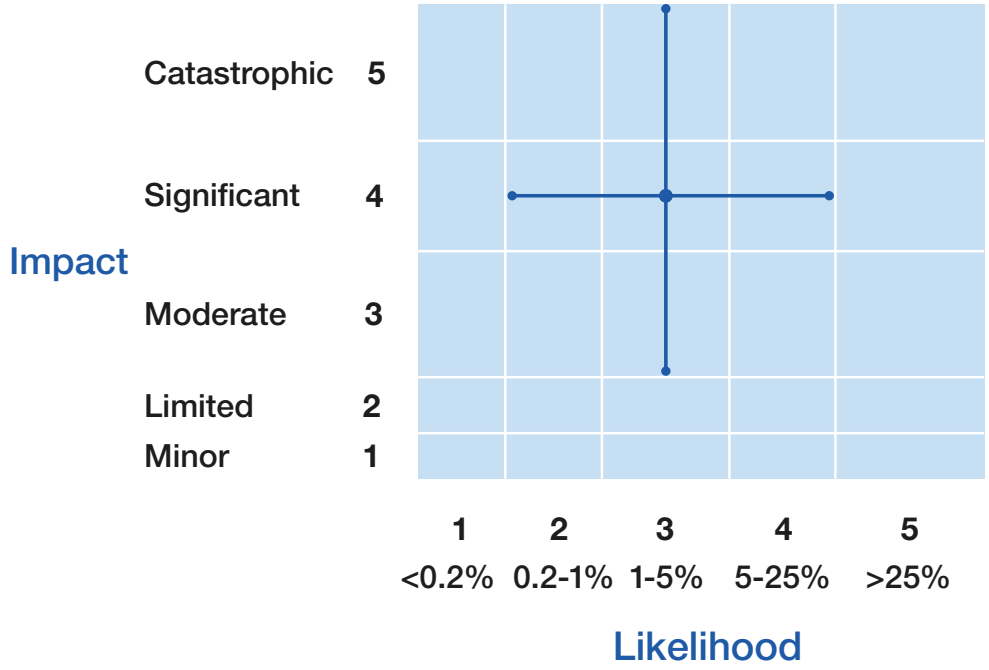
Climate change means that extreme heat has become more likely in the UK, with this trend expected to continue over the coming decades. Summer 2025 was the warmest on record and the UK experienced a series of heatwaves, with temperatures reaching 35°C in some areas.

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. There would be 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

The influence of climate change on the increased likelihood and intensity of high temperature episodes is already being observed, and this increase will continue.



Response capability requirements

Government and Agencies. The Met Office National Severe Weather Warning Service warns for severe weather (including extreme heat) up to 7 days ahead. The UK Health Security Agency (UKHSA) issues Weather Health Alerts for heat in England. The two services are closely connected through a common risk assessment and decision-making process which also underpins wider coordination and action across government and the resilience community. UKHSA's Adverse Weather and Health Plan (AWHP) is part of a commitment under the National Adaptation Plan to bring together and improve existing guidance on weather and health. 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.

CNI and Wider Private Sector. Companies involved in key supply chains are encouraged to ensure they have effective contingency plans in place as high temperatures can affect staff, supply chains and power.

Voluntary, Community and Faith Sector. Organisations can assist by providing support to those disproportionately impacted by the high heat.

Recovery

Recovery from this event would be quite quick. However, high temperatures may lead to secondary impacts such as an increase in the likelihood and impact of wildfires and longer-term drought conditions, and recovery from these impacts may take longer.

Impact on vulnerable people

The effects of heat are exacerbated by health conditions and social factors. Vulnerability also depends on building design, proximity to green space and the ability of that population to be able to find a cool space, for example, an air-conditioned office. The over-60s and children are likely to be disproportionately impacted. There may also be animal fatalities which will disproportionately impact rural farming communities.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, government services, food, transport, energy, education, communications, water supply and sewage)
- disruption to financial services
- potential changes in public behaviour – including increased crime and risky behaviours around water

Low temperatures and snow

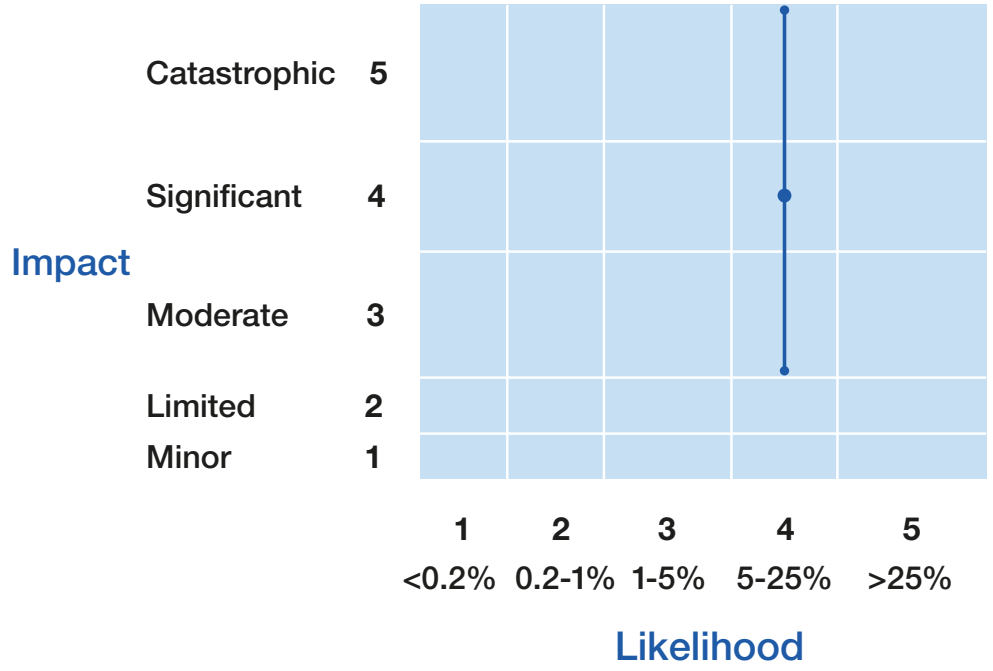
Winters with low temperatures and heavy snowfall pose a significant threat to human welfare, essential services and the economy. In late February and early March 2018, the UK experienced a spell of severe winter weather – named 'the Beast from the East' – with widespread impacts, including disruptions 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 300 m), for at least one week. After an initial fall of snow, there would be further snowfall 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 10 cm at a time, leaving snow depths of 30 cm in places, 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 weather would affect vulnerable communities, particularly older people and those with pre-existing conditions (such as cardiovascular/respiratory disease). Excess deaths, above those in a normal winter, are likely, with an increase in injuries due to falls, road accidents and hypothermia, placing significant pressure on health and social care services. Considerable impact on essential services, along with economic impact, would be likely due to disruption to transport networks, power or heating fuel supplies, telecommunications and water supplies.

Key assumptions

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

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

Government and Agencies. 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 UK Health Security Agency (UKHSA) issues Weather Health Alerts for cold weather in England. The Met Office and UKHSA services are closely linked through a common risk assessment and decision-making process which also underpins wider coordination and action across government and the resilience community. UKHSA's Adverse Weather and Health Plan (AWHP) is part of a commitment under the National Adaptation Plan to bring together and improve existing guidance on weather and health. 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.

CNI and Wider Private Sector. Companies involved in key supply chains are encouraged to ensure they have effective contingency plans in place as low temperatures and snow can affect availability of some commodities and transport can be disrupted.

Voluntary, Community and Faith Sector. Organisations assist by providing support to those disproportionately impacted by the cold weather.

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 snow melt, recovery due to these secondary impacts may take longer.

Impact on vulnerable people

This risk would disproportionately affect the older population, those with underlying health conditions, low incomes and homeless. There may be differential impacts across rural and urban communities and the type of housing that people live in will affect how susceptible they are to the cold.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, government services, food, transport, energy, education, communications, water supply and sewage)
- some properties may be affected by flooding
- disruption to security
- disruption to businesses
- disruption to financial services
- potential changes in public behaviour

Coastal flooding

Coastal flooding is caused by high tides, low pressure weather systems, large waves and surge conditions caused by strong winds blowing 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 for coastal communities. 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

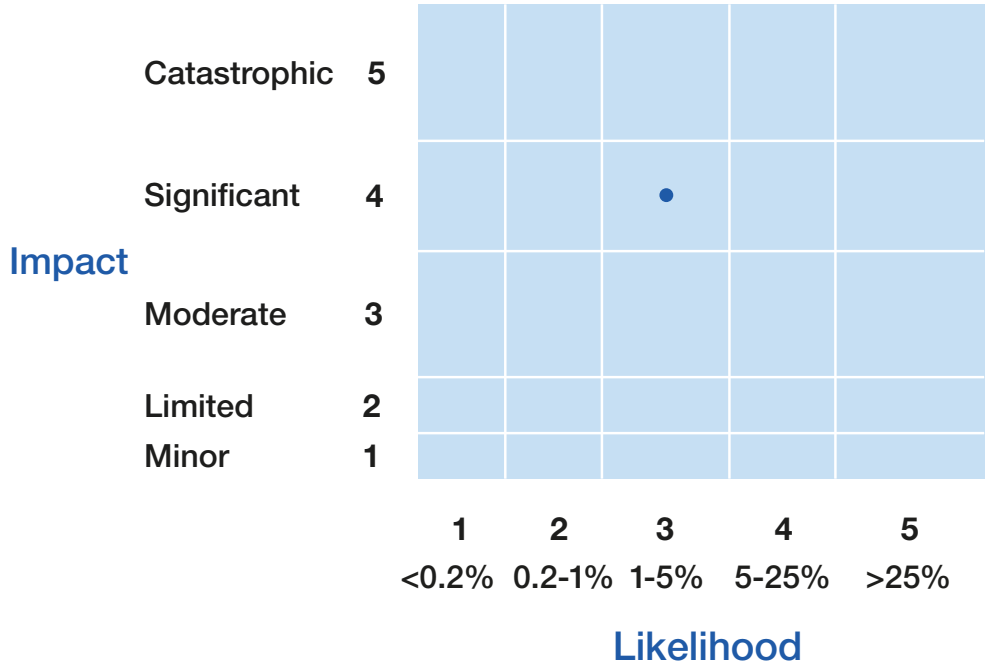
The reasonable worst-case scenario is based on coastal flooding across the east coast of England, impacting a very large number of residential properties. Comprehensive warning and informing systems would be employed and a large number of people would require evacuation and shelter. Large areas of road and railway could be flooded, with other major infrastructure such as schools, hospitals, care homes, emergency services and agricultural land also affected.

Key assumptions

In this scenario, there would be between 5 and 7 days of flood forecasts showing medium and then high risk of coastal flooding. Existing high levels of preparedness for local planning and response continue to operate. Investment in new coastal defences continues, as does maintenance of existing coastal defences.

Variations

Coastal flooding is highly variable. Certain areas are more vulnerable to flooding, and the impact in these areas would be higher.



Response capability requirements

Government and Agencies. 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. 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 Forums to support flood preparedness, operating defences and systems, and coordinating any evacuation efforts. The local response capability 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, 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.

CNI and Wider Private Sector. Local authorities have contractual agreements with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people and communities in affected areas. This could include support during evacuation and temporary accommodation.

Recovery

A major recovery operation will be required, considering 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.

Impact on vulnerable people

Some coastal communities have a higher proportion of elderly people than average across the UK. Age and physical mobility are recognised as two of the most significant factors in evaluating vulnerability or a person's ability to withstand the physical nature of the flood hazard.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- properties affected by flooding
- potential need for some people to be evacuated
- potential human and animal health impacts, which may include physical casualties, impacts on mental health and fatalities – saving lives and protecting communities from the dangers of flooding will be a top strategic priority
- disruption to essential services (including emergency services, health, food, energy, communications, water supply, sewage management, education and transport)
- disruption to security
- disruption to financial services in the affected area
- potential changes in public behaviour

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 would be widespread and may include damage to the local environment, properties and essential services. The government has well-established arrangements for minimising the risk from fluvial flooding.

Scenario

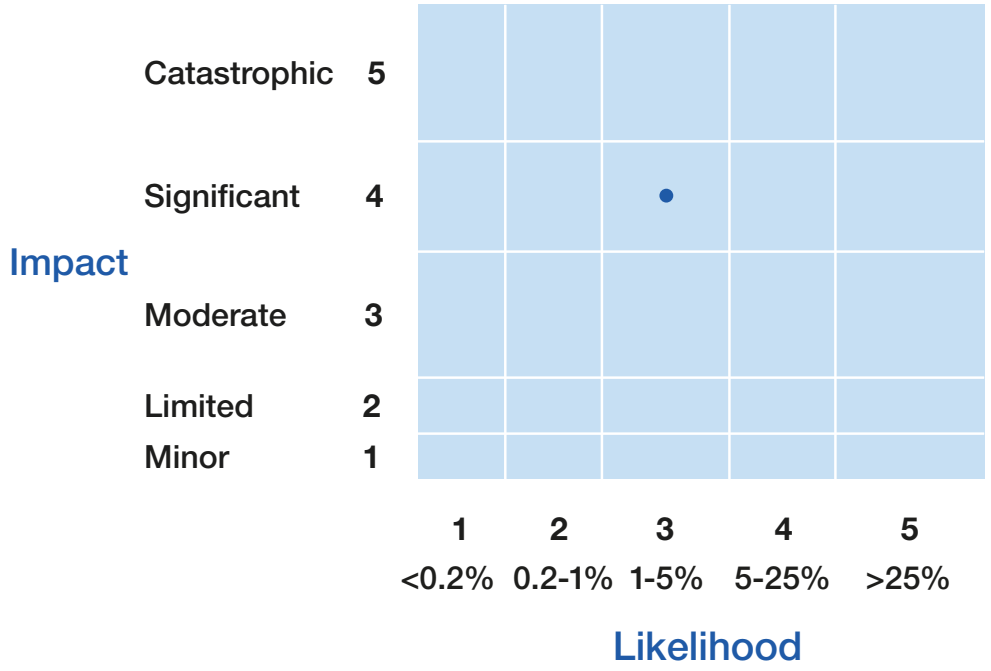
The reasonable worst-case scenario is based on a significant river flood event, resulting from cumulative local events or a series of concurrent events across multiple geographic regions, following a sustained period of heavy rainfall. This could possibly be combined with snow melt and surface water flooding. Flood defences would become overtopped by river levels and breaches may occur in riverbanks 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

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

Variations

A lower-impact scenario could involve fewer breaches of water-retaining structures and 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

Government and Agencies. An advanced flood forecasting capability is available via the Met Office and the Flood Forecasting Centre (FFC). 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 Forums (LRF) to support. 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, national mutual aid and military assistance can also support a local response.

CNI and Wider Private Sector. Local authorities have contractual agreements with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas. This could include support during evacuation and temporary accommodation.

Recovery

Major recovery impacts and long-term economic, environmental, infrastructure and humanitarian implications would go beyond two years, especially if significant repairs are required to infrastructure, homes and business.

Impact on vulnerable people

Age and physical mobility are recognised as two of the most significant factors in evaluating vulnerability or a person's ability to withstand the physical nature of the flood hazard.

Common consequences

Please see details provided in the coastal flooding risk summary.

Surface water flooding

Surface water flooding occurs when rainfall overwhelms the capacity of drainage systems, 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

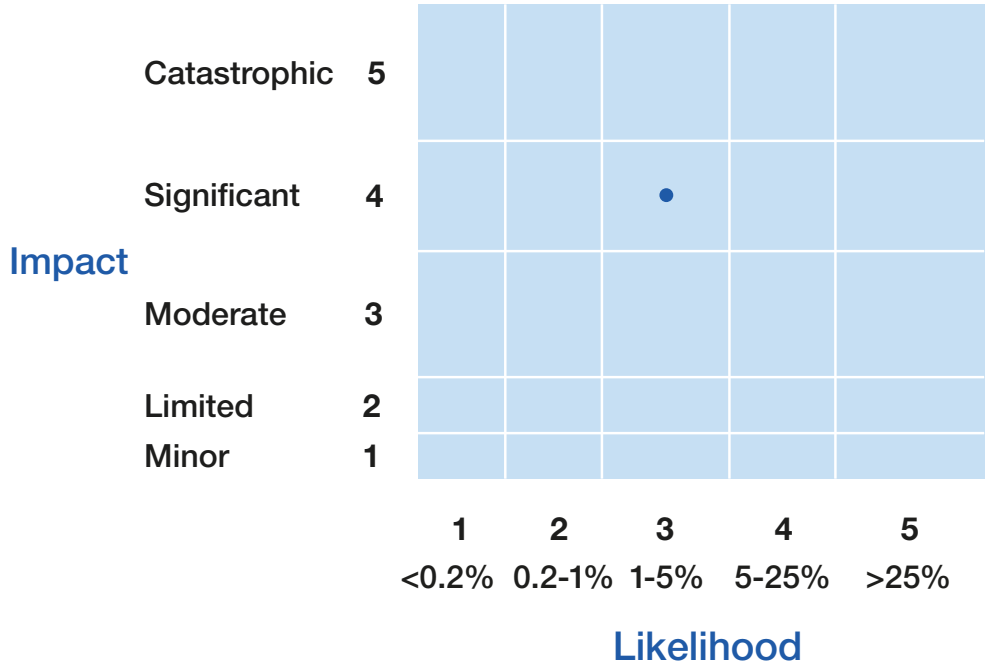
The reasonable worst-case scenario is based on a large flood event in a metropolitan area, resulting from a pocket of exceptionally high rainfall in the South East. The most severe impacts in any metropolitan area would lead to significant damage to homes and businesses. The evacuation of residents would 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, risk of sinkholes or landslides) in the impacted area. This could cause significant impacts to the local response, transport and other infrastructure in the impacted area.

Key assumptions

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

A higher-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

Government and Agencies. 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 Ministry for Housing, Communities and Local Government has well-established multi-Local Resilience Forum 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 to where they are needed.

CNI and Wider Private Sector. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas. This could include support during evacuation and temporary accommodation.

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.

Impact on vulnerable people

Age and physical mobility are recognised as two of the most significant factors in evaluating vulnerability or a person's ability to withstand the physical nature of the flood hazard.

Common consequences

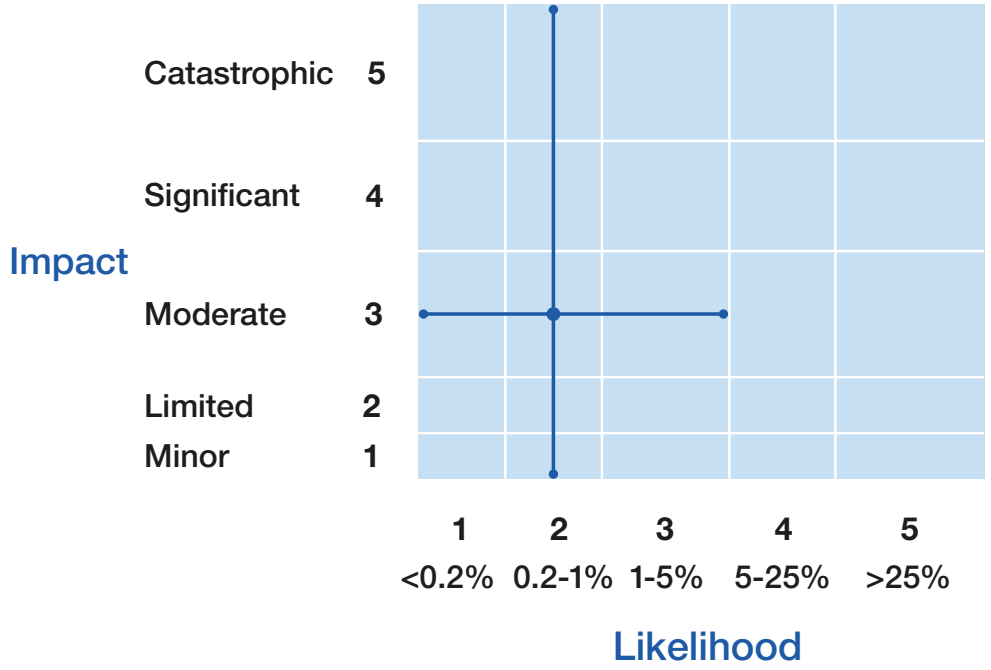
Please see details provided in the coastal flooding risk summary.

Drought

A drought may occur following a period of abnormally low rainfall, which results in a shortage of water. The future risk of drought due to climate change is increasing, and there is a trend towards hotter summers with associated high water demand. This was shown in 2025 when the Met Office declared the summer of 2025 as the hottest since records began in 1884, whilst the spring of 2025 was the driest in 132 years. At the same time, changes in consumer habits and population growth are increasing water use in the UK. This is particularly noticeable in the South East. Drought impacts can be reduced through water efficiency campaigns alongside 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 for 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. In this scenario, there would be significant losses to the UK economy, with serious impacts on industry, agriculture and businesses. Severe environmental damage due to drought conditions will occur, along with an increased fire risk due to the prolonged dry conditions. This would be combined with a reduced ability to fight fires due to water scarcity. Some of the critical national infrastructure (including energy, transport, hospitals, emergency services and telecommunications) will be impacted by water restrictions or loss of supply. Data centres, for example, are highly electricity-intensive and water-dependent.



Key assumptions

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

Variations

There are likely to be significant regional variations. A drought may end sooner than expected if a wetter period of weather occurs, depending on where the rain is and the duration of the rain.

Response capability requirements

Government and Agencies. The Environment Agency (EA) has 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 chaired by EA Director of Water. 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 in England are legally required to develop Drought Management Plans outlining the actions that they will take to effectively maintain essential water supplies and protect the environment in their area throughout each phase of a developing drought situation.

CNI and Wider Private Sector. Water companies should continue to utilise their comprehensive systems to monitor rainfall and water resources. Water companies may also consider temporary use bans and non-essential use bans to reduce water demand by the public and businesses, Drought Orders to manage water resources and Emergency Drought Orders to implement more significant and restrictive management in exceptional circumstances. Critical national infrastructure will be considered as part of water prioritisation policy and should provide data and information to Local Resilience Forums during a drought, to inform the response.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

Recovery

How quickly rainfall reaches normal levels, and the depth of impacts that have occurred during the drought, will impact the speed of recovery. Most businesses will 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, including long term impacts on biodiversity and plant health and impacts to freshwater ecosystems. There may be impacts on the wastewater network and treatment sites through the major decrease of flow through sewers during drought, and danger of flooding when rainfall returns.

Impact on vulnerable people

Drought is likely to affect those in denser and poorer-quality housing. This could be from damage to the property and indirectly through reduced access to ‘pleasant’ green spaces. Lower socioeconomic households will be less able to supplement alternative water provided by water companies. Compounding risks may also increase costs for these households (such as lower food yields increasing food costs). Due to the disparate nature of rural communities they may experience difficulty in accessing help. Water companies must provide alternative water supplies in the event of a loss of normal supply. Priority would be given to those domestic customers who are listed on the Priority Services Register (PSR). Commercial customers would not be prioritised for alternative water supply. Those using private water supplies are not covered by water companies’ protections, but local authorities have a statutory responsibility to provide water to these people.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, health, food, energy, communications, water supply, sewage management, government services, education and transport)
- potential changes in public behaviour including the potential for localised civil disorder

Poor air quality

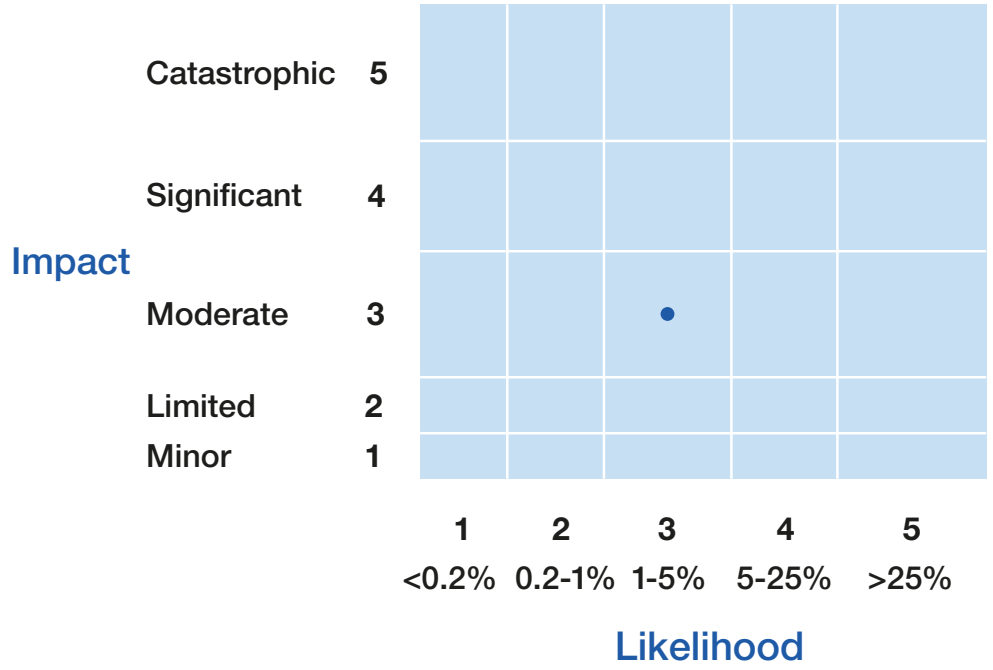
Air quality has improved significantly over recent decades. However, air pollution remains the largest environmental risk to UK public health and is linked with reduced life spans. Short-term surges in poor air quality occur primarily due to weather conditions preventing pollution from dispersing.

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 interim and long-term targets for PM set under the Environment Act 2021.

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

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

Variations

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

Government and Agencies. At the local level, access to healthcare professionals will be key to recovery, 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. At the national level, the government will focus on utilising 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.

Voluntary, Community and Faith Sector. Will have a role to play in ensuring the communications from government were reaching the wider community. All sectors should take active steps to reduce air pollution, aligning with governmental advice.

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.

Impact on vulnerable people

Air pollution can affect anyone's health; nevertheless, some individuals can be more susceptible than others. These include: children; the elderly; individuals with existing cardiovascular or respiratory diseases; pregnant women; communities in areas of higher pollution, such as close to busy roads. Due to these existing vulnerabilities these people may be at greater risk to the harmful effects of an air pollution episode.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some potential human health impacts, which may include physical casualties and mental health casualties.



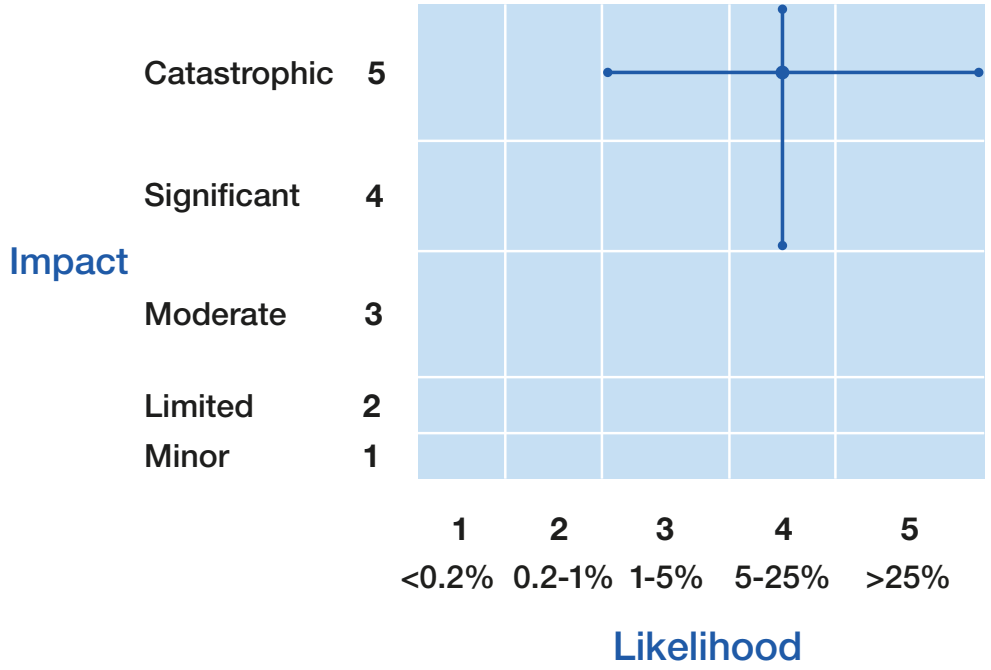
Human, animal and plant health

Pandemic

Pandemics are the result of a novel pathogen (viruses, 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. The government prepares for a range of pandemic and emerging infectious disease scenarios, across the five different transmission routes: respiratory, blood, and sexual, contact, oral (food and water), and by vectors such as mosquitoes. This approach covers known or unknown pathogens (referred to as 'Disease X' by the World Health Organization). 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 an unmitigated pandemic with an unassumed transmission route. The numerical assumptions are based on a respiratory pandemic (influenza), but the scenario could be caused by many pathogens. It is assumed that 50% of the total population becomes infected and experiences symptoms, and 35% of the total population becomes infected and is asymptomatic, with 4% of symptomatic cases requiring hospital care (about 1.34 million people) and a case fatality ratio of 2.5% (up to 840,000 deaths). The emergency response stage in the UK is at least 9 months and potentially, significantly longer, with impacts found for up to 2 years. The pandemic may come in single or multiple waves. The wave number depends on the characteristics of the disease, public behaviour, availability of effective antivirals for prophylaxis or treatment, vaccine development and rate of uptake and government intervention. The pandemic may lead to behaviour changes in the population.



Key assumptions

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, how the burden of mortality and morbidity is distributed across the population, including the age range affected, global travel.

Variations

While the scenario could be caused by many different pathogens, the numerical assumptions could vary significantly, particularly across different routes of transmission. There are variations of the reasonable worst-case scenario for the pandemic risk, based on different pathogens, some of

which have different routes of transmission. These include a possible novel enterovirus pandemic; a novel coronavirus pandemic; and, a novel sexually transmitted infection pandemic.

Response capability requirement

Government and Agencies. Robust regional and national command and control arrangements within the UK health and social care sector, other sectors, and by the Cabinet Office, to establish hierarchical and operational clarity for the command of a crisis. Effective disease surveillance and early detection, including timely and reliable data. The ability to isolate suspected cases at scale, supported by scalable contact tracing and diagnostics (both lab and rapid testing), as well as the ability to rapidly develop and procure new clinical countermeasures if they become available. 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. Ability 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.

CNI and Wider Private Sector. Every sector of the economy will be impacted by the pandemic and will require capabilities to respond, including mitigating for increased staff absences. Tourism and travel are almost certain to be significantly disrupted. Sectors considered high-risk are more likely to face restrictions and fear of the pathogen. Some sectors who are less able to adapt (e.g where workers are less able to work from home) will be disproportionately affected. Essential services are likely to see no or small reductions in demand, but will see some disruption through staff absence and, depending on exposure to international markets, due to supply chain issues.

Voluntary, Community and Faith Sector. The response to a pandemic will require a whole of society effort, with voluntary and community sector playing an essential role, for example to support vaccine deployment or providing support to patients and to support communications reaching all communities.

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.

Impact on vulnerable people

Vulnerable populations including ethnic minorities, socioeconomically disadvantaged groups, the elderly, digitally excluded individuals, and those with underlying health conditions could face disproportionate impacts. Disproportionate impact will be the result of existing inequalities, and vulnerabilities, the characteristics and progression of the disease across the country (e.g. mode of transmission), and the measures to control disease spread, as well as trust in health services and government. Some people will be at a higher risk of exposure (e.g. certain occupation groups); some people will be more susceptible to poor outcomes (may include those with an underlying health condition, those immunosuppressed or who have a disability, as well as those young and old, and pregnant women); some may have different levels of access to interventions.

Common consequences

The exact consequences will be dependent on the nature of the pandemic; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority. Measures to control the spread may reduce access to health and public services, result in financial impact, or impact mental health and wellbeing, or education
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, government services, health, food, education, water supply, sewage management, energy, transport, communications), to security, to financial services, wider business and potential changes in public behaviour

Outbreak of an emerging infectious disease

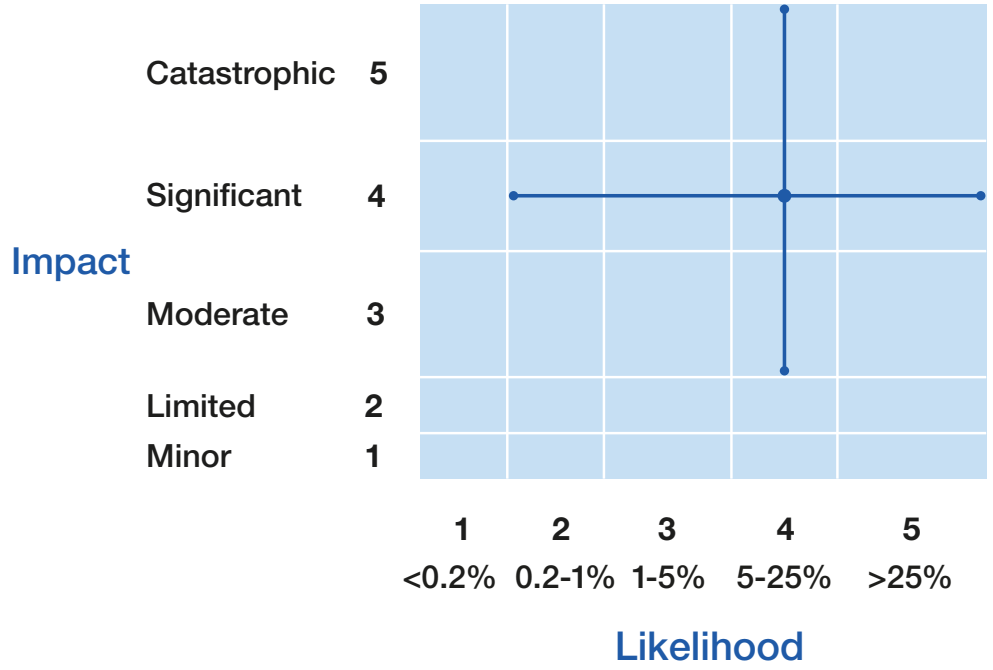
Emerging infectious diseases are newly recognised diseases that could result in large numbers of people falling ill. Some emerging infectious diseases are classified as High Consequence Infectious Diseases. Emerging infectious diseases require a rapid and enhanced individual, population and system response 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. However, we must be prepared for a disease spread via any of the five main routes of transmission: respiratory, blood, close contact, oral and by vectors such as mosquitoes. The outbreak could result in 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.

Key assumptions

It is assumed that there is no effective treatment or vaccine and 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 a degree of human-to-human transmissibility, and the outbreak is initially contained regionally. The outbreak would last between 2 and 6 months. Infected individuals would show identifiable 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

Government and Agencies. The national and local response would prioritise rapid containment and require intensive case and contact management, scalable testing capacity and sufficient laboratory capability. Response would require developed advice and guidance both to the general public and to healthcare providers, expanded diagnostic

capability, and securing reliable decontamination services to maintain a resilient response. The National Health Service would introduce infection prevention control measures and surge capacity for case management. A national communications plan would be needed to ensure the public has the information to protect themselves and enable introduction of public health and social measures.

CNI and Wider Private Sector. The private sector would play a key role in the supply of equipment and services during an outbreak including supplies of PPE and decontamination services. The private sector also develops tests, vaccines and therapeutics. Academia also plays a key role response by providing specialist scientific expertise to national government and supported accelerated research, including research into the new pathogen and clinical trials.

Voluntary, Community and Faith Sector. National government works with the VCFS to improve community engagement in outbreak response. The VCFS coordinate with local authorities to ensure support packages are in place for vulnerable people who may be isolated and need additional support.

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.

Impact on vulnerable people

There will likely be disproportionate impacts on some people depending on the outbreak. Impact could include the immunocompromised, pregnant women, those of a particular sex or age group, and from particular geographies or ethnicities.

Common consequences

The exact consequences will be dependent on the nature of the incident, but could include:

- potential human and animal health impacts, which may include physical and mental health casualties and fatalities.
- potential changes in public behaviour including altered patterns of travel, work, socialising and consumption, changes in health-seeking behaviour such as increased or decreased testing, uptake of vaccination, or willingness to self-isolate; and application of public health and social measures
- disruption to essential services; emergency services, health, energy, government services, education and transport.
- disruption to businesses and the economy
- disruption to security, which may include border security measures, biosecurity measures and law enforcement
- overseas response, which may include supporting British nationals abroad

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. A smaller scale outbreak in 2007 resulted in significant economic impact and disruption. 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

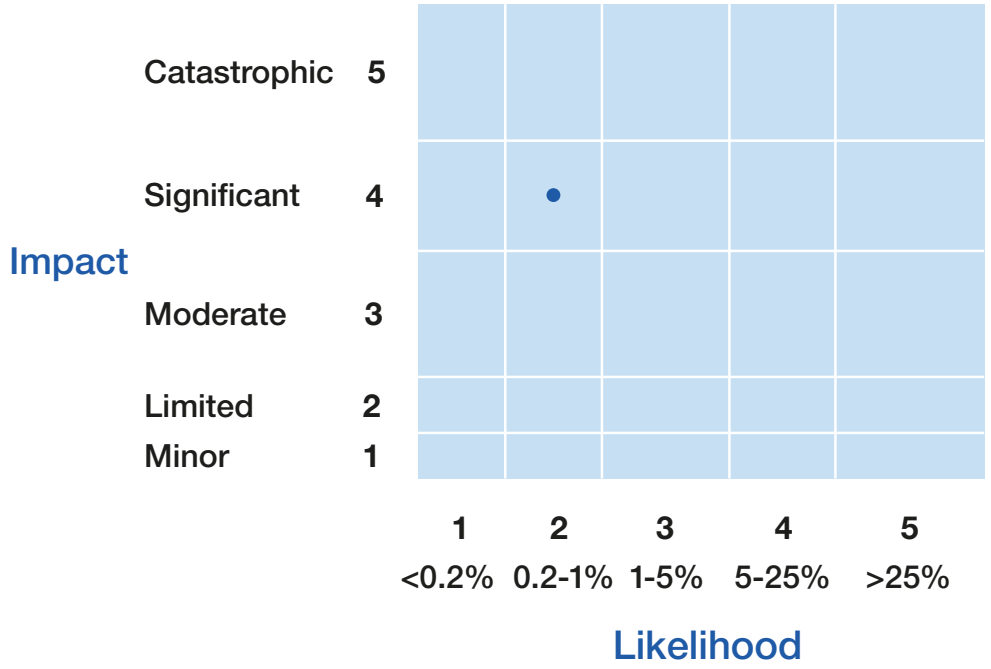
The reasonable worst-case scenario assumes that FMD is introduced into a sheep-farming area. Infected animals that are not yet exhibiting clinical signs would be sold or moved to other premises, including via livestock markets, before the disease is detected, resulting in multiple geographically dispersed 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 FMD outbreak in 2007, but less severe than the 2001 outbreak due to improvements to livestock movement regimes and control policies.

Key assumptions

There is a constant but low risk of an incursion of any exotic notifiable animal disease into the UK. Daily monitoring is in place.

Variations

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



Response capability requirements

Government and Agencies. Defra and the Animal and Plant Health Agency coordinate the responses supported by local authorities and local responders. There is a requirement for specialist staff to conduct surveillance, culls and dispose of infected animals. This includes vets, animal technicians, licensed slaughterers and carcass disposal logistics

experts. Sufficient carcass transport, rendering and incineration capacity, laboratory capacity 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.

CNI and Wider Private Sector. The private sector would play a key role in the supply across government, and partners of personal protective equipment (PPE) supplies, approved disinfectants and roll-out of a vaccination programme if required.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

Recovery

The minimum period to regain country free status for international trade is three months after the last FMD-infected premises is closed. If vaccination is used, exports can resume no sooner than three months after the last vaccinated animal has been culled, or six months after the date of last vaccination if a vaccinate-to-live policy is adopted. There would be long-term impacts on the environment, livestock sector, and the rural economy.

Impact on vulnerable people

The RWCS is likely to have a profound impact on the affected farmers, the staff involved in the control response, businesses and their employees in the restriction zones, trade, and potential loss of tourism in (and potentially beyond) the affected rural communities. Vulnerable people, such as the aging farming population or the workers whose first language may not be English could be isolated as a result of the restrictions, the inability to access digital communications, and the loss of income and livelihoods. The impact from culling operations and restrictions will impact other sectors including the veterinary profession and keeper's families.

Common consequences

The exact consequences will be dependent on the nature of the incident and response, but this could include human and animal health impacts (physical, mental health casualties and fatalities from accidents on farms), disruption to essential services, changes in public behaviour including customer choices and anti-government protests.

Animal disease: major outbreak of highly pathogenic avian influenza

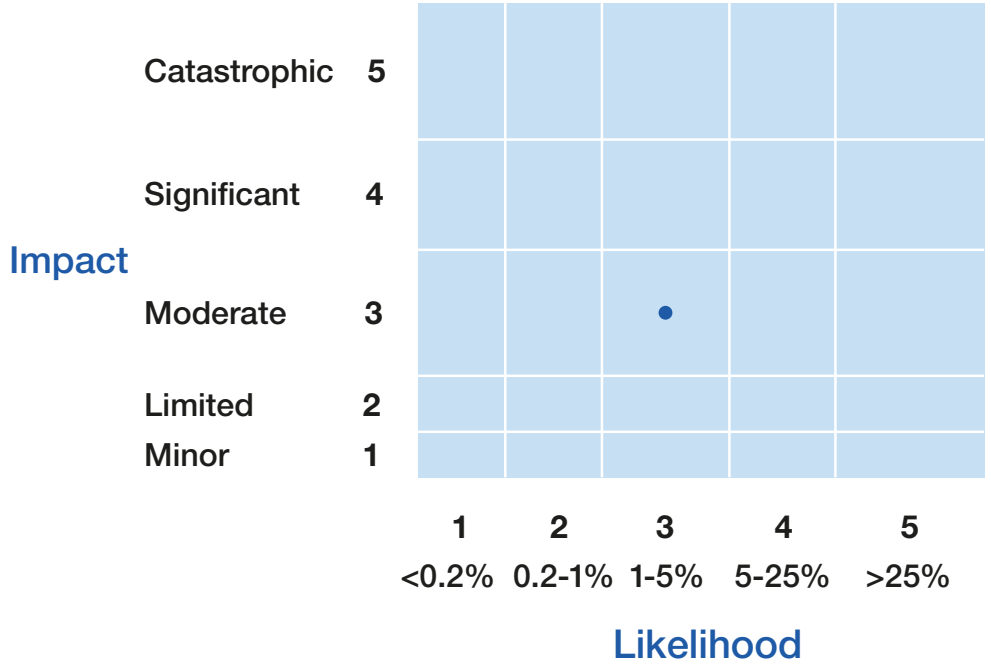
Highly pathogenic avian influenza (HPAI) is a severe, highly infectious influenza causing significant morbidity and mortality in susceptible avian species. HPAI is primarily a disease of birds, but can be transmissible to mammals including humans through prolonged, direct contact with infected birds or contaminated material. All strains of HPAI are legally notifiable if suspected in the UK, with the biggest outbreak to date being recorded in the 2022 to 2023 outbreak season. HPAI is a notifiable disease throughout the UK and anyone who suspects disease in poultry or captive birds (and mammals) must immediately report it. The Animal Plant and Health Agency (APHA) monitors HPAI outbreaks internationally and publishes outbreak assessments considering the risk posed to UK birds 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 via wild birds into multiple large-scale poultry businesses. Spread from both wild birds and between establishments 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

While this is not a strain which readily infects humans, occasional spill-over to humans cannot be ruled out and therefore local health protection teams would be involved in following up human contacts with each new infected establishment.



Variations

A strain with potential for transmission to mammals or humans could prolong the outbreak, complicate disease control and impact those with close occupational contact to infected birds or mammals. There would be increased impact on essential services and food safety. For strains causing severe disease in humans, casualties and fatalities could be expected. Disease control measures would need to be adapted to manage the additional impacts.

Response capability requirements

Government and Agencies. Defra and the Animal and Plant Health Agency with support from local authorities and local responders would coordinate the response. Specialist staff including vets, poultry catchers and staff for culling, disposal and cleansing and disinfection of premises would be required, along with sufficient transport capacity and access to rendering or incineration facilities. 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 the response would all be needed.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

CNI and Wider Private Sector. The private sector would play a key role in transport, disposal and the supply of personal protective equipment supplies, and approved disinfectants. These supplies will 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 culling and disposal and effective cleansing and disinfection at the last infected premises. Exports to the EU from within the zone can resume following the completion of enhanced surveillance in the restricted region, usually no less than 30 days after effective culling and disposal and effective cleansing and disinfection 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.

Impact on vulnerable people

The RWCS is likely to have a profound impact on the affected farmers, the staff involved in the control response and businesses. Vulnerable people in already isolated rural areas would be further isolated by the loss of income and livelihood.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities due to accidents on farms during culling - saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including food and transport)
- potential changes in public behaviour such as consumer purchasing choices, may occur (locally and nationally)

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 zebra act as a reservoir. 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.

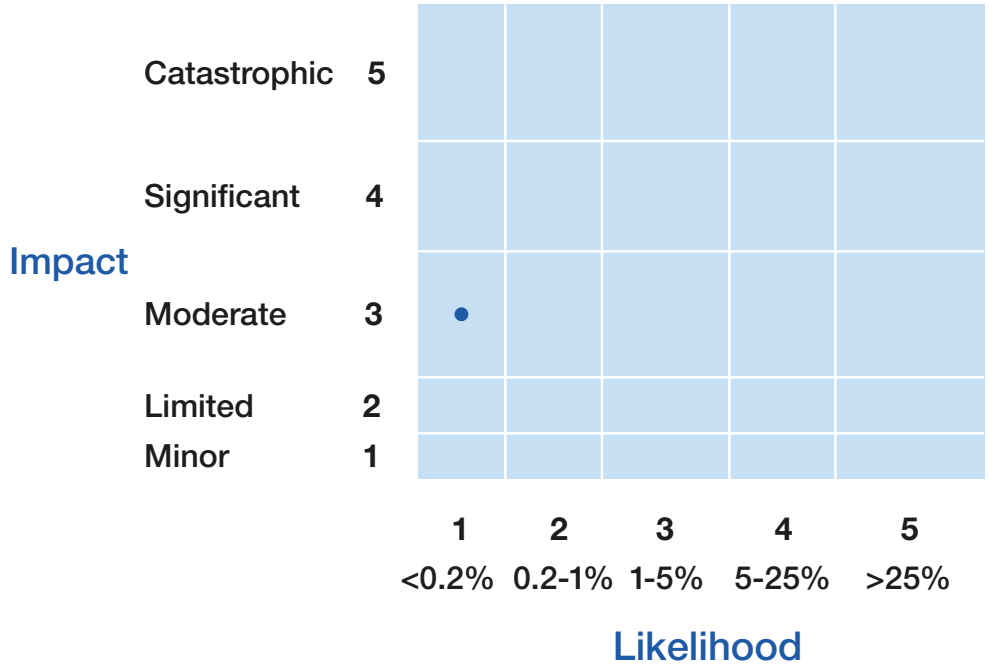
Scenario

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, AHS 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 and confirmed, AHS would be well established in geographically dispersed midge populations around the UK. Control measures include movement restrictions, euthanasia 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.

Key assumptions

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 equine animals. Sporadic illness and deaths in infected horses may not be attributed to AHS for the first few weeks, facilitating a wider geographic dispersal of the disease.



Variations

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 euthanasia until vaccines become available. An infected horse imported during the low vector activity season may not end in virus circulation but could still have a significant impact on trade and surveillance costs.

Response capability requirements

Government and Agencies. Defra and the Animal and Plant Health Agency with support locally from local authorities and local responders would coordinate the response specialist staff including equine vets (who may be private vets), animal technicians, licensed slaughterers (most likely undertaken by equine vets), and carcase disposal personnel would be required to conduct surveillance and dispose of euthanised 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.

CNI and Wider Private Sector. The horse-owning sector, National Parks and Commoners Associations, British Horseracing Authority, British Equine Veterinary Association and the British Horse Racing Levy Board would be crucial to recovery, their engagement will be necessary with specialists and local responders. The private sector would also play a key role in the provision of euthanasia supplies, vector proofing stables and approved disinfectants.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

Recovery

The minimum period to regain country-free status for international trade is two 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, competition and breeding sector, and rare populations of wild ponies could be severely impacted. The rural economy would also suffer heavy losses.

Impact on vulnerable people

The RWCS is likely to have a profound impact on the affected horse keepers, the staff involved in the control response, businesses affected by the movement and trade restrictions, and their employees. The social wellbeing impacts are expected to be greater than for other livestock diseases due to the companion animal status of many horses for the general public.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include potential human and animal health impacts, which may include mental health casualties and fatalities during control operations – saving lives and alleviating suffering is a top strategic priority. There would also be some changes in public behaviour following an outbreak.

Animal disease: major outbreak of African swine fever

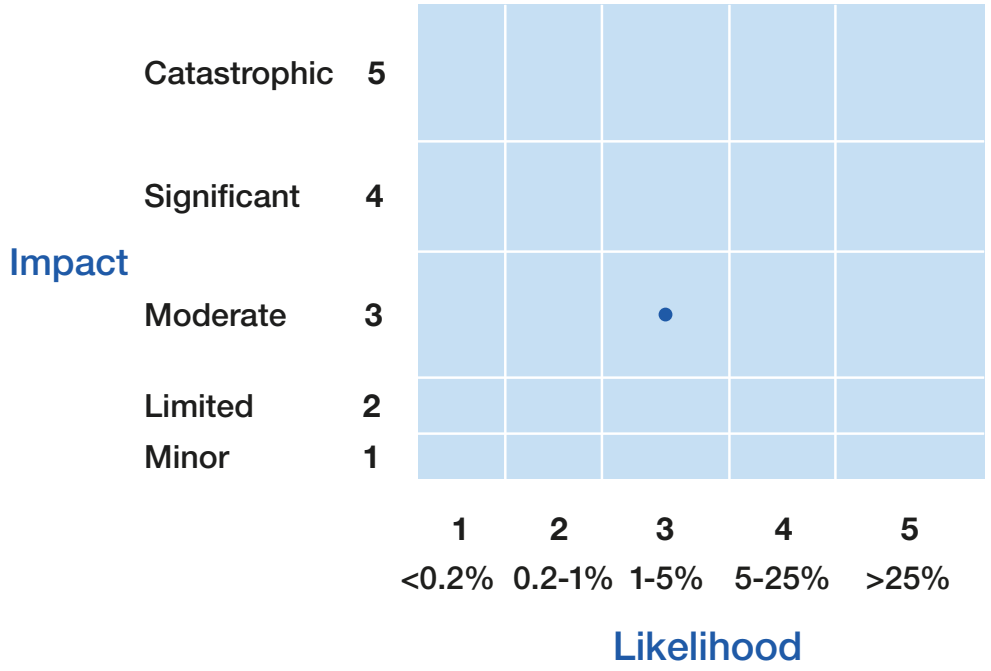
African swine fever (ASF) is a highly contagious haemorrhagic viral disease that affects pigs and wild boar but does not infect humans. It can be spread by direct contact with infected live or dead pigs, their secretions, pork products, contaminated feed, and non-living objects such as shoes, clothes 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. The outbreak in kept pigs could last for about 16 weeks, with restrictions on exports remaining in place for a minimum of nine months following the last confirmed infection. The outbreak in feral pigs could persist for up to 70 weeks.

Key assumptions

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

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

Government and Agencies. The disease response will be led by Defra and the Animal and Plant Health Agency. Local authorities, with support from central government, would provide enforcement. Specialist trained staff would be required to conduct surveillance while culling and disposal of infected animals and their cohorts will require additional teams. These staff include vets, wildlife experts and marksmen, licensed slaughterers and carcass disposal logistics experts, in addition to carcass transport, rendering and incineration capability. 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.

CNI and Wider Private Sector. The pig sector and local landowners where feral pigs are present would be crucial to the response, their engagement will be necessary with specialists and local responders. The private sector would also play a key role in the supply of trained personnel, personal protective equipment supplies and approved disinfectants, provision of rendering capacity and transport.

Voluntary, Community and Faith Sector. Coordinate with local authorities to ensure support packages are in place for vulnerable people in affected areas.

Recovery

For captive pigs, the minimum period to regain ASF Country-Free Status for international trade is three 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.

Impact on vulnerable people

The RWCS is likely to have a profound impact on the affected pig keepers, smallholders, landowners where feral pigs are present, the staff involved in the control response, businesses affected by the movement and trade restrictions and their employees, in the affected rural communities. Farmers are often considered vulnerable due to their age and social isolation, but also small holders have a more emotional connection to their animals, if considered pets. The social and wellbeing impact of an outbreak which results in culling on affected keepers can be severe.

Common consequences

The exact consequences will be dependent on the nature of the incident, but this could include some of the following:

- potential human and animal health impacts, which may include physical casualties, mental health casualties and fatalities due to accidents on farms during culling processes – saving lives and alleviating suffering is a top strategic priority
- potential changes in public behaviour

Major outbreaks of plant pest: *Xylella fastidiosa*

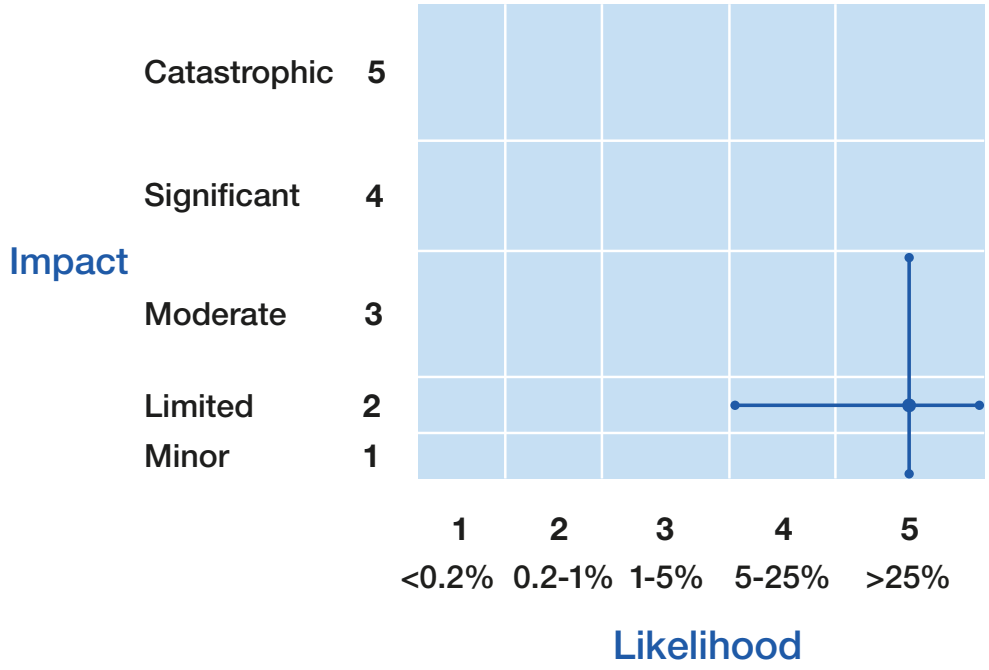
Xylella fastidiosa is a bacterium that is responsible for causing a number of named plant diseases. It was first detected in Europe in 2013 and is now established in France, Italy, Portugal and Spain. The bacterium has been reported from a wide range of hosts, and the number of plant species that have been shown to be infected is constantly increasing. Legislation has been updated to prevent the introduction of *Xylella* 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 *Xylella.* No outbreaks have occurred in the UK to date.

Scenario

The reasonable worst-case scenario is based on *Xylella fastidiosa* being found in a plant nursery, with a demarcated area established around it. Nurseries within the demarcated area are subject to pest management measures. Tracing of plants identifies up to 50 sites across the UK with potentially infected material. At one of these sites, surveillance confirms spread into the wider environment. A second demarcated zone is established and eradication measures implemented. While it is difficult to quantify the costs associated with *Xylella* impacting plant nurseries, there could be economic costs relating to lost working hours, lost stock and restrictions on trade. The outbreak would also have impacts on local ecosystem services, biodiversity, pollination, water regulation, and carbon storage on a local scale. In the short term, measures to remove plant species may impact air quality and water quality.

Key assumptions for this scenario

It is assumed that the measures in the plant health contingency plan would be followed and eradication would be feasible. If multiple outbreaks or outbreaks of other pests occur simultaneously, it is assumed that 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 and there is potential for more extensive spread into the wider environment requiring further management measures.

Response capability requirements

Government and Agencies. Agencies require surveillance capabilities to monitor the spread of the bacterium, capabilities to diagnose the pest, and procedures to report suspected cases. Surveillance activities and eradication measures are expected to continue for one year for an initial outbreak, extending to four years if a second outbreak occurs.

CNI and Wider Private Sector. Nurseries and landowners should be capable of removing and disposing of infected and suspect plants. Registered spray operators would be necessary for the application of pesticides to control vectors of the bacterium.

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. Lasting impacts on the wider environment are expected to be limited and could be mitigated by replanting with non-host species. However, recovery time will be dependent on the plants that are removed with the removal of mature trees leading to longer recovery times in comparison to herbaceous ornamentals.

Impact on vulnerable people

Significant financial losses, possible job losses, alongside the loss of plants in green spaces and urban tree removal, are likely to negatively impact the mental health of vulnerable people.

Common consequences

The exact consequences will be dependent on the specifics of the outbreak, but this could include some of the following:

- potential human health impacts, which could include mental health casualties
- economic losses for affected growers
- impacts on trade such as trade restrictions or increased costs to facilitate exports of *Xylella* hosts
- disruption to essential services (including transport)
- potential changes in public behaviour

Major outbreaks of plant pest: *Agrilus planipennis*

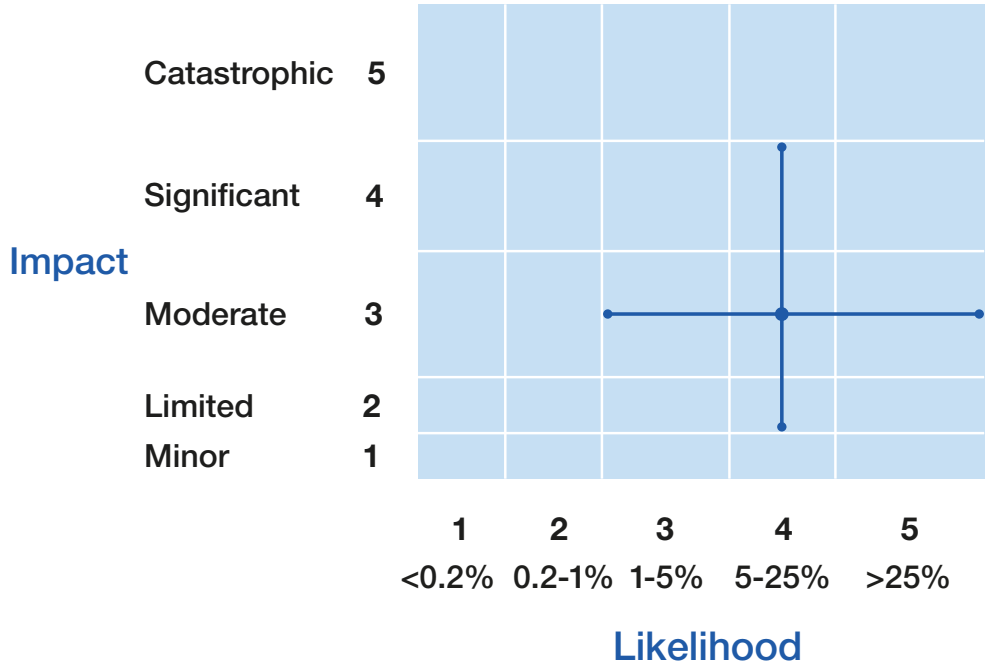
Larvae of the emerald ash borer beetle (*Agrilus planipennis*) bore into the inner bark and outer sapwood of ash trees, weakening the trees and causing them to die. There have been no previous outbreaks in the UK, but as the beetle spreads across Europe, there is an increasing likelihood that it will 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. The pathogen *Hymenoscyphus fraxineus* (causal agent of ash dieback disease) is also present and is reducing the health of ash trees in the woodland. Initial surveillance shows that the beetle has spread beyond a 100x100 m area and is detected at a further 2-5 geographically distinct sites. The beetle has been present at these additional 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 4 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 assumed that the measures in the plant health contingency plan would be followed, but that resources would be drained if multiple outbreaks or outbreaks of other pests occurred simultaneously, leading to an increased level of impacts. There are also assumptions around the biology of the pest and its host range.



Variations of this scenario

A high-impact variation involves a beetle found in southern England (with a more favourable warm climate, a high ash density and a significant level of ash dieback in woodlands), allowing the beetle to spread further and cause significant impacts more quickly. In comparison, in Scotland, which has a less favourable climate and lower ash density, the beetle will develop more slowly, minimising the impact on a smaller number of ash trees.

Response capability requirements

Government and Agencies. Agencies require surveillance capabilities to monitor the spread of the beetle, capabilities to diagnose the pest, and procedures to report suspected cases. Response capabilities also include research and development to improve detection and management methods, such as research to approve biological control agents.

CNI and Wider Private Sector. Landowners and forestry operators should be capable of destroying the worst-affected trees, including deploying tree-felling services to remove seriously damaged trees and dispose of them via chipping or incineration.

Voluntary, Community and Faith Sector. Citizen science surveillance schemes such as Observatree assist with surveillance activities, but require training inputs, triaging and follow up from government and agencies.

Recovery

It is likely that the majority of ash trees would be impacted in the outbreak areas. 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 recovery could take decades if mature trees are removed.

Impact on vulnerable people

Green spaces in the infested area will be altered, and the loss of ash trees through infestation or felling may have disproportionate negative impacts on the mental health of some vulnerable people.

Common consequences

The exact consequences will be dependent on the specifics of the outbreak, but this could include some of the following:

- potential human health impacts, which could include mental health casualties
- economic losses for landowners (timber/forestry products, removal of infested trees, carbon credits, replanting)
- impacts on trade such as increased costs to facilitate exports of ash timber and products
- environmental impacts and loss of ecosystem services (including water regulation, biodiversity, carbon release)
- disruption to essential services (including transport)
- potential changes in public behaviour



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, such as the Southport attacks of Summer 2024. Peaceful protests are not considered a form of public disorder, and the right to protest is enshrined in UK law.

Scenario

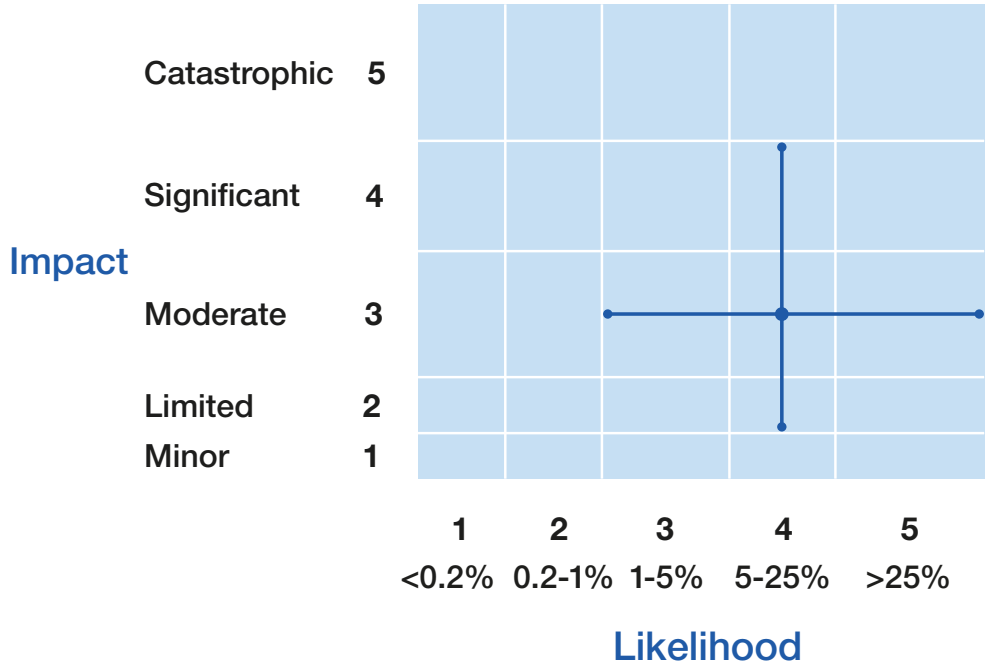
The reasonable worst-case scenario is based on widespread violent disorder in multiple areas simultaneously lasting up to seven days. There is the potential for criminal damage to property, significant impact on public trust, emergency services and government. In extreme circumstances, there may be disruption to CNI and public services, as well as injuries and potential fatalities, with health services coming under increased pressure.

Key assumptions

There are a number of specific trigger points, which would lead to localised disorder across urban locations, simultaneously or sequentially.

Variations

The scenario could vary significantly in length, location and the preceding trigger event. These aspects would influence the likelihood and impact.



Response capability requirements

Government and Agencies. The police would need to deploy specialist resources including public order and mounted officers, as well as neighbourhood officers, support units, and evidence gathering and custody teams. Central government would play a key role in coordinating agencies, and the wider criminal justice system (e.g. courts and prisons) would need to prioritise resources to encourage deterrence.

CNI and Wider Private Sector. As a result of the disorder, businesses may be impacted by criminal damage. Recovery of businesses and minimising the impact on supply chains will be a priority as part of recovery.

Voluntary, Community and Faith Sector. Voluntary organisations providing support to the vulnerable such as transportation for care workers and access to essential services for those who have mobility difficulties.

Recovery

Disorder events are typically resolved within a few days. Damage to local infrastructure may have a long-term and particularly acute impact on vulnerable communities. In addition, where disorder leads to the targeting of places of worship and/or community centres linked to local demographics, this can lead to longer-term damage to integration and community cohesion depending on the wider community response.

Impact on vulnerable people

In extreme circumstances, vulnerable individuals such as the elderly, disabled and those requiring medical care could face life-threatening situations if they are unable to access essential services, medication, or care workers due to transport disruption or wider impacts. Depending on the trigger event, minority communities and those with protected characteristics may also face heightened risks where they are targeted by harassment or hate crimes.

Common consequences

The exact consequences will be dependent on the nature of public disorder; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- disruption to essential services (including emergency services, health, food, education, transport, energy)
- disruption to security
- disruption to financial services
- disruption to business
- potential changes in public behaviour

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. This 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). The impact and likelihood of industrial action varies across different organisations. 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.

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 functioning, industrial action can lead to temporary closures of sites, reductions in the availability of key services with impacts ranging from inconvenience to severe risk to welfare and safety. Services might continue, but at a reduced capacity during a strike period.

Key assumptions

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.

Variations

This scenario could vary substantially depending on the context of industrial action and how long it lasts.

Response capability requirements

Government and Agencies. 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.

CNI and Wider Private Sector. Organisational resilience to industrial action varies by organisation. Appropriate contingency arrangements are enacted while the matter is resolved and operators are required to maintain plans for business continuity.

Voluntary, Community and Faith Sector. While the provision of services remains strained, support from voluntary organisations would aid value in the form of transportation for vulnerable people and support with access to essential services.

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.

Impact on vulnerable people

Industrial action places strain on the provision of services which will lead to some people being disproportionately impacted. Where possible disproportionate impacts will be minimised. However, this risk cannot be entirely mitigated.

Exact impacts on vulnerable people are sector-specific.

Common Consequences

The exact consequences will be dependent on the nature of industrial action; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- disruption to essential services (including emergency services, health, energy, transport, food, education)
- disruption to security
- disruption to financial services
- potential changes in public behaviour

This risk is featured in the full matrix on page 19. The average impact score for risks grouped under the ‘industrial action’ category is 2 (limited) and the average likelihood score is 3 (1-5%).

Reception and integration of British nationals arriving from overseas

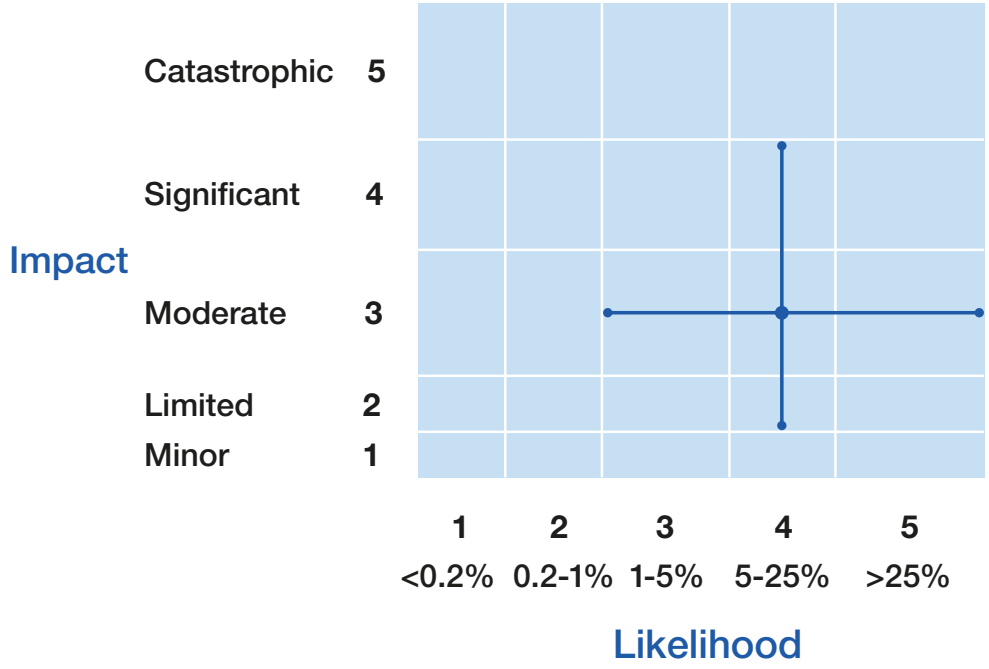
It is estimated that approximately 5.5 million British nationals (BNs) reside abroad. An adverse event in another country, such as a terrorist attack, conflict or disaster, may result in a sudden influx of a proportion of these overseas based BNs returning to the UK.

Scenario

The reasonable worst-case scenario assumes a large number of destitute or vulnerable BNs and their dependents arriving from overseas following an emergency or crisis overseas. This is likely to occur over a 3- to 4-week period, requiring reception services and integration support. As these BNs are not normally resident in the UK a percentage of them may not have accommodation or support options of their own. In addition, there may be a small number of deaths and injured BNs because of the overseas emergency or crisis.

Key assumptions

It is assumed that a proportion of impacted BNs would seek to enter the UK, as opposed to another country, with minimal notice. Arrival into the UK could be via different means and routes depending on circumstances. Identification of the scale, and the exact types of support required may not be possible until the BNs have arrived in the UK. Government funding may be required to support local responders towards immediate and longer-term integration assistance for vulnerable and destitute BNs.



Response capability requirements

Government and Agencies. The circumstances of departure may mean that support services are required immediately on arrival, including transport, accommodation, health and social care and welfare. Local authorities (in conjunction with other agencies and the voluntary sector) should have support packages in place for vulnerable or destitute BN arrivals, to include support at arrival and longer term. This could include provision of 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. Longer-term housing, education, healthcare and employment support may be required for some depending on circumstances.

CNI and Wider Private Sector. Private companies employing BNs overseas may be involved in the repatriation and should be able to support those individuals in the UK when they arrive. In some cases, key UK supply chains may also be affected by consequential impacts on supply. Local authorities have agreements and call-offs with providers who may need to enable access to a range of supplies as the need arises, e.g. food, accommodation etc.

Voluntary, Community and Faith Sector. VCFS partners will coordinate with local authorities to ensure support packages are in place for vulnerable or destitute BN arrivals, to include support at arrival and longer-term as needed.

Recovery

It is likely that most BNs will have either successfully integrated, or may have decided to return back to the country they were evacuated from as soon as they are able. However, long-term integration packages may need to be provided to support vulnerable and destitute BNs, including engagement with a range of agencies and the voluntary sector. This may include access to accommodation, welfare, employment assistance, education, and health and social care services.

Impact on vulnerable people

BNs arriving into the UK may have one, or a mix, of vulnerabilities. These could include: English as a second language, destitution, the very young, the elderly, individuals requiring ongoing health support, individuals with disabilities, pregnancy, and those who have been traumatised by the events leading to the evacuation.

Common consequences

The exact consequences will be dependent on the specific circumstances leading to return to the UK; this could include an overseas response and potential human health impacts including physical and mental health casualties and fatalities.

Significant disruption to the Criminal Justice System

The adult male prison population has steadily grown over recent years, leading to an acute pressure on prison estate capacity. This has required the introduction of early release schemes to ensure that core criminal justice functions could continue to operate.

Scenario

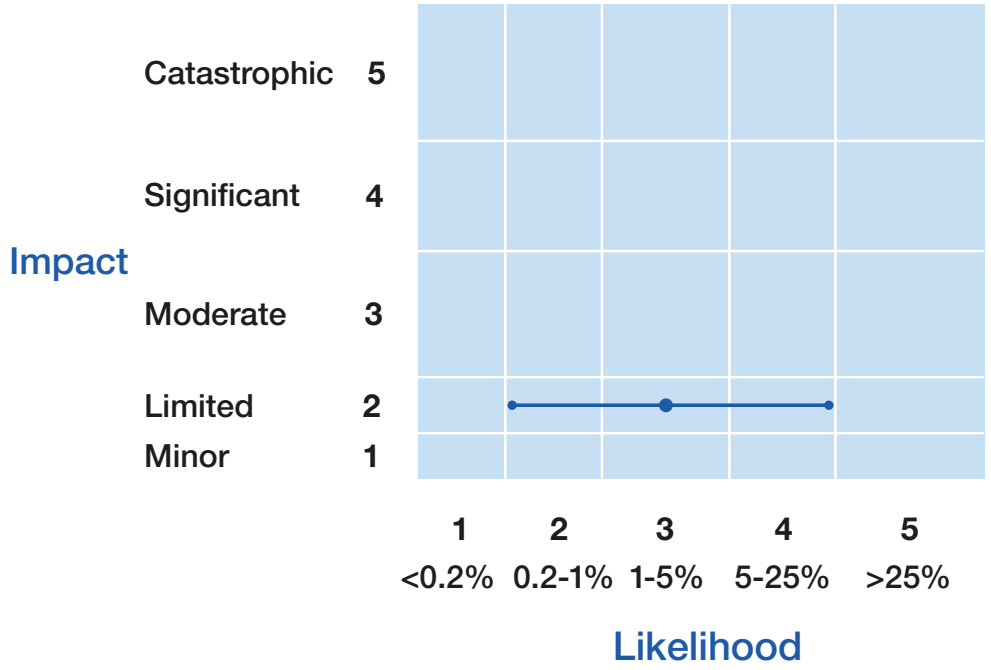
The prison population has increased at unsustainable rates, resulting in new receipts exceeding available capacity with pre-emptive contingencies having been activated and exceeded. This effectively results in a one-in, one-out scenario with priority given to higher-risk cohorts.

Key assumptions

The demand outstrips supply and emergency levers have been exhausted.

Variations

Concurrent risks could exacerbate or cause this risk to manifest. Large-scale industrial action by critical staff groups could result in similar impacts.



Response capability requirements

Government and Agencies. The Criminal Justice System Strategic Command (CJSSC) would be activated to provide tactical coordination of the response, as well as managing the risk and its impacts. Contingency measures may be implemented to minimise and limit disruption at various stages during a period of challenge in operability.

CNI and Wider Private Sector. Private prisons will be impacted in the same way as the public estate. Co-ordinated response will be managed through existing HMPPS structures.

Voluntary, Community and Faith Sector. It is not anticipated that the voluntary sector will be required to fulfil additional roles beyond what is already delivered as part of regular, justice-related services within prisons, delivering services in the community as part of or alongside probation services, or within courts. However, demand for some of these existing services may increase, particularly for victim support and through-the-gate services.

Recovery

Overcrowding may cause reduced access to rehabilitation programmes, prisoners subsequently released may therefore be more likely to reoffend, placing further pressure on the system.

There is likely to be an increase in court backlogs, resulting in increased waiting times for trials.

Impact on vulnerable people

It is anticipated that there will be an impact upon victims, particularly mental health impacts resulting from longer waits for justice or alternative holding arrangements for those awaiting trial.

This scenario places strain on the provision of services to those with specific medical needs held within the criminal justice system. Steps will be taken to prioritise care and services to vulnerable people; however, this risk cannot be entirely mitigated.

There may be increased pressure on through-the-gate release services should there be an increase in demand resulting from contingencies enacted to release the pressure on the criminal justice system – this may disproportionately impact vulnerable people who are at higher risk of homelessness or abuse.

Significant disruption to other routine prison services (e.g., education) is not expected. Localised disruption may occur and steps will be taken, where possible, to minimise the impact on vulnerable prisoners.

Common consequences

The exact consequences will depend on the length of disruption. There could be disruption to security and changes in public behaviour, as well as possible human health issues through second order impacts.



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. 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 and defence operations. Space capabilities are already central to many basic and safety critical civil functions, and this dependency on space will only increase. AI can automate the process of launching cyber-attacks, making them faster, more efficient and lower the barrier for entry. MOD, DSIT and the space sector will continue to monitor how current and emerging AI influences the potential for disruption to space based services.

Scenario

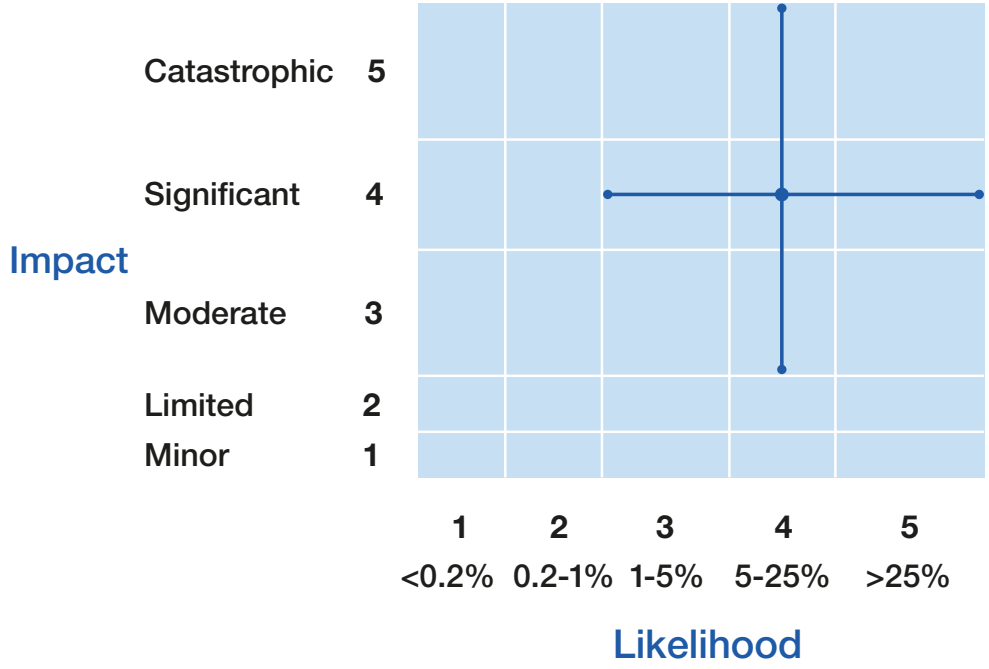
The reasonable worst-case scenario is based on an attack on UK or allied space-based systems or services by a state or a proxy. There would be immediate and longer-term impacts on UK space systems, resulting in severe disruption to essential services downstream. These could include food and water, and financial market infrastructure and communications.

Key assumptions

The scenario takes into account disruption of entire space systems, including ground sites.

Variations

The scenario could manifest itself in multiple variations, where attacks come in various forms eg: kinetic or cyber.



Response capability requirements

Government and Agencies. A multitude of measures could assist response capability. Government and the local level will aim to minimise disruption and reduce the impact to individuals and communities. Collaboration with international partners offers further opportunities to enhance the overall resilience. The government will also explore the potential offered by alternative infrastructure and service solutions (such as terrestrial-based navigation and timing systems).

CNI and Wider Private Sector. Cyber security measures, counter-jamming technology and interference detection capabilities could help to protect against an electronic attack.

Voluntary, Community and Faith Sector. Given there may be some disruption to food and water, the voluntary sector would play a key role in supporting local communities and the vulnerable.

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.

Impact on vulnerable people

This risk would disproportionately impact vulnerable people, particularly those in remote, low-income, or disaster-prone areas.

Common consequences

The exact consequences will be dependent on the nature of the disruption to space services; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- overseas response
- disruption to essential services (including emergency services, government services, health, education, food, water supply, sewage management, energy, communications, transport)
- disruption to security
- disruption to cyber services
- disruption to financial services
- loss of or disruption to Global Positioning Systems (GPS)
- potential changes in public behaviour

Attack on a non-NATO partner requiring UK assistance

Scenario

The reasonable worst-case scenario for this risk involves a military escalation between two or more countries – resulting in an attack on at least one non-NATO UK partner, where the UK is placed in a position where it is required to respond. This will lead to implications on the UK economy, trade and supply chains.

Key assumptions

This scenario would occur as part of a broader escalation. It is expected that threats could quickly develop in a variety of scenarios.

Variations

The scenario could vary substantially depending on the location of the crisis, severity of attack and the response of other allies.

Response capability requirements

Government and Agencies. Government – notably the military – would play a key role in the response and there would be well understood roles and responsibilities for government departments.

CNI and Wider Private Sector. This risk could affect the UK's supply chains and impact resilience of key infrastructure. Contingency plans for impact to supply chains are required (e.g. flow of energy, goods and materials).

Voluntary, Community and Faith Sector. Humanitarian assistance and support for those seeking repatriation would be required.

Recovery

The length of recovery will be dependent on the nature of the attack and required response. The range of possible targets which would have wider impact are vast. The nature of any military activity, for example its duration and intensity, would shape the recovery.

Impact on vulnerable people

There are multiple ways that vulnerable people may be impacted. For example, those seeking repatriation, those unable to evacuate, or through impact to diaspora groups within the UK.

Common consequences

The exact consequences will be dependent on the nature and duration of the attack. It is expected that there will be an overseas response and potential disruption to energy supplies and international security.

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 North Atlantic 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 an adversary 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 the crisis continues. There is disruption to UK and European economies. 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 supply chains.

Key assumptions

For Article 5 to be reached it relies on the consensus of 32 Allies to respond in support of the Ally which has been attacked. 'Triggering' Article 5 is context-dependent and relies on NATO political consensus. Whilst this scenario focuses on an attack overseas, it is likely the UK would also see an increase in hybrid attacks, and potential military action around (naval) and in Homeland.

Variations

The scenario could vary substantially depending on the location of the crisis, severity of attack and the response of allies.

Response capability requirements

Government and Agencies. Management of this risk is best achieved through avoidance through effective deterrence. This includes sufficient UK and allied military capability to effectively deliver NATO deterrence and defence of the Euro Atlantic area.

CNI and Wider Private Sector. Companies involved in supply chains will be impacted by this incident and would need to adapt to minimise disruption to supply chains. Travel providers and insurers support the response through customer identification, repatriation and medical logistics.

Voluntary, Community and Faith Sector. Humanitarian organisations assist by delivering specialised victim support and welfare services to those affected.

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.

Impact on vulnerable people

Vulnerable British nationals in the country where the attack occurs are particularly at risk. Refugees travelling to the UK may also become vulnerable.

Common consequences

The exact consequences will be dependent on the nature of the attack. It is expected that there will be an overseas response and potential disruption to transport, energy supplies, cyber services and security.

Conventional attack on the UK mainland or Overseas Territories[3]

Protection of the UK, its citizens, property, and territory, from adversarial states, is the first responsibility of 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, using a combination of conventional missiles and cyber operations. This attack causes NATO allies to invoke Article 5 of the North Atlantic Treaty. 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.

Key assumptions

This scenario assumes that the adversary has intent to cause disruption and destruction of UK assets.

Variations

Additionally, whilst it is likely that any attack on the UK mainland would be preceded by sub-threshold activities, escalation could also take a non-linear path. A non-linear progression could result in different impacts.

Impact on vulnerable people

Any people in the surrounding areas that are targeted will become vulnerable as a result of this attack. Those already vulnerable are also likely to be disproportionally impacted.

Common consequences

The exact consequences will be dependent on the nature of the attack; this could include some of the following:

- potential human health impacts, which could include physical casualties, mental health casualties and fatalities – saving lives and alleviating suffering is a top strategic priority
- potential need for some people to be evacuated
- overseas response, including activities in post- and wider diplomatic efforts
- disruption to essential services (including emergency services, food, government services, health, water supply, sewage management, education, energy, transport, communications)
- disruption to security
- disruption to cyber services
- disruption to financial services
- potential changes in public behaviour

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

Nuclear miscalculation not involving the UK or its allies

Nuclear miscalculation refers to the risk that a state will mistake the intentions of another state and respond by launching a nuclear strike. 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 or its allies. The impacts in the affected area would depend on factors such as the location, size of the yield of the weapon, and the size of the local population, particularly in terms of numbers of casualties and fatalities. There would likely be implications for UK businesses with direct or indirect ties to the affected region, given the potential for economic disruption. HMG facilities may be affected. British nationals in the region would require support. There would be the potential for high levels of migration from the affected region, increasing pressure on regional infrastructure. There is the possibility an incident could lead to increased community tensions and protests.

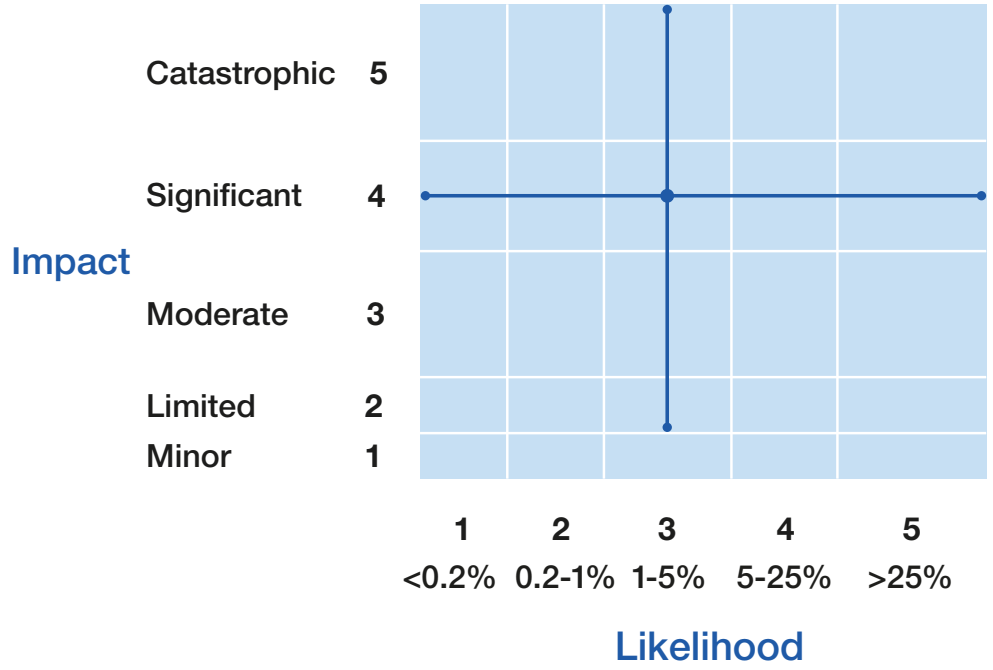
Response capability requirements

Government and Agencies. The UK maintains a civilian staff qualified to monitor radiation levels. Consular support for affected British nationals.

Voluntary, Community and Faith Sector. Humanitarian assistance would be provided.

Recovery

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



Impact on vulnerable people

The impact on vulnerable people would depend largely on the circumstance of the incident. Vulnerable people may find it more challenging to evacuate from the affected area.

Common consequences

The consequences of the incident would again largely depend on the exact circumstances. Local impacts could include fatalities, destruction of property and infrastructure including key services. British nationals in the region could be affected. Internationally there is the possibility of disruption to supply chains and civil aviation.

© Crown copyright 2026

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