D4.1

Case study scenarios

Date
22.02.2025

Author: Femke Mulder, Dr. Gianluca Pescaroli, Rabea Schulz
Organisation: University College London, Johanniter-Unfall-Hilfe e.V.

Funded by the European Union

Project funded by the European Union's Horizon Europe and the UK Research and Innovation (UKRI) programme under the UK government's Horizon Europe funding guarantee grant agreement n°10062626

D4.1
Case study scenarios

Grant Agreement	101121356
UKRI numbers	10062626
Call identifier	HORIZON-CL3-2022-DRS-01
Project full name	AGnostic risk management for high Impact Low probability Events
Due Date	31.01.2025
Submission date	22.02.2025
Project start and end	01.10.2023 - 30.09.2027
Authors	Femke Mulder, Dr. Gianluca Pescaroli, Rabea Schulz

Abstract

This deliverable, D4.1 Case Study Scenarios, outlines the AGILE project's methodology for developing hypothetical scenarios to support stress testing in disaster risk management. It reviews current practices among AGILE's case study partners, providing insights into diverse approaches to scenario development. The document provides a reference list of past HILP events to inform future risk assessments, based on the HILP criteria developed in D1.1. A key focus is balancing a risk-agnostic, systems-focused approach - designed to uncover systemic vulnerabilities - with the specific needs and contexts of the case studies to ensure applicability and relevance. The scenario development methodology incorporates the AGILE Card Game to generate dynamic, multi-hazard scenarios, integrates local to cross-border contexts, and employs counterfactual analysis to enhance resilience. Example scenarios illustrate the adaptability of this approach across varying operational environments.

Document revision history

Issue	Date	Comment	Author
V0.1	25.11.2024	Draft structure	Rabea Schulz
V0.2	10.12.2024	Adjusted structure after UCL feedback	Rabea Schulz
V1.0	08.01.2025	First draft	Femke Mulder
V2.0	24.01.2025	Second draft	Rabea Schulz, Femke Mulder, Gianluca Pescaroli
V2.1	04.02.2025	Internal review and review by SAB	Chris Needham-Bennett, Madalina Dusciuc
V3.0	20.02.2025	Final draft	Femke Mulder, Rabea Schulz

Acknowledgment

Project funded by the European Union's Horizon Europe under the grant agreement n°101121356 and the UK Research and Innovation (UKRI) programme. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Nature of the deliverable[1]	R

Dissemination level

PU	Public, fully open. e.g., website	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
CL	Classified information under the Commission Decision No2015/444	

Copyright notice

[1] Deliverable types:
R: document, report (excluding periodic and final reports).
DEM: demonstrator, pilot, prototype, plan designs.
DEC: websites, patent filings, press and media actions, videos, etc.
OTHER: software, technical diagrams, etc.

Table of content

Abbreviations

AD	Anno Domini
AGILE	AGnostic risk management for high Impact Low probability Events
AI	Artificial Intelligence
AM/FM	Amplitude Modulation / Frequency Modulation
BESS	Battery energy storage systems
CBRN	Chemical, biological, radiological, and nuclear
CI	Critical Infrastructure
COVID	Coronavirus disease 2019 (COVID-19)
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
DRR	Disaster Risk Reduction
Dx.x	Deliverable No. x.x
EV	Electrical vehicle
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HILP	High Impact Low Probability
ICT	Information and communication technology
IPCC	Intergovernmental Panel on Climate Change
ISO	International Organization for Standardization
LAN	Local Area Network
LNG	Liquefied natural gas
MORDOR	Massive, OveRwhelming Disruption of OpeRations
NATECH	Natural-hazard-triggered technological (incident)
NGO	Non-Governmental Organisation
NHS	National Health Service (United Kingdom)
SOC	Security Operations Centre
TETRA BOS	Digital radio for authorities and organisations with security tasks (Germany)
TLD	Top-Level Domain
U.S.	United States (of America)
UK	United Kingdom
USD	US-Dollar
VEI	Volcanic Explosivity Index
VIP	Very important person
WHO	World Health Organization

1. Introduction

This deliverable, **D4.1 Case Study Scenarios**, outlines AGILE's approach to scenario development for the stress test implementation. It explains how the scenario creation approach aims to balance a risk-agnostic perspective through randomisation and the specific interests of the case studies to ensure relevance and applicability.

The scenario approach and exemplary hypothetical scenarios outlined in this deliverable are fundamental to AGILE's mission to integrate innovative methodologies, such as stress testing and resilience assessment, into a unified disaster risk management approach. Stress testing, a core activity of the AGILE framework, relies on suitable scenarios that spark creativity and lateral thinking to identify common points of failure within systems confronted with High Impact Low Probability (HILP) Events. These scenarios contribute directly to the project's goals of understanding systemic risks, anticipating potential crises, and managing effective responses.

This deliverable contains the following key elements:

Scenario Development Methodology: The deliverable outlines a structured approach to creating hypothetical scenarios, incorporating risk-agnostic principles and a systems-focused perspective. It uses the AGILE Tier 1 Card Deck, which includes hazard, wild, and infrastructure cards to simulate complex emergencies and cascading failures.

Integration of Historical HILP Events: Historical case studies are used to highlight past systemic failures and lessons learned, providing valuable insights for future risk management. These examples help reduce cognitive biases against considering improbable scenarios.

Hypothetical Scenarios for Stress Testing and Adaption to Local Contexts: The document presents example scenarios, including regional, national, and cross-border events, tailored to different operational contexts. These scenarios are designed to "break" existing preparedness systems, fostering creativity and lateral thinking in identifying vulnerabilities. The methodology is adaptable to different geographical scopes and organisational needs. It includes mechanisms for modifying scenario elements to reflect specific local, regional, or national risks.

Counterfactual Analysis: A key component is the use of downward counterfactual analysis to explore alternative outcomes and identify additional vulnerabilities, enhancing the depth of risk assessment and preparedness planning.

2. Current practices of AGILE's case study partners

A survey was shared with AGILE's case study partners to get an overview of their current practices in regard to scenario exercises and scenario building. Seven out of nine case study partners provided input.

The survey responses reveal diverse practices in scenario development and scenario-based exercises across organisations. Scenarios are typically developed by internal teams, external consultants, or through collaboration between the two. The development process relies heavily on inputs such as historical data, risk assessments, expert judgment, and current or projected events. While some organisations adhere to established frameworks like ISO standards (e.g., ISO 9001, 27001, 22398) or Bloom's taxonomy, others prefer to use custom methodologies tailored to their specific needs.

Regarding the consideration of improbable or "freak" scenarios varies among organizations, while most focus on plausible or likely scenarios, some incorporate worst-case or High Impact, Low

Probability events into their planning. Only one organisation explicitly stated an openness to extreme "freak scenarios" such as alien invasions, with most favouring evidence-based and realistic approaches. Scenario design tends to prioritise practicality and alignment with organisational goals, leveraging stakeholder input and detailed risk analyses to ensure relevance.

Creativity is supported to some extent through role-playing and the incorporation of complexity in scenarios, which encourage participants to adapt dynamically. However, the emphasis generally leans more toward realism and practical relevance than fostering highly creative or unconventional thinking.

Challenges in scenario development and execution were also highlighted. These include difficulties in ensuring that modelled scenarios remain relevant, inconsistencies in stakeholder engagement, and gaps in hazard projection knowledge. Some organisations also noted the lack of comprehensive frameworks for guiding scenario design. Opportunities for improvement include enhancing creativity in scenario development by incorporating innovative methods and addressing knowledge gaps to create more robust and adaptable scenarios.

3. HILP Event Reference List

This section provides a summary of the insights and examples provided in AGILE D1.1. It starts by outlining the criteria that designate an event as a HILP, followed by a table summarising the HILP events discussed in D1.1. as well as the challenges they pose to emergency management. It concludes with a discussion of the applicability of these events as references for future risk management.

3.1. Criteria for HILP events

An event can be classified as a HILP if it meets both red criteria, as well as at least one of the criteria within each subsection, listed in the table below. The historical examples provided in AGILE deliverable 1.1, summarised below in section 3.2, have been selected based on these criteria.

Low probability	
Complexity and the role of uncertainty	
	Existence of concurrent, compound, interacting or interconnected dynamics
	Dynamics such as a sudden onset, creeping crises, or crossing thresholds/ tipping points
	Failure of tightly coupled systems that are designed and engineered to be highly reliable
Recombination of known and unknown patterns	
	The recombination of relatively common hazards that together result in an uncommon scenario
	The recombination of physical and social dynamics that are not directly associated with each other
Role of history	
	Events with a low recurrence / long return period / low likelihood.
	There is limited knowledge of known precursors
	There is a loss of memory / knowledge /awareness (total or partial) of the previous event
	Precursors are embedded in societal memory, but significant geomorphological and/or socio-technological changes have occurred since the event

High impact	
Quantitative measures	
	Context-specific impacts range from serious to catastrophic
Contextual impacts	
	A certain degree of irreversibility with regard to losses, both tangible or intangible
	A substantial, compromising, or disproportionate effect on a closed or isolated system
	High uncertainty in the dimensions of impact
System dynamics	
	There is a substantial loss of critical services and critical functions
	There are widespread or escalating cascading effects
	There is a lack of mitigation
Emergency response	
	There is a need to mobilise scarce resources and/or expertise, requiring aid from the international community and/or the creation of new expertise
	Impacts are associated with major policy changes and/or the development of new technology.

3.2. Previous HILP events

The table below lists historical HILP events that meet the HILP criteria outlined above.

Using the Grenfell Tower Fire as a concrete example, it meets the criteria in the following way:

- Existence of interacting dynamics - a malfunctioning refrigerator on the fourth floor + the presence of combustible cladding and insulation that had been installed during a recent refurbishment.
- Recombination of known and unknown patterns - fire in a high-rise building (known) + combustible cladding and insulation (unknown and unexpected: the actions of the fire brigade assumed that the cladding and insulation would *not* be highly combustible).
- Role of history – learning from history was no longer correct. The (wrong) learning was that modern buildings would not have highly combustible cladding and insulation.
- Quantitative measures – the context-specific impacts were serious: 72 people died and many were injured.
- Contextual impacts – the damage to Grenfell Tower was irreversible.
- System dynamics – the fire had widespread effects and there was no adequate mitigation.
- Emergency response – the event triggered broader building-regulation reviews and changes in high-rise safety policies.

The table below lists selected HILPs from D1.1 chronologically and clustered into natural hazards and technological hazards (both European and worldwide). The description includes key points about the HILP event and key insights and challenges for the emergency management.

Events before 1946	
Mount Vesuvius Eruptions (79 AD, 1631 AD)	
Natural hazard: volcanic eruption	
Key Points: • 79 AD eruption (VEI ~5) buried Pompeii and Herculaneum in pyroclastic flows and ash.	Emergency Management Insights/ Challenges: • Early warning systems did not exist historically; modern-day seismic, gas,

• Thousands of fatalities, largely from asphyxiation, thermal shock. • 1631 eruption resulted in significant local destruction, 3,000–6,000 fatalities.	and ground-deformation monitoring could mitigate impacts. • Today, dense urbanisation near Vesuvius increases risk: need for comprehensive risk assessments and land-use planning. • Effective evacuation plans and public awareness crucial.
Katla Eruption (1755) & Historic Volcanic Activity in Iceland	
Natural hazard: volcanic eruption	
Key Points • Large subglacial eruptions every ~60 years. Katla in 1755 caused glacial-outburst floods (jökullhlaups) • Significant ash fallout: farms were abandoned, grass/vegetation destroyed. • Coincided with unseasonably cold weather and famine; ~5,800 people died in total across Iceland.	Emergency Management Insights/ Challenges: • Compound effects (volcano + extreme weather + famine). • Importance of alternative food or supply routes in isolated regions. • Modern impacts on aviation (2010 Eyjafjallajökull eruption) highlight need for coordinated emergency response plans.
Carrington Event (1859)	
Natural hazard: solar flare	
Key Points • One of the largest recorded solar flares; caused global auroras and disrupted telegraph systems. • Fires started from induced currents in telegraph wires.	Emergency Management Insights/ Challenges: • Modern reliance on electrical grids, communication networks, and satellites means a Carrington-like event today could cause global blackouts, GPS failures, etc. • Very short lead times for space-weather forecasting call for robust contingency planning and resilient infrastructure.
Krakatoa Volcanic Eruption (1883)	
Natural hazard: volcanic eruption	
Key Points • Massive eruptions; ~36,000 fatalities, mostly from tsunamis. • Ash ejected 80 km high: global temperatures dropped by ~0.5°C. • Collapsed island generated further pyroclastic flows and tsunamis.	Emergency Management Insights/ Challenges: • Large-scale eruptions (“super volcanoes”) have far-reaching impacts on climate, agriculture, trade routes, and even global stability. • Potential for global disruption, requiring international cooperation and contingency planning.
Tunguska Meteoroid Event (1908)	
Natural hazard: meteoroid event	

Key Points	Emergency Management Insights/ Challenges:
• Remote region of Siberia; ~2,000 km² of forest flattened. • Massive explosion/atmospheric impact, but minimal immediate human impact due to remoteness.	• The event can be used to reflect on the possible impacts and implications of similar size events as well as the statistical implications • It can also be used to reflect on the common variations in the environment that could be triggered by similar low probability high impact events e.g. variations in sun light that were recorded just during Krakatoa eruptions.
Messina Earthquake (1908)	
Natural hazard: earthquake	
Key Points	Emergency Management Insights/ Challenges:
• Magnitude 7.1–7.5. Killed ~60,000–100,000 in Sicily & Calabria, Italy. • Tsunami of ~10–12m followed the quake, complicating rescue efforts.	• Importance of building codes and earthquake-resistant construction. • Need for pre-designated safe zones to avoid tsunami inundation.

Events between 1946 and 2001	
Netherlands Floods (1953)	
Natural hazard: floods	
Key Points	Emergency Management Insights/ Challenges:
• Severe storm + spring tide overwhelmed dikes. • 1,836 fatalities; tens of thousands of animals lost, huge infrastructure damage. • Led to Delta Works flood-protection program.	• Timing (evacuation decisions must be made early, under uncertainty). • Involvement of multiple agencies (local, provincial, private sector). • Difficulty ensuring a consistent public message. • Prevention vs. reaction: pre-emptive infrastructure shutdowns and mass evacuations.
Vajont Dam Disaster (Italy, 1963)	
Natural hazard: landslide	
Key Points	Emergency Management Insights/ Challenges:
• Massive landslide displaced water, causing a 250m wave overtopping the dam. • ~2,000 lives lost; towns of Longarone, Erto, Casso devastated.	• Importance of rigorous risk assessment in infrastructure projects, especially in geologically unstable regions • Importance of regulatory oversight, accountability in dam construction and operation

	• Need to strengthen regulatory frameworks, enforce safety standards, and ensure transparent monitoring and inspection processes
Chernobyl Disaster (1986)	
Technological hazard: nuclear accident/incident	
Key Points • The accident was triggered by a flawed reactor and unsafe testing procedures. • Over 300,000 people were evacuated; exclusion zone up to 30 km established.	Emergency Management Insights/ Challenges: • Initial response indicated a lack of preparedness. Decisions had to be made on criteria that could have been established beforehand - areas of overlapping responsibility and jurisdiction should have been clearly defined & permanent infrastructure (including rapid communication systems, intervention teams, monitoring networks) should have been set up beforehand. • Many countries took steps to establish such monitoring networks and reorganise their emergency response efforts - accident led to major changes in safety culture and in industry cooperation worldwide.
Baltimore Freight Rail Crash (USA, 2001)	
Technological hazard: train derailment	
Key Points • Derailment caused fires, toxic smoke, water main rupture, internet disruption (fibre optic cable damage). • Prolonged closure of downtown Baltimore.	Emergency Management Insights/ Challenges: • The case highlights compounding failures in tightly coupled systems • A lack of understanding of existing interdependencies led to difficulties in predicting cascading effects • It shows the importance of coordination, information sharing, prioritisation, and plans for escalating the response across operational sectors
Events between 2002 and now	
Floods in Prague (2002)	
Natural hazard: floods	
Key Points • Massive rainfall led to floods in several Central European countries.	Emergency Management Insights/ Challenges: • Cascading effects (chemical spills, utility shutdowns, water contamination).

• Prague severely flooded: damage to cultural heritage, chemical spills from industries. • Cross-border impacts on power plants, water treatment, disease outbreaks (hepatitis).	• International coordination for relief. • Prompted Europe-wide reforms (Floods Directive).
Indian Ocean Tsunami (2004)	
Natural hazard: tsunami	
Key Points • Deadliest tsunami in recorded history (~230,000–300,000 fatalities), multi-country impact. • Initiated by a 9.1–9.3 magnitude undersea earthquake off Sumatra. • Lack of effective early warning systems in the Indian Ocean resulted in a delayed response and increased casualties.	Emergency Management Insights/ Challenges: • Challenges in coordinating an international response and facilitating effective communication. • Destroyed critical infrastructure (including communication networks, transportation systems, and healthcare facilities) hampered relief. • Lessons led to Indian Ocean Tsunami Warning System.
Hurricane Katrina (USA, 2005)	
Natural hazard: tropical cyclone	
Key Points • Storm surge overwhelmed levees: ~80% of New Orleans flooded. • 1,800 lives lost: costliest storm in US history (~$160+ billion). • Major social and political fallout over delayed response.	Emergency Management Insights/ Challenges: • Inadequate flood-protection and evacuation planning. • Complex, large-scale sheltering and logistics. • Spotlight on critical infrastructure (levee design, power, communications).
Northern Rock Crisis (UK, 2007)	
Financial & economic hazard: bank run	
Key Points • First UK bank run in ~140 years; depositors withdrew ~£3 billion in 3 days. • Bank nationalised; exposed systemic weaknesses in short-term funding dependence.	Emergency Management Insights/ Challenges: • Revealed vulnerabilities in financial regulation, oversight, deposit insurance schemes. • A business model reliant on securitisation faced a “liquidity freeze.” • Showed how HILP financial events can cascade quickly into wider economic crisis.
Alluvial Flooding in Madeira (2010)	
Natural hazard: flooding	
Key Points	Emergency Management Insights/ Challenges:

• Extreme rainfall exceeding all previous records in Portugal (~185 l/m²). • Flash floods, slope failures, structural collapses; 47 fatalities, ~600 homeless. • Major transport/logistical difficulties on a mountainous island.	• Lack of historical precedent led to underestimation of impacts. • Damage to infrastructure hindered rescue. • High reliance on external resources (reinforcements from mainland).
Deepwater Horizon Oil Spill (Gulf of Mexico, 2010)	
Technological hazard: industrial accident/incident	
Key Points • Largest marine oil spill in history (~4.9 million barrels). • The Deepwater Horizon offshore drilling rig suffered a catastrophic blowout while drilling an exploratory well. • The blowout preventer, a critical safety device designed to seal the well in the event of an emergency, failed to activate. • Massive environmental damage to fisheries, tourism, and marine ecosystems.	Emergency Management Insights/ Challenges: • The scale and complexity of the spill required a coordinated multi-agency response. • The remote location of the spill site presented logistical challenges for containment and clean-up operations. • The failure of critical safety systems and inadequate contingency planning highlighted the need for better regulatory scrutiny and industry practices.
Eyjafjallajökull Eruption (Iceland, 2010)	
Natural hazard: volcanic eruption	
Key Points • Volcanic ash cloud disrupted European air traffic for ~1 week, stranding ~8.5 million passengers. • Physical damage in Iceland was relatively small; global transport disruption was severe.	Emergency Management Insights/ Challenges: • Tight coupling of air transport system with global supply chains. • Highlighted importance of volcanic ash monitoring and crisis coordination for aviation. • Economic ramifications from the secondary/cascading effects were far larger than direct impacts.
Tōhoku Triple Disaster (Japan, 2011)	
Natural and technological hazards: earthquake, tsunami, and nuclear accident	
Key Points • Magnitude 9.0 earthquake + tsunami killed ~18,000. • Fukushima Daiichi nuclear accident forced evacuation of ~200,000 people. • Global economic impact (supply chain disruptions, nuclear debate).	Emergency Management Insights/ Challenges: • Worst-case natural–technological cascade (earthquake → tsunami → nuclear meltdown). • Complexity of multi-hazard response; vital infrastructure (ports, roads) severely damaged. • Long-lasting radioactive contamination, political debate over nuclear safety.

WannaCry Cyberattack (2017)	
Technological hazard: cyber attack	
Key Points • Ransomware exploited unpatched Windows systems; 230,000+ computers worldwide hit in <24 hours. • NHS (UK) severely impacted: 595 GP practices, one-third of hospital trusts disrupted.	Emergency Management Insights/ Challenges: • Outdated and unpatched software in critical sectors. • Rapid spread highlighted global interconnectivity vulnerabilities. • Need for continuous cybersecurity monitoring, patching, backups, crisis protocols.
Grenfell Tower Fire (UK, 2017)	
Technological hazard: major structural fire	
Key Points • High-rise residential fire killed 72 people. • Rapid spread due to combustible cladding and insulation. • Major inquiry into building safety, cladding, and “stay put” fire policy.	Emergency Management Insights/ Challenges: • Flammable external cladding catalysed fire spread, rendering “stay put” strategy lethal. • Communication breakdown about evacuation instructions. • Triggered broader building-regulation reviews and changes in high-rise safety policies.
Forest Fires in Central Portugal (2017)	
Natural hazard: wildfire	
Key Points • Worst summer in terms of forest fires on record: ~440,000 hectares burned, 115 fatalities. • Rare weather phenomena (down-burst), strong winds, extremely dry conditions. • Most of the burnt area and fatalities were recorded outside the periods considered most critical. Pedrógão Grande fire in June killed 66 in <24 hrs, many fires in October. • Damages of ~€500 million, political fallout and resignations.	Emergency Management Insights/ Challenges: • Rapid spread overwhelmed firefighting resources. • The events exposed systemic vulnerabilities, prompting calls for reforms and improvements in forest fire prevention, detection, and response mechanisms. • Enhancing coordination, communication, and capacity-building emerged as critical priorities for strengthening resilience against future fire seasons.
Venice Floods (2019)	
Natural hazard: floods	
Key Points • Acqua alta reached 187 cm, ~80% of city underwater, massive property/cultural heritage damage.	Emergency Management Insights/ Challenges:

• Resulted from several moderate factors combining (storm surge + full moon tide + local pressure anomaly). • Two fatalities, hundreds of millions of euros in damages.	• Compounding hazards: moderate events aligning can create an extreme outcome. • Small errors in forecasting can lead to big misses in water-level predictions. • Repeated high tides immediately afterward impeded recovery.
COVID-19 Pandemic & Loss of Critical Services (2020–2022)	
Biological hazard: pandemic	
Key Points • Pandemic was not entirely unexpected, as pandemics were recognized as likely (e.g., risk registers, WHO, World Bank). • Cascading failures: healthcare system overload, supply-chain disruption, economic upheaval. • Showed vulnerability of networks, reliance on just-in-time supply chains, and complexities of concurrent hazards (e.g., Texas power crisis in February 2021).	Emergency Management Insights/ Challenges: • Coordinating multifaceted response across public health, economic, and social domains. • Preparedness and stress-testing for interdependent systems (healthcare, supply, energy). • Complex, protracted emergencies require adaptive, agile governance.
Suez Canal Blockage (2021)	
Technological hazard: failure in transport	
Key Points • The mega container ship *Ever Given* ran aground in high winds, blocking ~12% of global trade for six days. • Backlog of ~450 ships; major delays in container flows, ~15–17 billion USD in goods held up daily. • Cleared on 29 March; global supply chains felt residual effects for weeks.	Emergency Management Insights: Insights/ Challenges: • Single choke point with no redundancy; high vulnerability to disruption. • Necessitates alternative routes or strategies (e.g., Cape of Good Hope, air freight, or other canals). • Shows fragility of global trade networks and need for robust risk mitigation.
Floods in Germany (2021)	
Natural hazard: floods	
Key Points • Storm “Bernd” caused up to 150 mm rain/48 hrs; 180+ fatalities, widespread destruction. • Major infrastructure damage (power, mobile networks, water treatment). • Flood forecasting, warning and response systems proved largely ineffective.	Emergency Management Insights/ Challenges: • In Germany, responsibility for non-police emergency response lies at the municipal-level – some too small to effectively prepare for events of this magnitude. • Overloaded crisis communications (specifically: the disaster control radio system TETRA BOS).

	• Need for central leadership, better training, and more effective communications.
Wildfires in Hawaii (2023)	
Natural hazard: wildfires	
Key Points • Fast-moving fires in Lahaina (Maui), 98 fatalities; the deadliest U.S. wildfire in ~100 years. • Powerful winds, extremely dry conditions, limited firefighting resources. • Communication gaps (power outages, sirens sounding just one tone – no instructions on what to do, local media confusing evacuation advice for wildfires with that for tsunamis) led to delayed evacuations.	Emergency Management Insights/ Challenges: • Incomplete and confusing messaging, delayed alerts, and power disruptions hindered evacuation efforts. • The lack of clear evacuation plans, especially for densely populated areas, led to traffic management failures and delays • The reliance on sirens and incomplete information dissemination proved inadequate, highlighting the need for integrated, advanced alert systems

3.3. The applicability of historic HILP events as references for future risk management

HILP events typically arise from an improbable combination of stressors that converge simultaneously or compound one another in unexpected ways. Because each HILP involves a unique set of interacting factors, the exact same scenario is unlikely to repeat. Nevertheless, studying historical HILP events is extremely valuable. These past incidents often highlight common points of failure and systemic vulnerabilities in disaster preparedness and mitigation—weak spots that are likely to appear in other extreme crises as well.

Another important benefit of looking at historical HILPs is that it can reduce people's reluctance to consider how their systems might fare under "fantastical" or highly improbable conditions. Since these events have already happened, they provide real-world evidence that even seemingly far-fetched scenarios can become reality. By examining how existing preparedness and mitigation measures performed - or failed - during previous HILPs, decision-makers, planners, and stakeholders can strengthen their strategies to be more resilient against future high-impact threats, no matter how unlikely they may seem.

4. Development of Hypothetical Scenarios for Tabletop Exercises

4.1. Scenario Development Methodology

4.1.1. The approach to scenario creation

The AGILE Tier 1 Stress Test combines a risk-agnostic, systems-focused approach with concrete scenarios. These scenarios may be fully randomised - allowing participants to analyse their preparedness and response from fresh perspectives - or partially predetermined so they can concentrate on hazards and infrastructure systems aligned with their specific objectives. The goal is to confront participants with high-impact, low-probability events (such as unexpected, concurrent, compounding hazards with cascading impacts on unforeseen infrastructure systems).

The scenarios are intended to be so extreme as to “break” existing preparedness and mitigation systems. In doing so, the scenarios demand creativity and lateral thinking, ultimately fostering deeper strategic insights into systemic vulnerabilities and how best to mitigate them.

This deliverable builds on the guidelines for scenario development provided in AGILE D1.3. The main purpose of scenarios is to provide planners with insights into the needs, constraints, and assumptions that shape disaster management in different situations. Disaster scenarios help disaster managers prepare for future crises and understand their broader context, including political, socio-economic, and infrastructural components. Alexander (2000, 2002, 2017) emphasised the value of structured exercises in addressing these complexities. AGILE D1.3 highlights the benefits of a risk-agnostic, systems-focused approach to scenario building because it concentrates on the underlying principles - such as leadership, coordination, and communication - that apply across a wide range of potential hazards, rather than on any single threat. By centring on universal needs, constraints, and limitations, organisations become more adaptable and better prepared for unexpected crises. This flexibility ensures that core capabilities remain relevant whether the emergency is an earthquake, a flood, or an entirely unforeseen event. D1.3 notes that it can be hard for participants to grasp “generic” scenarios initially and therefore recommends exposure to a diverse range of specific hazards over time to cultivate the capacity to generalise effectively.

Focusing on HILP (High-Impact, Low-Probability) scenarios is especially helpful because they help organisations identify and address systemic weaknesses by “pushing their systems to the limit” and revealing critical vulnerabilities. This process fosters more versatile contingency plans that centre on the broader consequences rather than on every conceivable threat. It also encourages organisations to look beyond preventive measures and develop robust response strategies for when prevention fails. The inherent uncertainty of HILPs requires decision-makers to adopt flexible, creative, and forward-looking approaches, enabling them to adapt and improvise effectively when traditional planning falls short. Ultimately, these efforts lead to greater resilience against extreme events. D1.3 also highlights the importance of integrating strategic foresight and lateral thinking (or creativity) into scenario development because this helps organisations anticipate and respond to previously unthinkable crises. By combining systematic exploration of future trends (strategic foresight) with imaginative, flexible thinking (lateral thinking), planners can imagine unexpected possibilities, overcome rigid assumptions, improve engagement, increase adaptability, strengthen coordination, and shift from reactive to proactive approaches. By proactively preparing for less obvious threats, communities become better equipped to weather - and even mitigate - catastrophic events.

4.1.2. The AGILE Card Game

Unique scenarios will be developed for the Tier 1 Stress Test by drawing cards from a deck. Below follows an overview of this process. The expected duration of the Tier 1 Stress Test is approximately 3 hours.

Structure

Prior to the stress test

Facilitators and case study representatives co-design the scenario, supported by AI.

- Two hazard cards, one infrastructure card, and one wild card are drawn. This process can be fully or partially randomised. See sections 4.1.3 and 5 for details.
- Up to nine elective facilitation questions are selected (three per level) out of a total of 152 to ensure that the scenario addresses the requirements of the case study. Identifying useful and relevant elective facilitation questions is done based on a 10-item questionnaire (to be developed). See sections 4.1.3 and 5 for details.

- The above details are entered into a LLM (like Chat GPT) to develop a coherent narrative that encompasses all elements of the emerging scenario.
- Informed by Tier 0 and based on the scenario that has emerged, facilitators and case study representatives will identify concrete participants to invite to take part in the stress test. Alternatively, if it is not possible to invite external stakeholders, concrete roles will be identified for participants to role play.

Introduction (30 minutes)

The session begins with an introduction lasting 30 minutes. This segment will outline the objectives, provide background context, and clarify the methodology to be used throughout the exercise. It some situations, it may be possible to implement the four bullet points outlined above under “prior to the stress test” during the introduction, e.g., when no external stakeholders participate.

Main Analysis (3 progressive steps, 45 minutes each)

The core of the session consists of three progressive steps, each lasting 45 minutes:

Step 1: Start with the two hazard cards and one wild card.
In this step, participants evaluate the impacts of two separate hazard events within a specific context defined by the wild card. Each hazard is assessed individually and in isolation. The goal is to establish what impacts the two events have in common and identify common points of failure in preparedness and mitigation. Next, focusing on one of these hazards, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Step 2: Add no new cards.
In this step, participants evaluate what would happen if the two hazards they selected happened at the same time within a specific context defined by the wild card. The two hazards are assessed together, with the aim of identifying concurrent and potentially compounding impacts. Next, focusing on both hazards together, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Step 3: Add the infrastructure card.
This final step extends the complexity of the analysis by incorporating cascading impacts on potentially unexpected infrastructure systems - within a specific context defined by the wild card. Next, focusing on both hazards and their cascading impacts, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Evaluation during the stress test
During the stress test, facilitators observe and note down examples of how participants approach systemic risk and to what extent they display lateral thinking, focusing on the following points:

- How often do participants discuss shared vulnerabilities across hazards?
- How explicitly do participants identify “must-have” capabilities, services, or infrastructure?
- How frequently do participants link failures in one system to cascading impacts in others?
- Were participants proposing out-of-the-box solutions or only standard procedures?

During the stress test, the facilitators score the participants’ performance against these four points on a scale of 1-3. Whereby 1 = not demonstrated, 2 = adequately demonstrated, 3 = thoroughly demonstrated.

Debrief (Maximum 30 minutes)

The stress test concludes with a comprehensive debrief that examines how participants approached systemic risk and demonstrated lateral thinking. As part of this session, each

participant spends two or three minutes documenting the most creative or unconventional idea they encountered—or proposed themselves. This exercise aims to gauge the variety of creative solutions and understand their perceived value. In addition, the results of the in-test evaluation are shared, and participants are encouraged to reflect on the overall experience. Discussion questions might include, “Which moment in the exercise pushed you to think differently about the problem?” and “Did you feel comfortable challenging assumptions or proposing untested ideas? Why or why not?” These reflections provide deeper insight into how participants understood and approached the challenges presented by the scenario.

4.1.3. Consideration of Local, Regional, National and Cross-border Contexts

The Tier 1 case study partners differ widely in the geographical scope of their mandates, their levels of maturity in disaster management, and the specific objectives they aim to achieve through the stress test. The Tier 1 stress test is designed to be flexible and can be adapted to meet the geographical remit, capacity, and goals of different participants. This adaptability is achieved in three ways:

1) Modifying the card deck.
2) Identifying specific participants / roles to include in the stress test.
3) Tailoring the facilitation questions.

Each approach will be discussed in detail below.

The Card Deck

The card deck can be used in three different ways to develop a scenario for the stress test:

1) Full Randomisation. Case study partners have the option to fully randomise all hazard cards, the wild card, and the infrastructure card. Full randomisation is optimal for AGILE’s risk-agnostic systems-focused approach. The unexpected combinations of hazards, contexts (wild cards), and cascading impacts (infrastructure cards) can shed new light on preparedness and mitigation systems. This method challenges participants to apply creativity and lateral thinking, fostering deeper strategic insights into systemic vulnerabilities and how to address them.

2) Prefiltered Card Deck. Research presented in D1.3 highlights that some participants are uncomfortable with scenarios that include hazards that are too fantastical (e.g., alien invasion), preferring instead to focus on hazards that could realistically occur in their geographical area. To accommodate this preference, facilitators can pre-filter the hazard deck to include only hazards listed in the relevant local, regional, or national risk registers. Furthermore, to adjust the difficulty of the scenario, certain wild cards can be excluded. Please see section 3.2.2.“Set of Possible Circumstances”

3) Preselected Cards Specific hazard or infrastructure cards can be preselected to align with participants’ particular objectives. This approach can be combined with filtering the deck based on the relevant risk register. To ensure that the resulting scenario is not fully predetermined, no more than two cards should be preselected. Ensuring some randomisation preserves an element of surprise, pushing participants to step outside their comfort zones and examine their systems from new perspectives, identifying gaps in preparedness and mitigation that may otherwise be overlooked.

The Participants / Roles to include in the Stress Test

During the Stakeholder Mapping conducted for Tier 0, broad stakeholder categories for inclusion in the Tier 1 Stress Test will have been identified, such as “emergency response,” “interest groups,” or “infrastructure management.” As part of the preparation for the Tier 1 Stress Test, facilitators, working with case study representatives, will determine which specific organisations or roles to involve. This selection will be guided by the hazard cards, wild card, and infrastructure

cards chosen for the exercise. For instance, if the Tier 0 stakeholder map includes the category “NGOs” and the scenario involves flooding, it would be logical to include local flood action groups in the stress test. Likewise, if “emergency services” are mapped in Tier 0 and the scenario features a wildfire, members of the fire brigade should be involved.

The Facilitation Questions

As part of facilitation, the scenarios are further adapted to participants’ geographical scope, objectives, and experience level. Each of the three main analysis steps starts with two mandatory questions, followed by up to three optional questions that participants can choose based on their specific needs and goals. Afterward, a downward counterfactual analysis is conducted, guided by a structured set of questions.

The optional questions are grouped into three categories:

- Physical: Focused on sensors, facilities, equipment, system states, and capabilities.
- Information and Cognitive: Addressing data creation, manipulation, and storage, as well as understanding, mental models, preconceptions, biases, and values.
- Social and Organisational: Exploring interaction, collaboration, and self-synchronisation among individuals and entities.

The elective questions are listed at the end of this section.

Step 1: Two single hazards (discussed in turn) followed by a counterfactual analysis.

In this step, participants evaluate the impacts of two separate hazard events within a specific context defined by the wild card. Each hazard is assessed individually and in isolation. The goal is to establish what impacts the two events have in common and identify common points of failure in preparedness and mitigation. Next, focusing on one of these hazards, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Mandatory questions

Spend 15 minutes exploring the following questions.

- Discuss for each hazard event, in turn, how you know what happened.
- Which systems could be affected by both hazard events? What vulnerabilities or point of failures could they have in common that would be affected by both events?

Elective questions

Let participants choose a maximum of 3 questions from any or all of the categories listed below, in line with their focus and objectives. Spend 20 minutes exploring these questions.

[The elective questions are listed at the end of this section].

Counterfactual analysis

Spend 15 minutes exploring the following questions, focusing on one of the two hazards and the wild card.

- What if you have no reserves, experience a just-in-time failure, or have less availability than expected?
- What’s the worst thing that could happen given the circumstances?

Step 2: Two concurring hazards, compounding effects and a counterfactual analysis.

In this step, participants evaluate what would happen if the two hazards they selected happened at the same time within a specific context defined by the wild card. The two hazards are assessed together, with the aim to identify concurrent and potentially compounding effects. Next, focusing

on both hazards together, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Mandatory questions
Spend 15 minutes exploring the following questions.

- In what ways could the two hazards interact to compound the effect of the crisis? What credible challenges or failures in disaster management or governance could happen that would escalate the emergency?
- What is essential to ensure flexibility in the response? Are there any backups you assume would be functional? How would they be affected if the two hazards occurred at the same time?

Elective questions
Let participants choose a maximum of 3 questions from any or all of the categories listed below, in line with their focus and objectives. Spend 20 minutes exploring these questions.

[The elective questions are listed at the end of this section].

Counterfactual analysis
Spend 15 minutes exploring the following questions, focusing on both of the hazards, their interactions, and the wild card.

- Would the resources currently allocated to managing the individual hazards still be adequate if the two hazards occurred at the same time – and if not, how would you address this?
- Are there any points of failure that have not been discussed to date to prevent damaging relationships or partnerships? What would the implications of this be if both hazards happened at the same time?

Step 3: Two concurring hazards, compounding effects, cascading impacts, and a counterfactual analysis
This final step extends the complexity of the analysis by incorporating cascading impacts on potentially unexpected infrastructure systems - within a specific context defined by the wild card. Next, focusing on both hazards, any compounding effects, and cascading impacts, participants are asked to conduct a downward counterfactual analysis, exploring what else could have gone wrong.

Mandatory questions
Spend 15 minutes exploring the following questions.

- What is the maximum level of disruption that the selected critical infrastructure could withstand? How might its failure cascade into other connected systems?
- Which assets and processes lack diversity or redundancy, and how might this increase the risk of cascading impacts?

Elective questions
Let participants choose a maximum of 3 questions from any or all of the categories listed below, in line with their focus and objectives. Spend 20 minutes exploring these questions.

[The elective questions are listed at the end of this section].

Counterfactual analysis
Spend 15 minutes exploring the following questions, focusing on both of the hazards, their interactions, any cascading impacts, and the wild card.

- How could insider risk undermine your preparedness and response?
- How could failures in training or coordination trigger broader impacts?

Elective questions

During the preparation for the stress test, facilitators will help participants select up to three elective questions per step to explore. Participants are not expected to read through all 152 elective questions; instead, facilitators will match questions to the scenario, the step, and the objectives of the case study partners. A 10-item questionnaire will be created to guide facilitators in identifying the most relevant questions for each group.

Physical Exposure		
Population		
Exposure of vulnerable categories	1)	To what extent have population categories that are more vulnerable to disaster risks been identified at the national and sub-national levels? (e.g., elderly)
Medium term recovery	2)	To what extent have the medium-term needs of vulnerable population categories affected by disaster risk been addressed by effective recovery practices? (e.g., accommodation, access to services, livelihood opportunities in the host community).
Geographical concentration of vulnerable categories	3)	To what extent has an assessment process been developed to identify geographical concentrations of vulnerable population categories at the national and sub-national levels? Has this been contextualized within broader disaster risk reduction strategies and led to targeted actions? (e.g., elderly)
Population vulnerable to concurrent climate extremes	4)	To what extent have categories of the population that are more vulnerable to concurrent climate extremes, such as those exacerbated by climate change, been assessed and identified at national and sub-national levels? Has this been integrated into broader disaster risk reduction strategies and resulted in targeted actions? (e.g., people with cardiac conditions)
Population vulnerable to technological failures (e.g. blackouts)	5)	To what extent have categories of the population that could be more vulnerable to technological failures, such as blackouts, been assessed and identified at the national and sub-national levels? Has this been contextualized within broader disaster risk reduction strategies and resulted in targeted actions?
Ecology and ecosystem		
Awareness and understanding of ecosystem services and functions	6)	Beyond merely recognizing natural assets, to what extent is there a shared understanding of the ecosystem services and functions they provide at the national and subnational levels?

Integration of green and blue infrastructure into city policy and projects	7)	To what extent are green and blue infrastructures being promoted in major urban developments and infrastructure projects through policies at the national and subnational levels? (e.g., landscape elements such as parks and ponds)
Transboundary environmental issues	8)	To what extent is the importance of natural assets beyond their administrative or jurisdictional borders recognized, and are there plans at the national and subnational levels to support their protection and management?
Green infrastructure as mitigation	9)	To what extent have green and blue infrastructures been explored as potential risk reduction measures for the effects of concurrent climate extremes? (e.g., droughts and heatwaves)
Critical infrastructure, lifelines, and logistics		
Critical infrastructure identification and protection	10)	To what extent has the country identified its critical infrastructure and implemented protection plans to safeguard these infrastructures from disasters?
Hazardous infrastructure	11)	To what extent have critical infrastructures that pose specific standalone hazards (e.g., nuclear facilities) been assessed for emergency planning and disaster risk reduction at the national and subnational levels?
Maintenance	12)	To what extent are the monitoring, maintenance, and renewal of essential critical infrastructure promoted at the national and subnational levels?
Supply chain disruption	13)	To what extent has the risk of supply chain disruptions affecting critical national infrastructure been assessed, and have adequate risk reduction measures been implemented at the national and subnational levels?
Spare capacity	14)	How much spare capacity exists in high-ranking critical infrastructures, such as main power plants and primary wastewater treatment facilities?
Interdependencies and critical dependencies	15)	To what extent have critical dependencies and interdependencies been identified, documented, and analysed at the national level?
Coordination infrastructure	16)	To what extent has the vulnerability of national and subnational coordination centres been tested under various high-probability and low-probability risk scenarios, including complex situations? (e.g., the impact of blackouts or transport failures on governmental buildings, simultaneous triggers, hybrid scenarios)
Multi-level damage assessment	17)	To what extent can damage to critical infrastructure caused by disasters be

		calculated at the national and subnational levels? Additionally, to what extent does this assessment include the indirect and cascading effects of reduced operational capacity on society?
Energy disruption	18)	To what extent have the possible worst-case scenarios of disruptions in the energy sector and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Transport disruption	19)	To what extent have the possible worst-case scenarios of disruptions in the transport sector (ground, air, water, rail) and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Communication disruption	20)	To what extent have the possible worst-case scenarios of disruptions in the communication sector and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Internet disruption	21)	To what extent have the possible worst-case scenarios of disruptions in the internet sector and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Satellite infrastructure disruption	22)	To what extent have the possible worst-case scenarios of disruptions in the satellite infrastructure sector and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Water and wastewater	23)	To what extent have the possible worst-case scenarios of disruptions in the water and wastewater sector and their cascading effects at national and subnational levels been assessed? Have any risk reduction measures been implemented?
Emergency facilities	24)	To what extent have the possible worst-case scenarios of disruptions to emergency services at the national and subnational levels been assessed? Have any risk reduction measures been implemented?
Logistic nodes	25)	To what extent have geographic areas that depend on a single or primary transport infrastructure been assessed at the national and subnational levels? Have any risk reduction measures been identified to mitigate possible worst-case scenarios in those areas?
Climate change	26)	To what extent have protective mitigation measures been designed to account for climate change drivers and the increased concurrency of triggers? To what extent has

	this been integrated into existing disaster risk reduction strategies?
Built environment (including housing)	
Land use zoning	27) Are all geographic areas appropriately zoned, considering the impacts of key risk scenarios on economic activities, agricultural production, and population centres?
Housing vulnerability	28) To what extent has housing in areas exposed to the "most likely" and "most severe" risks been assessed at the national and subnational levels to identify vulnerable structures, leading to the adoption of specific disaster risk reduction actions (e.g., retrofitting)?
Education facilities	29) To what extent has the vulnerability of schools and educational facilities to the "most probable" and "most severe" risks been analysed at the national and subnational levels, leading to the adoption of specific risk reduction actions?
Emergency shelter	30) To what extent have emergency shelters been identified at the national and subnational levels for the "most likely" and "most severe" risks? Were their locations chosen with consideration of their vulnerability to complex scenarios?
Retrofitting for climate extreme	31) To what extent have heating and cooling systems in social housing and public facilities been designed to account for the effects of projected climate extremes? Have any buffering measures and redundancies been planned?
Industrial sites and touristic areas	
DRR for industrial sites	32) To what extent has the country identified and supported the implementation of targeted disaster risk reduction measures in areas with high concentrations of industrial sites and supply routes at the national and subnational levels? (e.g., safe evacuation routes)
Bottlenecks industrial sites	33) To what extent are logistical bottlenecks in areas with high concentrations of industrial sites and supply routes recognized at the national and subnational levels? How is this information shared to support the coordinated development of business continuity strategies at these levels?
DRR for touristic areas	34) To what extent has the country identified and supported the implementation of targeted disaster risk reduction measures in touristic areas at the national and subnational levels? (e.g., multi-language information, safe practices, and instructions for hotels)

Hybrid threat for strategic production	35)	To what extent have targeted risk assessments for hybrid risks been conducted in areas with high concentrations of industrial sites at the national and subnational levels? To what extent did these assessments include the prioritization of strategically important targets?
Hybrid threat in touristic areas	36)	To what extent have the implications of hybrid risks for touristic areas been assessed at the national and subnational levels and utilized to develop new scenarios? (e.g., reputational and economic damages caused by misinformation during peak tourist seasons)
Chemical and biological sites vulnerability to cascading failures	37)	To what extent have the dependencies and vulnerabilities of chemical and biochemical sites been assessed for scenarios involving disruptions in other critical infrastructure sectors at the national and subnational levels? (e.g., electricity, telecommunications, and transport)
Chemical and biological sites vulnerability to hazards	38)	To what extent has the country assessed the locations of chemical or biological sites in areas vulnerable to natural hazards or man-made threats at the national and subnational levels? Have these sites been ranked based on their potential to initiate cascading events? (e.g., NATECH)
Chemical and biological sites vulnerability to concurrence	39)	To what extent have the vulnerabilities of chemical and biochemical sites to concurrent climate extremes been assessed at the national and subnational levels?
Chemical and biological sites vulnerability to interacting hazards	40)	To what extent have the vulnerabilities of chemical or biological sites to interacting hazards been assessed at the national and subnational levels?
Food and water supply		
Root causes loss of water and food supply	41)	To what extent have the possible root causes leading to a significant loss of water and food supply been assessed and understood at the national and subnational levels? Has this been integrated into any disaster risk reduction actions? (e.g., reasonable worst-case scenarios)
Integrated water resources management	42)	To what extent are strategies or actions in place at the national and subnational levels to improve integrated water resources management in areas prone to floods, droughts, or storm surges, taking into account the potential impact of climate change?
Strategic food supply	43)	To what extent does the country have strategies or actions in place to ensure food security during crises? (e.g., stockpiling, contingency arrangements, or controlling the food market)

Water conservation	44) To what extent does the country have strategies or actions in place for water conservation in situations of reduced rainfall and extreme heat at the national and subnational levels?
Networked failures affecting food and water supply systems	45) To what extent have the cascading effects of disruptions in other critical infrastructure services on food and water supply been assessed and understood? (e.g., power failures affecting water and food supply)
Cultural heritage	
Ranking of Icon sites and cultural heritage	46) To what extent have iconic sites and cultural heritage been listed and ranked at the national and subnational levels?
Role of icon sites and heritage for economics	47) To what extent has the country been able to estimate the direct and indirect economic losses associated with damage or destruction of cultural heritage due to disasters?
Risk reduction of cultural heritage	48) To what extent has the country assessed the resources required to enhance the safety of cultural heritage and iconic sites located in areas vulnerable to natural and technological hazards?
Disruption of cultural heritage	49) To what extent has the country assessed and identified the potential escalating needs resulting from damage to cultural heritage and iconic sites in 'worst-case scenarios'? Additionally, how have the implications for resources and recovery capabilities been evaluated?
Interacting and concurrent impacts on CI	50) To what extent have the impacts of concurrent events and interacting hazards on cultural heritage and iconic sites been assessed and used to develop mitigation actions?
Information	
Cyber infrastructure	
Redundancies	51) To what extent has the redundancy of physical components in cyber infrastructure been assessed at the national and subnational levels?
Cyber security	52) To what extent is cyber security integrated into everyday risk management practices and organisational resilience?
Privacy and data breaches	53) To what extent have the implications of privacy and data losses been specifically addressed in national risk assessments?
Protection of cyber infrastructure	54) To what extent has a consistent strategy for the protection of cyber infrastructure been implemented at the national and subnational levels?
External dependencies (e.g., internet providers, electricity, water) and internal system dependencies (e.g., intercom	55) To what extent have internal and external system dependencies been identified and prioritised?

LANs, secure communication procedures).	
Relationship between cyber and satellite infrastructure.	56) To what extent have the dependencies and interdependencies between cyber and satellite infrastructure been examined to assess the implications of targeted attacks on one or both systems?
Contact points	57) To what extent have entities (e.g., multinational organisations) that may influence or be affected by cyber-attacks on national cyber infrastructure been assessed? Have contact points been identified?
Protocols and procedures	
Skills and experience	58) To what extent do national and subnational governments have access to the skills and experience necessary to reduce risks and respond to disaster scenarios identified in the risk register?
Languages	59) To what extent have key (non-strategic) protocols and procedures been made available in all the languages most commonly spoken in the country?
Threat and hazard horizon scanning	60) To what extent are new and emerging threats and hazards considered when implementing disaster risk reduction actions? Are there procedures in place to effectively translate these considerations into practice?
Strengthening early warning platforms	61) To what extent have improvements to early warning systems and communication platforms been identified, and have associated procedures been adopted to support their implementation at national and subnational levels?
Role of stakeholders	62) To what extent have efforts been made to map all relevant stakeholders for disaster risk reduction at the national and subnational levels? Does this include an assessment of whether stakeholders' roles are clearly defined and understood by them?
Low tech intensive procedures	63) To what extent have low-technology-intensive procedures been identified and developed at the national and subnational levels to address extended technological failures? (e.g., paper-based procedures following cyber-attacks)
Resilience of emergency services and institutions	64) To what extent have the cascading effects of multiple technological failures on emergency services and government institutions been understood and analysed, including their implications for organisational resilience? (e.g., blackouts, ICT failures, and concurrency with hybrid threats)
Procurement	65) To what extent have the resources required to address service disruptions caused by technological failures been assessed and prioritised at the national and subnational

		levels? (e.g., resources needed for blackouts and ICT failures)
Operational continuity		
Business continuity management - government	66)	To what extent does the government have business continuity plans in place to ensure the continued provision of critical public services following a disaster?
Business continuity - private sector	67)	What proportion of businesses have a documented business continuity plan that has been reviewed within the past 18 months?
Planning	68)	Does the current contingency planning approach at the national and subnational levels incorporate disaster risk reduction strategies aligned with the Sendai Framework?
Ensuring continuity of capacities	69)	To what extent are plans in place to ensure the continuity of risk management capacities at the national and subnational levels? Do these plans include commitments to long-term resource allocation and mechanisms to enable synergies across different knowledge and policy sectors?
Shared understanding of infrastructure risk	70)	Is there a shared understanding of risks between national and subnational authorities, utility providers, and other agencies responsible for managing infrastructure—such as power, water, and transport—regarding system stress points and risks at national and subnational scales?
Operational continuity of personnel	71)	To what extent have targeted procedures been implemented to address technological failures (e.g., loss of telecommunications or transport) and maintain the operational capacity of key personnel in national and subnational organisations? (e.g., designated meeting points and duty stations)
Critical technological nodes	72)	To what extent have technological systems or assets that could cause cascading effects across multiple users or departments if disrupted (e.g., servers) been identified?
Availability of backup systems	73)	To what extent are emergency backup systems, including generators, available, maintained, tested, and operational in key governmental buildings at the national and subnational levels?
Heating and cooling	74)	To what extent are the cooling and heating systems in critical national and subnational buildings regularly updated and maintained? Do their capacities align with the latest projections of climate extremes?
Datasets		
Data recording and collection	75)	How effectively does the government collect, calculate, and store disaster loss data in a national context, including information on

	mortality, affected populations and areas, and economic losses?
Data sharing	76) To what extent is data on DRR capacity shared between organizations involved with national resilience?
Hazard assessment	77) To what extent are national and subnational governments aware of the key hazards faced by cities and their likelihood of occurrence?
Identifying disaster risk reduction and climate change adaptation overlaps	78) To what extent have areas of overlap between Disaster Risk Reduction and Climate Change Adaptation activities been identified to optimise the use of funds and resources more efficiently in either domain at the national and subnational levels?
Analysis tools	79) To what extent are tools and models available to analyse complex risks, interdependencies, and cascading impacts? (e.g., indirect loss of life caused by cascading effects of power failures combined with cold waves)
Hazards and critical infrastructure mapping	80) To what extent have hazard risk mapping and infrastructure criticality mapping been updated and integrated at the national and subnational levels?
Data on interferences and complex dynamics	81) To what extent are data on critical infrastructure interdependencies and the complex risks arising from them collected and maintained in datasets?
Interacting hazards assessments	82) To what extent do national and subnational governments have knowledge of natural hazards that could result from the interacting geophysical characteristics of specific areas?
Concurrency assessments	83) To what extent do national and subnational governments have knowledge of natural hazards that are more likely to occur concurrently?
Communication and knowledge sharing	
Co-operation with media partners	84) To what extent has the country collaborated with traditional and new media corporations on emergency and risk awareness communication to establish a unified effort, making public information dissemination a key priority? (e.g., fostering a culture of collaboration)
Bridging knowledge between science and policy	85) To what extent has the country developed strategies or plans to employ or enable individuals to act as intermediaries between science and policy on disaster risk reduction and climate change adaptation? To what extent have scientific institutions and teams capable of generating valuable knowledge been identified at the national and subnational levels?
Facilitate communication and knowledge sharing between different levels.	86) To what extent have efforts been made to establish credible and relevant knowledge-sharing platforms, networks, and events

		across government entities and sectors, as well as between national, regional, and municipal/local levels?
Multi-media platforms for risk awareness	87)	To what extent have efforts been made to establish credible and relevant knowledge-sharing platforms, networks, and events across government entities and sectors, as well as between national, regional, and municipal or local levels?
Countering misinformation and disinformation.	88)	To what extent have strategies been developed at the national and subnational levels to counter the spread of false information during ongoing emergencies, disasters, or crises?
Public communications	89)	To what extent do current practices ensure effective communication with the public during responses to technological failures, such as internet and telecommunication breakdowns, at the national and subnational levels? (e.g., blackouts, cyberattacks, extreme space weather events)
Delivering training	90)	Are training courses on risk and resilience issues available to all sectors, including government, businesses, NGOs, and communities?
Training for complex risks	91)	To what extent is training used to enhance disaster preparedness for complex risks at the national and subnational levels?
Language	92)	Are training materials available in the majority of languages commonly used at the national and subnational levels?
Lessons learnt	93)	To what extent are corrective actions and lessons learned from exercises or disruptive events integrated into future practices?
Practicing roles	94)	To what extent is it ensured that emergency response and risk management professionals participate in training and crisis scenario simulations, including real-time exercises, gaming, and other relevant formats?
Exercises	95)	To what extent are exercises conducted to enhance disaster preparedness for complex risks at the national level?
Hybrid emergency	96)	To what extent have scenarios involving fake information and cyber-attacks during ongoing emergencies been tested through exercises at the national and subnational levels?
MORDOR scenario	97)	To what extent have scenarios involving reduced operational capacity of emergency services due to cascading effects and concurrent events been tested and exercised?
Learning from others	98)	Is the national government proactively engaging in knowledge exchange and learning from other national governments facing similar challenges?

Organisational culture	99) Is the organisational culture at national and subnational levels open enough to allow risks identified at lower levels to be escalated appropriately and for top management to share risk information with stakeholders and the public?
Cyber culture	100) To what extent has a cyber-aware culture been established, promoting cyber safety through education on individual and collective behaviours?
Technology driven behaviours in households	101) To what extent have household behaviours been investigated to understand how technology influences disaster risk reduction practices? For example, do households still possess AM/FM radios, and can these be considered reliable tools for disaster risk and response information dissemination?
Technology driven behaviours by individuals	102) To what extent have individual behaviours been investigated to understand how technology influences disaster risk reduction requirements at the national and subnational levels? For example, is the prevalence of cashless payments considered, and how might this be impacted by blackouts or ICT failures?
Social	
Legal & Regulatory	
Regulation	103) To what extent does the country have regulatory frameworks in place to reduce existing risks, prevent the creation of new risks, manage risk identification, reduction, and mitigation, and strengthen economic and social resilience? Are these frameworks regularly reviewed and updated?
Application of zoning, building codes and standards	104) Are zoning rules, building codes and standards widely applied, properly enforced and verified?
Risk assessment	105) To what extent are risks identified, assessed, and analysed within national and subnational contexts?
Coordination	106) To what extent does the country utilise formal mechanisms to coordinate disaster risk reduction activities across all sectors and areas of activity?
Warnings and evacuation	107) To what extent does legislation facilitate the dissemination of warning messages (e.g., by meteorological services and health authorities) and authorise precautionary evacuations?
Planning	108) To what extent do national strategies and plans incorporate disaster risk reduction approaches aligned with the Sendai Framework? To what extent do these strategies address cascading, concurrent, interacting, and hybrid risks?

Regulation of lifelines	109) Is there a legal framework in place to secure emergency lifelines, such as energy, food, and communication, during national emergencies?
Intermodality	110) To what extent does the country have regulatory frameworks in place to facilitate the coordination of intermodal transportation for managing risks or responding to large-scale disruptions at the national and subnational levels? To what extent do these frameworks include agreements with neighbouring countries for cross-border crises? (e.g., volcanic ash clouds)
Compliance with standards	111) To what extent do providers of essential assets or services, such as banks, adhere to security and organisational resilience standards as part of their routine operations?
Political, humanitarian and diplomatic	
Political mandate	112) To what extent is disaster risk reduction at the national level enabled by a political mandate?
Accountability	113) To what extent are measures in place to incentivise and ensure the accountability of leadership and government bodies in actively engaging in disaster risk reduction?
Mainstreaming	114) How thoroughly have policies and strategic initiatives for disaster risk reduction been reviewed? To what extent do these efforts strengthen capacities at national and subnational levels while aligning with the region's specific hazard and risk profiles?
Assessing and balancing capacities	115) To what extent has a comparison of capacities across national and subnational government bodies been conducted to assess whether they are balanced and free from gaps, ensuring coordinated efforts in addressing disaster risks?
Knowledge transfer	116) To what extent is the country engaged in the transfer and exchange of knowledge, science, technology, and innovation in disaster risk reduction, involving both national and subnational levels?
Building partnerships for transboundary crisis management	117) To what extent has the country established agreements with neighbouring governments for transboundary crisis management, including the clarification of mandates? How far has this process been supported by the development of joint exercises with relevant counterparts in these countries?
Aligning capacities with the latest risk assessments	118) To what extent are policies and strategies for improving disaster risk reduction capacities aligned with the latest risk assessments, including regionally downscaled climate model projections from international bodies like the IPCC?

Policies on cascading risk	119) To what extent are cascading risks and interconnected failures integrated into strategies and policies for enhancing disaster risk reduction capabilities?
Intelligence for transboundary crisis management	120) Is there timely exchange of intelligence with allied governments on how fake information, public disorder, and cyber-attacks could be leveraged to escalate threats and ongoing crises?
Institutional (including admin and defence)	
Budget for disaster risk reduction	121) To what extent has financial support been provided to establish and update work on risk assessment and disaster risk reduction?
Human resources	122) To what extent are human resources available to address disaster risk reduction needs at the national and subnational levels?
Aligning and streamlining priorities	123) To what extent has the country taken steps to ensure that government entities at both national and subnational levels have aligned their strategies, using consistent terminology and a shared understanding of concepts? For example, terms like risk and vulnerability, and risk assessment methods that can be applied across different hazard types.
Clarifying mandates for coordination	124) To what extent has the country identified institutional barriers and taken steps to clarify or revisit the mandates of different stakeholders involved in emergency response and risk reduction activities at the national and subnational levels?
Setting up coordination forums	125) To what extent has the country established forums to coordinate activities between the bodies responsible for risk reduction and emergency response, as well as between governmental and non-state actors, such as NGOs and the general public?
Procurement	126) To what extent have the resources required to manage service disruptions during technological failures been assessed and prioritised at the national and subnational levels? (e.g., resources needed for blackouts and ICT failures)
Payment backups	127) To what extent does the country have administrative arrangements in place to ensure the payment of salaries, pensions, and subsidies in the event of disruptions to government payments and other transactions, and their cascading effects on society?
Innovation in addressing complex risks	128) To what extent does the national research agenda for innovation and technology development prioritise the assessment and understanding of complex risks, including interdependencies and cascading dynamics? To what extent does this consider the needs

	and involvement of the private sector, such as service providers?
Economic & Financial	
Incentives	129) What financial incentives are available for different sectors of business and society to support resilience building, risk-aware recovery, and the reconstruction of businesses and households? (e.g., relocation, retrofitting)
Making the value of disaster risk reduction investments visible	130) To what extent have national and subnational efforts been made to estimate and demonstrate the economic and social benefits of long- and medium-term disaster risk reduction and climate change adaptation measures to elected officials and communities? To what extent are standardized procedures or guidelines in place for this?
Financial plan and budget for resilience, including contingency funds	131) To what extent does the national government have a designated protected budget and contingency fund arrangements in place for local disaster risk reduction?
Insurance	132) What level of disaster insurance coverage is available nationwide for businesses and communities?
Innovating existing disaster risk financing structures	133) To what extent have current disaster risk financing schemes been assessed and reviewed with the aim of innovating the process and making risk financing more transparent?
Financial plan and budget for cascading events	134) To what extent does the national government have a designated protected budget and contingency fund arrangements in place to address rapidly escalating cascading events caused by cross-sectoral infrastructure failures?
Contingency plans and thresholds for financial disruptions	135) To what extent has the country developed risk assessments, exercises, and contingency plans for the cascading effects of financial disruption in the private sector? Are timelines and criticality thresholds available for small, medium, and large enterprises?
Education	
Public education and awareness	136) Does a coordinated public relations and education campaign exist, with structured messaging and communication channels to ensure hazard, risk, and disaster information is effectively disseminated and understood by the public?
Innovative disaster risk awareness campaigns	137) To what extent has the country fostered the development of risk (and response) memories to support preparedness and risk awareness campaigns and strategies at the national and subnational levels?

Risk knowledge	138) To what extent has a national strategy been developed to raise societal awareness of the most likely risks and hazards the country may face, and the key measures required to reduce disaster risk at the national and subnational levels?
Education on interacting risks	139) To what extent has a national strategy been developed to raise societal awareness of the most likely interacting risks the country may face, and the necessary risk reduction measures? (e.g., heatwaves interacting with flooding)
Education on compound events	140) To what extent has a national strategy been developed to raise societal awareness of the most likely concurrent natural risks the country may face, and the necessary risk reduction measures? (e.g., storms during a cold wave)
Education on technology failures	141) To what extent has a strategy been developed to raise public awareness about technological failures, providing guidance on how to react during such events? (e.g., blackouts or telecom failures)
Education on disinformation and misinformation	142) To what extent has an educational strategy been developed to raise public awareness about the potential spread of false information during ongoing emergencies? To what extent does this strategy include guidance on relying only on trusted and reliable sources?
Public/private risk ownership	
Organisation, coordination and participation	143) Is there a multi-agency and multi-sectoral mechanism, with adequate authority and resources, to address disaster risk reduction?
Integration	144) Is disaster risk reduction and resilience planning effectively integrated with other key functions and portfolios? (e.g., sustainability, investment approvals, finance and compliance, community engagement, emergency management, code compliance, infrastructure management, and communications)
Industry participation	145) To what extent are private sector and industry actors engaging in disaster risk reduction as a corporate priority and a component of social responsibility?
Legal requirements	146) To what extent are utility providers and other businesses delivering public services legally required to manage disaster risks and report to the government?
Provision of incentives for sharing	147) To what extent has the country promoted the value of data and knowledge sharing among public and private actors, for example, through workshops, conferences, or by showcasing successful knowledge-sharing

	practices related to disaster risk reduction and climate change adaptation?
Social cohesion and livelihoods	
Community or “grassroots” organisations	148) To what extent are grassroots or community organisations participating in pre-event planning and post-event response? E.g. through civil protection bodies
Bottom-up evaluations	149) To what extent has the country put in place mechanisms that ensure evaluations are completed after crises, emergencies and disasters (i.e. to identify lessons)? To what extent are all relevant actors involved and expected to adopt the resulting recommendations?
Citizen engagement techniques	150) How effective are city authorities at citizen engagement and communications in relation to disaster risk reduction?
Utilising local stakeholder knowledge for disaster risk reduction actions	151) To what extent are efforts made at the national/subnational to establish mechanisms that ensure that the voices of minority groups are heard by policy and decision makers in regard to disaster risk reduction?
Involvement in multi-hazard early warnings	152) To what extent have community and grassroots organisations been involved in the development/evolution of multi-hazards warnings/early warning systems? Has local knowledge been considered in scenarios of interacting and concurrent threats at the national/subnational levels?

4.1.4. The Use of War Gaming Strategies and Their Similarity to Existing Emergency Practices

Lin-Greenberg et al. (2022) define a wargame as an interactive event characterised by human players, scenario immersion, rules-based interaction, and consequence-based outcomes. They emphasise human decision-making processes in the context of real-world decision-making environments. They follow rules that can be rigid or allow free play, which ensure that players face outcomes based on their decisions. Wargames can range from tabletop exercises to larger-scale simulations involving multiple teams and moves. Their primary value lies in understanding how and why decisions are made rather than predicting specific outcomes. Both wargames and emergency exercises use scenario-driven simulations to prepare participants for complex, high-stakes situations. By modelling hypothetical crises - such as natural hazard events, cyberattacks, or military conflicts - these simulations help explore potential responses, outcomes, and stress-test existing systems. Linkov et al. (2022) note that current approaches typically emphasise risk-based stress testing, which can be of limited value because it focuses mainly on identifying which parts of a system fail under different stress loads. Instead, they propose adding a systems-thinking perspective that accounts for the interconnections across various domains to gauge how disruptions affect a system’s ability to recover and adapt—its resilience. They further recommend a tiered approach that combines risk and resilience stress testing for complex, interconnected systems, as used in AGILE.

4.2. Scenario Elements and Structure

4.2.1. Triggering Event (Threat)

As outlined above, the scenario will consist of two hazard cards, one wild card, and one infrastructure card that determines which system will be affected by unexpected cascading effects. The hazard cards and infrastructure cards are listed here. The wild cards are discussed below under 3.2.2 “Set of Possible Circumstances”.

Hazard cards

The card deck contains the following 56 hazard cards:

Geophysical

1. Earthquake – Ground shaking and structural damage.
2. Mass Movement – Landslides, avalanches, and rockfalls causing disruption.
3. Tsunami – Coastal flooding and infrastructure damage due to seismic waves.
4. Volcanic Activity – Eruptions, ash clouds, and lava flows affecting populations and infrastructure.

Hydrological

5. Flood – Inundation of areas due to heavy rainfall, river overflow, or dam failure.
6. Landslide – Earth movement causing property damage and access blockages.
7. Wave Action – Coastal erosion, high tides, and storm surges impacting settlements.

Meteorological

8. Convective Storm – Thunderstorms, hail, and lightning strikes causing disruptions.
9. Extratropical Storm – Intense low-pressure systems with heavy rain and winds.
10. Extreme Temperature – Heatwaves or cold spells impacting health and infrastructure.
11. Fog – Reduced visibility affecting transport and aerial operations.
12. Environment-Driven Pollution – Air and water contamination due to natural conditions.
13. Ice Storm – Freezing rain causing damage to infrastructure and utilities.
14. Wind and Gales – Strong winds causing structural damage and disruptions.
15. Tropical Cyclone – Hurricanes and typhoons bringing high winds and flooding.
16. Glacial Lake Outburst – Sudden release of water from glacier-dammed lakes causing downstream flooding.
17. Wildfire – Uncontrolled fires affecting forests, settlements, and air quality.
18. Permafrost Melting – Ground instability and infrastructure damage due to thawing.
19. Atmospheric or Oceanic System Change – Long-term shifts impacting weather patterns and ecosystems.

Extra-terrestrial

20. Space Weather – Solar flares and geomagnetic storms affecting satellites and communication.
21. Impact by Space Debris – Collisions causing damage to satellites and infrastructure.
22. External Agents (e.g., bacteria) – Biological contamination from extra-terrestrial sources.

Biological

23. Human Disease/Epidemic – Outbreaks affecting public health and healthcare systems.
24. Insect and Pest Infestation – Agricultural damage and public health concerns.
25. Animal Incident – Wildlife attacks or animal intrusions disrupting operations.
26. Plant Disease/Epidemic – Crop failures and food supply chain impacts.
27. Animal Disease/Epidemic – Livestock infections affecting food supply and economies.

Technological

28. Nuclear Accident/Incident – Radiation leaks and contamination risks.
29. Industrial Accident/Incident – Chemical spills, explosions, or factory malfunctions.
30. Infrastructure Accident/Incident – Failures in transport, utilities, or essential services.
31. Technological Accident/Incident – Failures in automated systems or robotics.
32. Cyber Failure – IT outages, data breaches, or cyber-attacks.
33. Chemical, Nuclear, or Biological Pollution – Contamination affecting ecosystems and populations.

Financial & Economic

34. Financial Shocks – Sudden disruptions in markets or banking systems.
35. Trade Disputes – Economic conflicts impacting supply chains and exports.
36. Economic Recession – Periods of economic decline affecting livelihoods.
37. Positive Shocks – Unexpected growth or economic booms creating imbalances.

Political & Social

38. Geopolitical Conflict – Wars or disputes disrupting regions and economies.
39. Political Violence – Acts of terrorism or violent protests.
40. Malicious Attack – Targeted acts of sabotage affecting critical infrastructure.
41. Organised Crime – Illegal activities impacting safety and governance.
42. Political Instability – Governmental uncertainty impacting decision-making.
43. Animal-Human Conflict – Incidents caused by interactions between wildlife and humans.
44. Operational Failure – Management breakdowns in key sectors or services.
45. Social Unrest – Protests or riots causing instability and damage.
46. Humanitarian Crisis – Emergencies requiring large-scale aid and response.
47. Famine – Food shortages leading to malnutrition and migration.
48. Water Scarcity – Limited access to clean water supplies.
49. Refugee Crises – Large-scale displacement requiring support and services.
50. Welfare System Failure – Breakdowns in social safety nets impacting vulnerable groups.

Known Unknowns

51. Artificial Intelligence – Failures or ethical concerns in AI-driven systems.
52. Space Exploration – Accidents or malfunctions during extra-terrestrial missions.
53. Broken Arrows – Incidents involving lost or unaccounted nuclear weapons.
54. Forgotten Weapons – Discovery of unexploded ordnance posing threats.
55. Other – Unspecified or emerging threats not covered above.

Unknown

56. Unclassified Events – Unpredictable or unprecedented occurrences requiring evaluation.

Infrastructure cards

Including very unlikely infrastructures in the scenario is useful because HILPs can have unexpected cascading effects that extend well beyond the initially impacted systems. Historical events such as the 2002 floods in Prague illustrate this point: massive rainfall across Central Europe led not just to widespread flooding, but also to damage to cultural heritage sites, chemical spills from industrial facilities, and significant disruptions to power plants and water treatment systems. Even public health issues emerged, such as the outbreak of hepatitis, highlighting how seemingly unrelated sectors can become intricately connected during a disaster. By exploring unlikely or seemingly tangential infrastructure failures within a HILP scenario, participants gain a more holistic understanding of how interconnected their systems truly are and can better prepare for a range of potential threats.

The card deck contains the following 91 infrastructure cards:

Energy sector

Electricity subsector

1. Failure of supply of electricity (electricity undertakings).
2. Failure of operation, maintenance and development of an electricity distribution system (distribution system operators).
3. Failure of operation, maintenance and development of an electricity transmission system (transmission system operators).
4. Failure of generation of electricity (producers).
5. Failure of nominated electricity market operator service (nominated electricity market operators).
6. Failure of demand response (electricity market participants).
7. Failure of aggregation of electricity (electricity market participants).
8. Failure of energy storage (electricity market participants).

9. Failure of district heating and cooling subsector: provision of district heating or district cooling (operators of district heating or district cooling).

Oil subsector

10. Failure of oil transmission (operators of oil transmission pipelines).
11. Failure of production of oil (operators of oil production).
12. Failure of refinement and treatment of oil (operators of oil refining and treatment facilities).
13. Failure of oil storage (operators of oil storage).
14. Failure of management of oil stocks, including emergency stocks and specific oil stocks (central stockholding entities).

Gas subsector

15. Failure of supply of gas (supply undertaking).
16. Failure of distribution of gas (distribution system operators).
17. Failure of transmission of gas (transmission system operators).
18. Failure of storage of gas (storage system operators).
19. Failure of operation of a liquefied natural gas (LNG) system (LNG system operators).
20. Failure of production of natural gas (natural gas undertakings).
21. Failure of purchase of natural gas (natural gas undertakings).
22. Failure of refinement and treatment of natural gas (operators of natural gas refining and treatment facilities).

Renewable energy subsector

23. Failure of operation and maintenance of solar farms (solar energy operators).
24. Failure of operation and maintenance of wind farms (wind energy operators).
25. Failure of operation and maintenance of hydroelectric facilities (hydroelectric operators).
26. Failure of large-scale battery energy storage systems (BESS operators).
27. Failure of operation and maintenance of EV charging stations (EV charging network providers).

Hydrogen subsector

28. Failure of the production of hydrogen (operators of hydrogen production).
29. Failure of storage of hydrogen (operators of hydrogen storage).
30. Failure of transmission of hydrogen (operators of hydrogen transmission).

Transport sector

Air subsector

31. Failure of air transport services used for commercial purposes (passenger and cargo) (air carriers).
32. Failure of operation, management and maintenance of airports and of airport network infrastructure (airport managing bodies).
33. Failure of air traffic control services (traffic management control operators).

Rail subsector

34. Failure of railway transport services (passenger and freight) (railway undertakings).
35. Failure of operation, management and maintenance of railway infrastructure, including passenger stations, freight.
36. Failure of terminals, railway yards and traffic control centres (infrastructure managers).
37. Failure of operation, management and maintenance of railway service facilities (operators of service facilities).
38. Failure of operation, management and maintenance of rail traffic management, control-command and signalling as well as telecommunication installations and systems used for control-command and signalling (infrastructure managers).

Water subsector

39. Failure of inland, sea and coastal water transport services (passenger and freight) (inland, sea and coastal passenger and failure of freight water transport companies).
40. Failure of operation, management and maintenance of port and port facilities, and operation of works and equipment within ports, including bunkering, cargo-handling, mooring, passenger services, collection of ship-generated waste and cargo residues, pilotage and towage (managing bodies of ports and entities operating works and equipment contained within ports).

41. Failure of vessel traffic services (operators of vessel traffic services).

Road subsector

42. Failure of traffic management control, including aspects related to road network planning, control and management services, excluding traffic management or the operation of intelligent transport systems where they are not an essential part of the general activity of public entities (road authorities).
43. Failure of Intelligent Transport Systems services (operators of Intelligent Transport Systems).

Public transport subsector:

44. Failure of public passenger transport services by rail and other track-based modes and by road (public service operators).

Transport sector, miscellaneous

45. Failure in operations of shared e-scooters and bike-sharing systems (micro-mobility service providers).
46. Failure at last-mile delivery operators for essential goods (logistics providers).
47. Failure at bridge and tunnel operators (infrastructure maintenance entities).
48. Failure at customs and port authority coordination centres.
49. Failure in emergency fuel supply systems: rapid response fuel supply for emergency vehicles (fuel logistics operators).

Banking sector

50. Failure in taking deposits (credit institutions).
51. Failure in lending (credit institutions).
52. Failure of financial market infrastructure sector:
53. Failure of operation of a trading venue (operators of trading venues).
54. Failure of operation of clearing systems (central counterparties).

Health sector

55. Failure in provision of healthcare services (healthcare providers).
56. Failure of research and development of medicinal products (entities carrying out research and development activities of medicinal products).
57. Failure in manufacturing of basic pharmaceutical products and of basic pharmaceutical preparations (entities manufacturing basic pharmaceutical products and pharmaceutical preparations).
58. Failure in manufacturing of medical devices considered as critical during a public health emergency (entities manufacturing medical devices).
59. Failure in distribution of medicinal products (entities holding a distribution authorisation).
60. Failure in provision of psychological first aid and crisis counselling (mental health support providers).
61. Failure in coordination and supply of blood products and organ transplantation (blood banks and organ procurement organisations)
62. Failure in telemedicine and remote health services: digital platforms providing remote medical consultations.

Drinking water sector

63. Failure in drinking water supply and drinking water distribution excluding distribution of water for human consumption where that service is a non-essential part of the general activity of distributors distributing other commodities and goods (suppliers and distributors of water intended for human consumption).
64. Failure at operators of desalination plants in water-scarce regions.

Wastewater sector

65. Failure in wastewater collection, treatment and disposal excluding collecting, disposing of or treating urban wastewater, domestic wastewater or industrial wastewater where they are not an essential part of the general activities of undertakings (undertakings collecting,

disposing of or treating urban wastewater, domestic wastewater and industrial wastewater).

Water, miscellaneous

66. Failure at operators of stormwater drainage systems and flood barriers.

Digital infrastructure sector

67. Failure in provision and operation of internet exchange point service (providers of internet Exchange Points).
68. Failure in provision of domain name system (DNS) service excluding services related to root name servers (DNS service providers).
69. Failure in operation and administration of top-level domain (TLD) name registries (TLD name registries).
70. Failure in provision of cloud computing services (providers of cloud computing services).
71. Failure in provision of data centre service (providers of data centre services).
72. Failure in provision of content delivery networks (providers of content delivery networks).
73. Failure in provision of trust services (trust service providers).
74. Failure in provision of publicly available electronic communications services (providers of electronic communications services).
75. Failure in provision of public electronic communications networks (providers of public electronic communications networks).
76. Failure at security operations centres (SOCs) and Computer Security Incident Response Teams (CSIRTs).
77. Failure at operation of blockchain-based financial or logistical systems.

Public administration sector

78. Failure in services provided by public administration entities of central governments
79. Failure at local emergency coordination centres: Regional/local entities coordinating disaster response.
80. Failure at critical census and population data management: Organisations managing census data critical for resource allocation.

Space sector

81. Failure in operation of ground-based infrastructure that supports the provision of space-based services, excluding providers of public electronic communication networks (operators of ground-based infrastructure).
82. Failure of satellite navigation services: Operators of GNSS (Global Navigation Satellite Systems) infrastructure.
83. Failure in space debris monitoring: organisations monitoring and mitigating risks of orbital debris.

Food sector

The production, processing and distribution of food sector (food businesses which are engaged exclusively in logistics and wholesale distribution and large-scale industrial production and processing)

84. Failure in large-scale industrial food production and processing.
85. Failure in food supply chain services, including storage and logistics.
86. Failure in food wholesale distribution.
87. Failure of agricultural irrigation systems: operators of irrigation networks for large-scale farming.
88. Failure in cold chain logistics: services maintaining the cold chain for perishable food and medical supplies.

Miscellaneous

89. Failure in animal health and veterinary services: veterinary care for livestock critical to food security.

90. Failure in critical waste management services: hazardous waste management during emergencies (hazardous waste operators).
91. Failure in private security services: operators of private security for critical infrastructure sites.

4.2.2. Set of Possible Circumstances

In addition to the two hazard cards and the infrastructure card, the deck also includes a wild card. This card either provides general context (26 cards), a vulnerability (20 cards), or an additional hazard (23 cards). The general context cards increase the complexity of the scenario, the vulnerability cards increase it further, and the additional hazard cards maximise its complexity.

Adjusting the difficulty level:

- It is advisable for participants with limited capacity in disaster management exclude cards 27-69.
- It is advisable for participants with intermediate capacity in disaster management to exclude cards 54-69.

General context cards

1. **National or Religious Celebration** – High population density and potential disruptions.
2. **Mass Event Ongoing** (e.g., football finals) – Increased crowds and demand for services.
3. **Work Peak (Monday)** – High traffic and operational demands.
4. **Holiday Peak (Sunday)** – Increased leisure activities and reduced service availability.
6. **Pay Day** – Elevated banking activity and consumer movements.
7. **Peak Hour** – High traffic congestion and resource demand.
8. **Middle of the Night** – Reduced visibility and slower emergency responses.
9. **Summer Midday** – Heat-related health risks and energy demand spikes.
10. **UFO Sightings** – Distractions or hoaxes impacting emergency focus.
11. **Royal Announcement** – Media focus and crowd management challenges.
12. **Celebrity Marriage or Divorce** – Increased public and media attention.
13. **Billionaire Trapped in a Shipwreck** – High-profile rescue demands.
14. **Tourist Vandalising Iconic Site** – Public outrage and reputation damage.
15. **Anomaly in Animal Behaviour** – Early warning signs or disruptions.
16. **Eurovision Event** – Mass gatherings and increased security needs.
17. **Speleologist Trapped in a Cave** – Rescue challenges in remote locations.
18. **Disappearance of Coffee and Tea** – Supply chain disruptions and public reaction.
19. **Election Day** – High public attention, potential protests, and political tensions.
20. **School Holidays** – Increased travel and reduced local service availability.
21. **Local Market Day** – Crowded urban and rural areas.
22. **Seasonal Migration** – Temporary population influx or exodus.
23. **Mass Pilgrimage** – High population density in specific regions.
24. **Cultural Festival with Fireworks** – Noise pollution and potential fire hazards.
25. **VIP Visit** – Security and crowd control requirements.
26. **Unidentified green lights in the sky** - Rampant speculation and viral conspiracy theories.

Vulnerability cards

27. **Language Barriers** – Challenges in communication with non-native speakers.
28. **System Updates** – Temporary outages or reduced IT service reliability.
29. **Infrastructure Upgrades: Ground Transport** – Traffic delays and diversions.
30. **Infrastructure Upgrades: Harbours** – Reduced cargo handling capacity.
31. **Infrastructure Upgrades: Dams and Barriers** – Flood management vulnerabilities.
32. **Infrastructure Upgrades: ICT Systems** – Risk of communication breakdowns.
33. **Electricity Grid Maintenance** – Reduced redundancy and local outages.
34. **Water System Testing** – Limited access to clean water in specific areas.

35. **Critical Software Vulnerabilities** – IT system shutdowns and security threats.
36. **Key Resource Misallocation** – Supply chain errors and delays.
37. **Logistics Vehicle Breakdown** – Delays in transporting critical supplies.
38. **Overloaded Waste Facility** – Blocked routes and fire hazards due to uncollected waste.
39. **Seismic Sensor Malfunctions During Construction** – False warnings and responder confusion.
40. **Delayed Reservoir Discharge Warning** – Communication delays causing non-catastrophic flooding.
41. **Supply Chain Contamination Alert** – Suspected contamination causing delays in distributing emergency supplies.
42. **Unannounced Drills** – Confusion between simulated and real emergencies.
43. **Unscheduled Fireworks Testing** – Noise, light pollution, and disruptions during emergency responses.
44. **Shift Change in Emergency Services** – Reduced immediate response capacity.
45. **Test (Exercise) Day** – Potential public confusion between drills and real emergencies.
46. **Foggy Conditions** – Visibility issues affecting transport and aerial operations.

Additional hazard cards ("easy")

47. **Feral Animal Intrusion** – Urban disruptions caused by stray animals.
48. **Autonomous Vehicle Malfunctions** – Traffic disruptions and accidents.
49. **Squirrel Attacks on Power Grid** – Localised power outages and repair delays.
50. **Unexpected Pollen Surge** – Mild respiratory issues and visibility challenges.
51. **Drone Interference with Powerlines** – Disruptions to electricity transmission.
52. **Algal Blooms** – Water contamination and ecological impacts.
53. **Wildlife Migration** – Road blockages and emergency operation interference.

Additional hazards cards (intermediate - hard)

54. **Cold Weather** – Increased heating demand and infrastructure vulnerabilities.
55. **Heatwave** – Elevated risk of dehydration, fires, and infrastructure strain.
56. **Rare Winds or Hailstorms** – Physical damage and transport disruptions.
57. **Fake Information** – Spread of false narratives leading to public panic.
58. **Rumours** – Misinformation affecting public perception and response.
59. **Industrial Strikes** – Limited manpower in critical sectors.
60. **Telecommunication Overload** – Network congestion and communication failures.
61. **Unusual Tidal Conditions** – Disruptions to coastal transport and activities.
62. **Bird Migration Delays Drone Operations** – Emergency drone interference caused by large flocks.
63. **Public Protests** – Infrastructure blockages and communication disruptions.
64. **Cyber Attacks on Harbour Cranes** – Operational delays and cargo mishandling.
65. **Jellyfish Blocking Nuclear Plant Cooling Systems** – Temporary shutdowns at coastal facilities.
66. **Annual Crop Production Decline** – Food shortages and supply chain strains.
67. **Data Leak** – Loss of sensitive information and public trust.
68. **Panic Buying** – Shortages of fuel, food, and essential supplies.
69. **Cats Taking Over** – Unusual and unpredictable incidents involving animals.

4.3. Examples of Hypothetical Scenarios

Using a specific scenario with defined hazards, contexts, and affected infrastructure does not contradict a risk-agnostic approach to disaster management because it provides a tangible narrative that makes it easier for people to grasp potential vulnerabilities and interconnections. By grounding the discussion in a concrete example, participants can more readily recognise systemic risks and identify common points of failure, rather than struggling with abstract concepts of risk. This scenario-based approach illuminates how seemingly disparate hazards, contexts, and infrastructures can be intertwined, highlighting systemic vulnerabilities and critical functions that could be impacted by a variety of threats. Ultimately, examining these specific elements helps

uncover insights that extend beyond the scenario itself, enabling stakeholders to prepare for multiple hazards and build resilience against a range of possible future disasters.

The insights Tier 1 generates on systemic risks, critical functions, and common points of failure are its main contributes to Tier 2, rather than any insights specific to the random hazards that were examined.

Below are three sample scenarios that the card deck might generate. During facilitation (as discussed above), each scenario can be tailored to match the specific geographical scope and objectives of the case study partners.

Additionally, text-based AI can be harnessed to create a scenario overview of the appropriate scope by providing it with:

- The defined scope
- The relevant hazards
- Details about infrastructure likely to be affected by cascading effects
- A selected wild card

4.3.1. A regional event

Hazards: plant disease + heightened pollution
Context: a VIP visit
Cascading impacts: hydrogen storage

1. **Overview**
   - A high-profile dignitary is scheduled to visit a hydrogen research and storage facility located in a region that has been grappling with a severe plant disease outbreak. The government has rushed to mitigate the disease by approving emergency pesticides and fertilizers, which inadvertently exacerbate local air and water pollution. During final preparations for the VIP visit, a cascade of unexpected events unfolds, posing risks to both the visiting delegation's safety and the integrity of the hydrogen storage infrastructure.

2. **Setting and Background**
   1. **Geographical Context**
      a. The facility is in a semi-rural region known for its lush farmland and moderate climate.
      b. Nearby farms rely on a key crop that is now threatened by a newly emerged, fast-spreading fungal disease.
   2. **Hydrogen Research & Storage Facility**
      a. A cutting-edge complex that stores hydrogen in high-pressure tanks and underground chambers.
      b. The facility has advanced monitoring systems to detect leaks, pressure changes, and potential contamination.
      c. Current capacity is at 90% due to recent increases in hydrogen demand for clean energy initiatives.
   3. **VIP Visit**
      a. The visiting dignitary is a globally recognised figure (e.g., a head of state or a prominent international ambassador) who champions renewable energy.
      b. Media coverage is high; security is tight, with significant resources invested in ensuring the dignitary's safety.

3. **Key Stress Points**
   1. **Plant Disease Outbreak**
      a. A newly discovered fungal blight is destroying local crops at alarming rates.

b. Desperate farmers have begun applying experimental pesticides without thorough environmental impact assessments.
c. The disease's spread is accelerated by recent unseasonal weather (heavy rains, then sudden heat waves), creating perfect conditions for fungal growth.

2. **Environment-Driven Pollution**
   a. The unregulated application of pesticides and fertilizers is leading to contaminated runoff into nearby waterways.
   b. Local water treatment facilities struggle to keep up; trace chemicals are detected downstream, affecting both wildlife and farmland irrigation systems.
   c. Air quality in the vicinity of the farms has deteriorated due to increased spraying operations and stagnant weather patterns, raising concerns about inhalation risks.
3. **Hydrogen Storage Hazards**
   a. The storage facility's sensors begin to register unusual readings—possibly influenced by pollutant-laden water that has seeped near underground hydrogen chambers.
   b. Rapid temperature fluctuations (linked to the changing weather) cause unanticipated pressure differences in hydrogen tanks.
   c. Staff are also distracted by the VIP security protocols, which divert attention and resources from routine monitoring and maintenance.
4. **Cascading Impacts**
   a. **Pervasive Pollution:** The introduction of novel agricultural chemicals leads to a chemical reaction in one segment of the facility's water-cooling system, corroding some infrastructure faster than expected.
   b. **Sensor Malfunction:** Continuous infiltration of polluted runoff triggers false readings in the hydrogen pressure monitoring systems. Over time, slight undetected anomalies combine to cause a significant alarm event.
   c. **Operational Overload:** Emergency response teams are split between dealing with the VIP protection detail and investigating odd signals from the hydrogen storage system. This leaves the facility under-staffed for critical maintenance operations.
   d. **Logistics Disruption:** Unchecked plant disease quarantines certain roads, impeding the movement of specialized repair teams and replacement parts crucial for the hydrogen facility's containment system.

4.3.2. A national event

Hazards: wildfires + COVID
Context: unidentified green lights in the sky
Cascades: operation, management and maintenance of port and port facilities

1. **Overview:**
   - A string of unexplained green lights has appeared in the sky, causing national alarm and fuelling rampant speculation. Meanwhile, an aggressive wildfire season is devastating vast regions of the country, straining emergency services and casting smoke over critical industrial corridors. On top of these challenges, a new, highly transmissible COVID variant is once again overwhelming healthcare systems and complicating disaster response measures. In this scenario, major port facilities—vital for trade, energy, and economic stability—face unprecedented operational hurdles. The combined effects of curious celestial events, relentless wildfires, and an escalating pandemic threaten to upend an entire nation's logistics, infrastructure, and public confidence.

2. **Setting and Background**
   1. **Geographical Span**
      a. The country has several key ports along its coastlines, serving as hubs for imports, exports, and energy supplies.
      b. Widespread wildfires are concentrated inland but moving closer to coastal areas, heavily impacting road and rail networks that link ports to the rest of the country.

c. Unidentified green lights have been spotted throughout the nation's skies, from rural farmland to large metropolitan areas, prompting widespread curiosity and concern.

2. **Economic and Logistical Importance of Ports**
   a. Ports handle a substantial portion of the country's economic activity, including shipments of essential commodities (food, medical supplies) and industrial goods.
   b. Ongoing COVID-related restrictions have already disrupted global supply chains, increasing dependence on timely port operations to prevent shortages of critical items.
   c. National security agencies rely on these ports for strategic military and humanitarian shipments.
3. **COVID Landscape**
   a. A newly emerged variant exhibits greater contagiousness, resulting in surging hospitalisation rates.
   b. Government authorities have reactivated partial lockdown measures in certain regions, limiting workforce availability in critical sectors, including port operations.
   c. A fatigued healthcare system struggles to cope with both wildfire-related respiratory issues and rising COVID caseloads.
4. **Public Climate**
   a. Growing mistrust in official statements about the green lights leads to rampant speculation and viral conspiracy theories, often linking them to the pandemic or secret military activities.
   b. Social unrest is on the rise, as businesses face renewed lockdowns, and citizens question government transparency.
   c. The unpredictable nature of these overlapping crises heightens anxiety nationwide.

3. Key Stress Points

1. **Unidentified Green Lights**
   a. Spectacular but unexplained nighttime displays unsettle citizens, resulting in a spike in emergency calls, amateur investigations, and social media frenzy.
   b. Port communities, which rely on nighttime work shifts, report worker hesitancy to come in after dark, fearing unknown risks associated with the lights.
   c. Military and aviation authorities impose temporary flight restrictions in areas where the lights are most frequent, adding complexity to airborne firefighting and cargo operations.
2. **Severe Wildfires**
   a. Intensified by heat waves and drought conditions, wildfires threaten major rail lines and highways leading to port facilities.
   b. Port authorities struggle to secure alternative transportation routes for inbound/outbound cargo.
   c. Smoke impacts visibility in coastal regions, periodically suspending maritime traffic and endangering dockside operations.
3. **Renewed COVID Variant**
   a. Workers at ports, which are essential infrastructure, face higher exposure risk given the crowded environment, leading to staffing shortages.
   b. COVID outbreaks force quarantines and shutdowns in certain port terminals, causing significant cargo backlogs.
   c. Strained healthcare resources in port towns, which also handle injured or displaced wildfire evacuees, further reduce the available workforce.

4. **Unexpected Cascading Impacts on Port Operations**
   1. **Supply Chain Bottlenecks**
      - Containers pile up on docks as wildfires block inland transport routes, triggering expensive demurrage fees and slowing the clearance of incoming ships.

- Shortages of crucial goods—fuel, pharmaceuticals, firefighting equipment—lead to nationwide resource rationing.

2. **Management and Maintenance Gaps**
   - COVID restrictions and workforce illness hinder regular equipment checks, crane inspections, and facility maintenance.
   - As fires threaten electrical grid stability, repeated blackouts and power surges damage critical port control systems, requiring frequent repairs.
3. **Operational Disruptions**
   - Night shifts become less efficient or are halted due to worker concerns over the eerie green sky displays, exacerbating the existing labour shortfall.
   - Logistical confusion arises from overlapping firefighting airspace closures and new routes being charted around wildfire zones, delaying maritime and ground transport schedules.

4.3.3. A cross-boundary event

Hazards: forgotten weapons, economic recession
Context: a major international mass event
Cascading impacts: functioning of central government public administration entities

1. **Overview:**
   - A major international mass event—drawing participants and spectators from across continents—coincides with the unearthing of forgotten weapons from a historic conflict. Simultaneously, a deepening economic recession strains governmental budgets, impeding coordinated responses to emerging security threats. As these cascading challenges unfold, public administration entities in multiple central governments scramble to maintain essential services, safeguard the public, and preserve international trust.

2. **Setting and Background**
   1. **Geopolitical Context**
      a. Several countries are hosting or co-hosting a high-profile series of cultural or sports events, attracting millions of global visitors.
      b. Diplomatic relationships are tense due to ongoing trade disputes and competition for dwindling resources in the midst of an economic recession.
   2. **Forgotten Weapons**
      a. Historical stockpiles of obsolete weaponry—ranging from leftover ordnance to old chemical agents—are discovered by chance near major urban centres.
      b. Originally thought to be inert or already cleared, these caches pose new risks when disturbed during construction for event facilities or infrastructure projects.
      c. Some discovered weapons might be partially decayed, heightening the unpredictability of their stability and the potential for accidental detonations or contamination.
   3. **Ongoing Mass Event**
      a. The event spans multiple countries, with large clusters of attendees converging in major cities, stadiums, and public squares.
      b. Coordinating security and emergency services is complicated by a shortage of trained personnel.
      c. Widespread media coverage amplifies public awareness of any security misstep, intensifying pressure on governments to respond effectively.
   4. **Economic Recession**
      a. A global financial downturn has slashed government revenues, leading to budget cuts and hiring freezes across public sectors.
      b. Unemployment is high, and social safety nets are under strain, intensifying public dissatisfaction and the potential for unrest.
      c. Governments struggle to fund infrastructure security upgrades and safety checks—particularly relevant if forgotten weapons caches are found in or near event venues.

3. **Key Stress Points**
    1. **Security and Public Safety**
        a. Fragmented cooperation among multiple national police and intelligence agencies makes it difficult to track or neutralise the newly discovered weapons.
        b. The large crowds at the ongoing mass event present soft targets for any accidental or malicious use of these weapons.
        c. Heightened concern about potential terrorism or sabotage arises, particularly if extremist groups exploit the situation.
    2. **Public Administration Services Under Strain**
        a. Central government entities must reallocate personnel to address sudden security threats, which in turn creates staffing gaps in routine but essential services (healthcare, tax administration, immigration, etc.).
        b. Emergency management agencies are overwhelmed by calls to inspect, disarm, or safely dispose of old ordnance; slower response times erode public confidence.
        c. Health ministries face additional burdens if the discovered caches include chemical or biological agents, requiring specialised containment and medical preparedness.
    3. **Economic and Logistical Pressures**
        a. With the recession limiting budgets, governments struggle to finance additional security measures, ordnance-disposal experts, and large-scale event security operations.
        b. Budget constraints also hamper the timely procurement of safety equipment and disposal technology.
        c. Ongoing inflation and unstable currency markets further undercut the effectiveness of government interventions, creating friction among international partners.
    4. **International Coordination Challenges**
        a. Multiple host nations for the mass event must synchronise security measures and response strategies for discovered ordnance.
        b. Conflicting national interests, regulatory standards, and budgetary restrictions impede swift cooperation.
        c. Diplomatic strain emerges if one nation is perceived to be under-prepared or unwilling to enforce stricter safety protocols, fuelling intergovernmental tensions.
    5. **Public Perception and Trust**
        a. Global media outlets spotlight every misstep, from delayed bomb-disposal responses to abrupt event cancellations or venue shifts.
        b. Misinformation and conspiracy theories about the weapons' origins spread on social media, exacerbating fear and stoking public demonstrations.
        c. Citizens already frustrated by economic hardships accuse governments of negligence, leading to civil unrest in certain regions.

5. Approach to Integration and Adaptation

5.1. Adaption to Individual Context

As described in section 3.1.3 the scenario approach can be adapted to the local context of each case study while still maintaining elements of randomisation. In the preparation of each Tier 1 stress test implementation, the case study host will decide on one of the three possible randomisation approaches, supported by UCL as the developer of the approach:

- Full Randomisation
- Pre-filtered Card Deck: Applicable (local, regional or national) risk registers will be scanned, and hazard cards will be selected that could realistically occur in the geographical area. Depending on the maturity of risk management processes and the level of experience with creativity and lateral thinking in risk management, the difficulty of the potential scenario can be adjusted by excluding certain wild cards (see. Section 3.2.2).

- Preselected Cards: To align with a case study's specific scope (e.g., focussing on a specific infrastructure sector), one or multiple hazard or infrastructure cards could be preselected. "Pre-filtered Card Deck" and "Preselected Cards" could be combined, but no more than two cards should be fixed as preselection to ensure an element of surprise.

Based on the desired level of difficulty and the objectives, the facilitators can pre-filter the facilitation questions. During introduction, the facilitators will then support the participants to pick questions that are suitable for the implementation step, the actual scenario and the scope of the actual discussions. To this end, a set of 10 questions will be developed to help participants select elective questions that are relevant to them.

5.2. Feedback and Input from AGILE Partners

UCL twice presented an overview of work-in-progress, once to AGILE's project advisory board (16.01.25) and once to AGILE's case study partners (23.01.25). UCL sought specific feedback from the meeting attendees - practitioners and researchers with backgrounds in disaster and risk management - on whether the approach was feasible, useful, and in line with participants' theoretical and practical understandings of scenario creation and use.

The meeting participants offered several comments and suggestions, most of which supported and extended UCL's draft approach. Key themes included:

Clarify the Target Audience and Purpose

- Who the scenario is for (e.g., government officials, local responders, private sector, communities) affects the scope and style of the scenario.
- Different end-users will have different goals, e.g., public safety, business continuity, finance, or civil protection.

How the scenario will be tailored to different case study partners has been outlined in sections 3.1.3 and 5.1.

Highlight Interconnectedness and Feedback Loops

- Several participants stressed that interdependencies among critical infrastructures or sectors (e.g., energy, communications, finance) must be explicitly mapped and tested.
- In the United States, for instance, critical infrastructure operators are required to conduct table top exercises. The approach outlined by UCL should help them identify "blind spots" or hidden dependencies.

The Tier 1 stress test will examine cascading effects and common points of failure qualitatively. Tiers 2 and 3 will map these interdependencies quantitatively.

Balance "Randomisation" vs. Relevance

- There were active discussions on whether scenario events should be fully randomised or based on a known risk register.
- While random, highly improbable events can spark creativity, organisations are more likely to engage with scenarios that match their recognised hazards and operational realities.
- Compound threats - multiple concurrent hazards - were highlighted as especially relevant.

Case study partners will be provided with different options regarding full or partial randomisation. This is described in section 5.1.

Emphasise Empirical and Past-Event Analysis

- Participants noted that insights from historical near misses and real-world failures could anchor creative scenarios in realistic grounds.

- Understanding what actually went wrong in previous disasters, and why, can highlight vulnerabilities and guide scenario building.

Facilitators will encourage participants to draw on their existing knowledge and experience, including relevant real-world failures and near misses, when analysing the scenarios, especially during the counter factual analyses.

Value of Multi-Stakeholder Participation

- Drawing on experience with "impact-based" or "consequence-based" alerts, participants noted how new angles often emerge only when diverse voices - operational staff, technicians, community representatives - are at the table.
- For instance, a field technician's on-the-ground insights can differ profoundly from leadership's assumptions.

UCL will explore with case study partners who they want to include in the stress test, noting this point.

Engagement of Strategic-Level Decision Makers

- Participants noted that high-level management should be involved to draw on – and develop – strategic foresight; otherwise, scenarios remain abstract.
- Operational staff often focus on improvisation under crisis conditions, but managers can integrate broad, long-term perspectives.

UCL will explore with case study partners who they want to include in the stress test, noting this point.

Maintaining Credibility While Encouraging Creativity

- Creative scenarios aimed at fostering lateral thinking must remain goal-oriented and practical.
- Scenarios perceived as far-fetched (e.g., extreme "alien invasion" type events) risk losing participant buy-in. Yet ignoring HILPs can undermine resilience planning.

Case study partners will be given the option to exclude far-fetched risks. See section 5.1.

Learning from Other Sectors

- Insurance and reinsurance industries, for instance, employ statistical approaches (e.g., tail value at risk) to conceptualise rare, extreme events.
- Story-based or "any town" framing can help overcome the "this could never happen here" mindset.

Tier 1 does not use quantitative methods. Whilst "any town" is helpful, the purpose of the AGILE stress tests is to identify systemic risks in case study partners' actual jurisdictions. Therefore, whilst valuable, these recommendations will not be adopted in Tier 1.

6. Discussion

The methodology for scenario development outlined in this deliverable has significant potential to enhance preparedness for High Impact, Low Probability (HILP) events. However, implementing this approach poses several challenges and limitations that must be carefully considered.

Confidentiality and Sensitive Information

Adapting the outlined scenario approach to the specific case studies in the case of pre-filtering or pre-selection of hazards, infrastructures or elective questions may require more detailed discussions about risk assessments, critical infrastructure data, and hazard-specific information,

which are frequently classified or sensitive. Sharing such data can be hindered by confidentiality agreements, national security considerations, and organizational policies. Ensuring robust mechanisms for handling sensitive information securely while facilitating collaboration is a critical challenge.

Resistance to Highlighting Weaknesses
Participants in scenario exercises may be hesitant to focus on aspects that expose systemic weaknesses or vulnerabilities within their organizations or jurisdictions. This reluctance is often driven by reputational concerns, fear of criticism, or internal cultural barriers. As a result, scenarios might downplay critical vulnerabilities, reducing the potential for identifying and addressing true systemic risks. Effective facilitation and trust-building are essential to overcome this limitation. In agreement with the case study partner, separate exercise sessions could be conducted that cover different levels of sensitivity, e.g. a session with high-level representatives from public and private bodies and another session including more community representatives, first responders etc. If required, confidentiality agreements may be discussed. As this would also affect the confidentiality of the outcomes, it may be needed to treat the related deliverables as “sensitive” instead of “public” as initially foreseen.

Perception of Risk and Unrealistic Scenarios
While the inclusion of extreme and compounding hazards is vital for stress-testing systems, some stakeholders may view these scenarios as unrealistic or irrelevant, particularly if they involve events that challenge conventional risk paradigms. This can limit participant engagement and reduce the perceived value of the exercise. Tailoring scenarios to local risk registers and carefully framing their purpose can help address this issue.

Balancing Generalization and Specificity
The flexibility of the proposed methodology, such as randomization and modular scenario design, can lead to generalized insights that lack immediate applicability to specific contexts. Conversely, overly tailored scenarios might fail to uncover broader systemic vulnerabilities. Striking a balance between these two approaches is essential to ensure both relevance and depth.

Operational Challenges in Scenario Execution
The multi-layered and iterative nature of the scenario-building process can create logistical and cognitive challenges for participants, especially in time-constrained environments. The complexity of the exercises might lead to participant fatigue or difficulty in drawing actionable conclusions. Simplifying facilitation and providing clear guidance are necessary to maintain focus and productivity.

While the outlined approach offers a comprehensive framework for enhancing disaster preparedness, these challenges highlight the importance of careful planning, facilitation, and adaptation to the needs of stakeholders. Addressing these limitations proactively will enhance the effectiveness and impact of the methodology, ensuring it remains a valuable tool for managing HILP events.

7. Conclusion

The outlined scenario development approach holds significant promise for improving disaster preparedness and resilience by addressing High Impact, Low Probability (HILP) events. However, its successful implementation requires overcoming key challenges, particularly around handling sensitive information, fostering an open and constructive environment for identifying weaknesses, and ensuring scenarios remain relevant while pushing participants to explore systemic vulnerabilities.

As a next step, the methodology will be pilot tested on 25th February 2025 with postgraduate students from University College London and members of the Greater London Authority, AGILE’s case study partners. This pilot will serve as a cross-check to validate the approach, ensuring its

feasibility for practitioners and refining the methodology based on end-user feedback. The key areas of focus include:

1. **Scenario Tailoring and Validation**: Ensure scenarios are both challenging and context-specific by incorporating feedback from case study partners and aligning with local risk registers.
2. **Enhancing Facilitation Techniques**: Provide concise guidance for facilitators to manage sensitive discussions and maintain engagement during complex scenarios.
3. **Strengthening Stakeholder Engagement**: Integrate lessons from historical HILP events and maintain a focus on actionable insights that lead to tangible improvements in preparedness and response systems.
4. **Establishing Trust and Data Security Measures**: In discussions with the individual case study partner, develop clear procedures for handling confidential information to encourage open sharing of risks and vulnerabilities among participants.
5. **Building a Culture of Transparency**: Within the stakeholder communication and the exercise introduction focus on trust-building and creating a safe discussion environment to reduce resistance to addressing potential weaknesses and systemic failures.

By addressing these priorities, the methodology for developing scenarios can be refined to support the AGILE project's broader mission of enhancing disaster resilience across diverse contexts and stakeholders and serve as a foundation for resilience stress testing, guiding decision-makers in local, regional, and national contexts.

References

Alexander, D. (2000). *Scenario methodology for teaching principles of emergency management. Disaster Prevention and Management: An International Journal, 9*(2), 89-97.

Alexander, D. E. (2002). *Principles of Emergency Planning and Management.* United Kingdom: Oxford University Press.

Alexander, D. E. (2017). *How to write an emergency plan.* United Kingdom: Liverpool University Press.

Lin-Greenberg, E., Pauly, R. B., & Schneider, J. G. (2022). *Wargaming for international relations research. European Journal of International Relations*, *28*(1), 83-109.
January 9,

Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction, 82*, 103323.