Report No.450

epa Research

Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards

Authors: Ilaria Bernardini, Mark Tucker, Moreno Stellini and Emmanouil Kakouris.

www.epa.ie

Rialtas na hÉireann
Government of Ireland

Environmental Protection Agency

The EPA is responsible for protecting and improving the environment as a valuable asset for the people of Ireland. We are committed to protecting people and the environment from the harmful effects of radiation and pollution.

The work of the EPA can be divided into three main areas:

Regulation: Implementing regulation and environmental compliance systems to deliver good environmental outcomes and target those who don't comply.

Knowledge: Providing high quality, targeted and timely environmental data, information and assessment to inform decision making.

Advocacy: Working with others to advocate for a clean, productive and well protected environment and for sustainable environmental practices.

Our Responsibilities Include:

Licensing

- Large-scale industrial, waste and petrol storage activities;
- Urban waste water discharges;
- The contained use and controlled release of Genetically Modified Organisms;
- Sources of ionising radiation;
- Greenhouse gas emissions from industry and aviation through the EU Emissions Trading Scheme.

National Environmental Enforcement

- Audit and inspection of EPA licensed facilities;
- Drive the implementation of best practice in regulated activities and facilities;
- Oversee local authority responsibilities for environmental protection;
- Regulate the quality of public drinking water and enforce urban waste water discharge authorisations;
- Assess and report on public and private drinking water quality;
- Coordinate a network of public service organisations to support action against environmental crime;
- Prosecute those who flout environmental law and damage the environment.

Waste Management and Chemicals in the Environment

- Implement and enforce waste regulations including national enforcement issues;
- Prepare and publish national waste statistics and the National Hazardous Waste Management Plan;
- Develop and implement the National Waste Prevention Programme;
- Implement and report on legislation on the control of chemicals in the environment.

Water Management

- Engage with national and regional governance and operational structures to implement the Water Framework Directive;
- Monitor, assess and report on the quality of rivers, lakes, transitional and coastal waters, bathing waters and groundwaters, and measurement of water levels and river flows.

Climate Science & Climate Change

- Publish Ireland's greenhouse gas emission inventories and projections;
- Provide the Secretariat to the Climate Change Advisory Council and support to the National Dialogue on Climate Action;
- Support National, EU and UN Climate Science and Policy development activities.

Environmental Monitoring & Assessment

- Design and implement national environmental monitoring systems: technology, data management, analysis and forecasting;
- Produce the State of Ireland's Environment and Indicator Reports;
- Monitor air quality and implement the EU Clean Air for Europe Directive, the Convention on Long Range Transboundary Air Pollution, and the National Emissions Ceiling Directive;
- Oversee the implementation of the Environmental Noise Directive;
- Assess the impact of proposed plans and programmes on the Irish environment.

Environmental Research and Development

- Coordinate and fund national environmental research activity to identify pressures, inform policy and provide solutions;
- Collaborate with national and EU environmental research activity.

Radiological Protection

- Monitoring radiation levels and assess public exposure to ionising radiation and electromagnetic fields;
- Assist in developing national plans for emergencies arising from nuclear accidents;
- Monitor developments abroad relating to nuclear installations and radiological safety;
- Provide, or oversee the provision of, specialist radiation protection services.

Guidance, Awareness Raising, and Accessible Information

- Provide independent evidence-based reporting, advice and guidance to Government, industry and the public on environmental and radiological protection topics;
- Promote the link between health and wellbeing, the economy and a clean environment;
- Promote environmental awareness including supporting behaviours for resource efficiency and climate transition;
- Promote radon testing in homes and workplaces and encourage remediation where necessary.

Partnership and Networking

- Work with international and national agencies, regional and local authorities, non-governmental organisations, representative bodies and government departments to deliver environmental and radiological protection, research coordination and science-based decision making.

Management and Structure of the EPA

The EPA is managed by a full time Board, consisting of a Director General and five Directors. The work is carried out across five Offices:

1. Office of Environmental Sustainability
2. Office of Environmental Enforcement
3. Office of Evidence and Assessment
4. Office of Radiation Protection and Environmental Monitoring
5. Office of Communications and Corporate Services

The EPA is assisted by advisory committees who meet regularly to discuss issues of concern and provide advice to the Board.

Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards

Authors: Ilaria Bernardini, Mark Tucker, Moreno Stellini and Emmanouil Kakouris.

Identifying pressures

Extreme weather events such as storms, landslides, river floods and coastal phenomena have threatened and damaged many different regions across Ireland. These events, while rare and often short-lived, can have a devastating impact on critical infrastructure systems. As a result of climate change, these events are becoming more frequent and more intense, affecting not only physical infrastructure but also the environment and society as a whole.

Using risk-based approaches in assessing the impacts of extreme weather events and climate change is a well-established method of identifying the most vulnerable infrastructure, assessing the risks posed to that infrastructure and developing strategies to minimise those risks.

Therefore, the objective of this project was to develop a design for a full-scale study to assess the risk posed to critical infrastructure in Ireland by climate change, with due consideration of interdependencies between different infrastructure types (i.e. cross-sectoral issues) and primary and cascading hazards, that was both achievable and beneficial to the infrastructure owners, society and the environment.

Informing policy

A Several national documents are published in Ireland that identify not only the key infrastructure sectors, but also the weather events they are exposed to. These documents provide assistance to the infrastructure owners/managers within the key sectors to develop sectoral adaptation plans to minimise the risk posed by extreme weather events to the infrastructure. While risk assessment is a recommended means of evaluating the vulnerability of a particular infrastructure to a particular event, there are many different risk formulations and methodologies that can be used to undertake a risk assessment, the complexity of which is largely dependent on data and resource availability.

Given the various methodologies available to conduct risk assessments, this project provided an overview of them, outlining the various requirements and information needed to conduct risk assessments of various complexities. Furthermore, an overarching risk assessment methodology was proposed considering the methodologies currently used by relevant stakeholders in Ireland and the information available to them to conduct a meaningful risk assessment.

Developing solutions

This report presents an overarching risk assessment methodology for assessing risks posed to critical infrastructure by climate change. While the methodology proposed was developed through reviewing both national and international research and the authors' own experience in developing risk assessments, the key element in successfully achieving the objectives of the project was extensive engagement with key stakeholders across multiple infrastructure sectors. This engagement provided invaluable information on and insights into current practices and the challenges and barriers faced when implementing meaningful risk assessments. Equally, the presence of cross-sectoral stakeholders highlighted the opportunities and challenges of ensuring that a cross-sectoral approach to risk assessing infrastructure can be achieved. From these interactions, recommendations were made on key issues, such as data collection, data sharing, data security, resource requirements and monitoring regimes, that could be reasonably implemented in the Irish context.

EPA RESEARCH PROGRAMME 2021–2030

INFRALINC

Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards

(2021-CE-1068)

EPA Research Report

Prepared for the Environmental Protection Agency

by

Roughan & O'Donovan Ltd

Authors:

Ilaria Bernardini, Mark Tucker, Moreno Stellini and Emmanouil Kakouris

ENVIRONMENTAL PROTECTION AGENCY
An Ghníomhaireacht um Chaomhnú Comhshaoil
PO Box 3000, Johnstown Castle, Co. Wexford, Ireland

Telephone: +353 53 916 0600 Fax: +353 53 916 0699
Email: info@epa.ie Website: www.epa.ie

ACKNOWLEDGEMENTS

This report is published as part of the EPA Research Programme 2021–2030. The EPA Research Programme is a Government of Ireland initiative funded by the Department of the Environment, Climate and Communications. It is administered by the Environmental Protection Agency, which has the statutory function of co-ordinating and promoting environmental research.

The authors would like to acknowledge the members of the project steering committee, namely Lee Chapman (University of Birmingham), Mary Curley (Met Éireann), Seosamh O'Laoi (Department of the Environment, Climate and Communications), Maurice Harnett (Department of Transport), Stephen Flood (EPA), Sean O'Leary (formerly EPA) and Fintan McGrath (Department of Transport).

DISCLAIMER

Although every effort has been made to ensure the accuracy of the material contained in this publication, complete accuracy cannot be guaranteed. The Environmental Protection Agency, the authors and the steering committee members do not accept any responsibility whatsoever for loss or damage occasioned, or claimed to have been occasioned, in part or in full, as a consequence of any person acting, or refraining from acting, as a result of a matter contained in this publication. All or part of this publication may be reproduced without further permission, provided the source is acknowledged.

This report is based on research carried out/data from March 2022 to February 2023. More recent data may have become available since the research was completed.

The EPA Research Programme addresses the need for research in Ireland to inform policymakers and other stakeholders on a range of questions in relation to environmental protection. These reports are intended as contributions to the necessary debate on the protection of the environment.

EPA RESEARCH PROGRAMME 2021–2030

Published by the Environmental Protection Agency, Ireland

ISBN:978-1-80009-153-5 February 2024

Price: Free Online version

Project Partners

Ilaria Bernardini
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Ilaria.Bernardini@rod.ie

Mark Tucker
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Mark.Tucker@rod.ie

Moreno Stellini
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Moreno.Stellini@rod.ie

Emmanouil Kakouris
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Emmanouil.Kakouris@rod.ie

Frances O’ Kelly
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Frances.OKelly@rod.ie

Ciaran Carey
Roughan & O’Donovan Ltd
Arena House
Arena Road
Sandyford
Dublin
D18 V8P6
Tel.: +353 1 294 0800
Email: Ciaran.Carey@rod.ie

Dermot Collins
Dublin City Council
Civic Offices
Wood Quay
Dublin 8
D08 RF3F
Tel.: +353 1 222 2222
Email: Dermot.collins@dublincity.ie

Cathal Mangan
Iarnród Éireann (Irish Rail)
Connolly Station
Amien Street
Dublin 1
D01 V6V6
Tel.: +353 87 290 7885
Email: cathal.mangan@irishrail.ie

John Scully
Eir
Knockmay
Portlaoise
Laois
R32 YK81
Tel.: +353 85 174 2251
Email: john.scully@openeir.ie

Contents

List of Figures

List of Tables and Boxes

Tables

Boxes

Executive Summary

The INFRALINC (Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards) project aimed to develop a design for a full-scale study to assess the risk posed to critical infrastructure (CI) in Ireland by climate change. The project specifically focused on risk calculation, with consideration of interdependencies between different infrastructure types, cascading hazards, prioritisation of risks and/or mitigation and adaptation measures.

Significant efforts have been made in the past to develop frameworks and simulations to formulate interdependent risk calculation for CI with varying levels of success. Acknowledging that cross-sectoral risk metrics, data sharing and data security are typically the key stumbling blocks for multi-modal risk assessment, the INFRALINC project presented an overarching methodology for developing a design for a full-scale study that is both achievable and beneficial to the infrastructure owners, society and the environment by bringing together the key infrastructure owners in Ireland.

The objectives of the project were achieved through a series of work packages, each contributing to the evolution of the project. Initially, an inventory of CI and associated climate-related events was developed, highlighting the impacts and consequences of various past events on elements of infrastructure, including cascading failures. Subsequently, to provide context and background on the recommended frameworks and methodologies to be used in the Irish context, existing and implemented frameworks were reviewed, in which interdependencies, cascading events, cross-sectoral impacts, cumulative impacts and vulnerabilities in current and future scenarios were examined. Essential components of any risk assessment methodology are the data requirements, data availability and data sharing issues, for which an initial high-level investigation was undertaken. Based on the data availability, or lack of it, a monitoring regime for infrastructure was then proposed to ensure that adequate and accurate data could be obtained for the recommended risk assessment methodology. Lastly, general recommendations were made about the most appropriate approach to developing a design for a full-scale study, which suggested that, while a quantitative approach is recommended, data availability and data sharing issues are limitations in the Irish context.

A key to successfully achieving the objectives of INFRALINC was engagement with stakeholders, which was facilitated through the following workshops: “Critical Infrastructure and Extreme Weather Events”, “Data Availability and Requirements” and “Data Ongoing Monitoring and Security”. Attended by representatives from the transport, energy, waste, water, defence and telecommunications sectors, the workshops provided invaluable information on the pertinent issues analysed in INFRALINC and being faced by CI owners.

1 Introduction

The INFRALINC (Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards) project aimed to develop a design for a full-scale study to assess the risk posed to critical infrastructure (CI) in Ireland by climate change, considering interdependencies between different infrastructure types and cascading hazards. In order to develop a framework that would allow interdependent risk calculation for CI, the INFRALINC project reviewed frameworks and methodologies that had been implemented in the past with different levels of success. The framework proposed in INFRALINC also considered cross-sectoral risk metrics, data sharing and data security, issues that are typically key stumbling blocks for multi-modal risk assessment. Stakeholder engagement played a key part in the project and took place over a number of topic-specific workshops. The framework proposed should be both implementable by, and beneficial to, the relevant stakeholders, and therefore their input contributed in no small part to the final recommendations.

The INFRALINC project aimed to achieve the following objectives:

- produce an inventory of CI and associated climate-related events;
- develop cross-sectoral climate hazard vulnerability assessment recommendations for the Irish context;
- identify what data is currently available and what data will be required as a minimum to perform a climate impact assessment for Irish CI;
- formulate a monitoring regime for Irish infrastructure owners to ensure that sufficient data is available, allowing for future changes in the scientific environment and climate change;
- identify data sharing issues and propose a regime to appropriately consider security concerns in cross-sectoral data usage.

This report presents a summary of the work done in the INFRALINC project, the current challenges in the development of the framework and the overall findings and conclusions. Chapter 2 gives an overview of the CIs and extreme weather events (EWEs) identified in the Irish context based on a literature review and stakeholder interaction. Chapter 3 describes the proposed risk assessment framework for a full-scale study, detailing the steps of the methodology and giving recommendations on the best methodologies to be used. Chapter 4 focuses on data and its availability and requirements for carrying out a risk assessment, and Chapter 5 analyses the issues of data sharing and possible solutions. Chapter 6 provides an overview of the potential costs associated with the implementation of the full-scale study. Lastly, Chapter 7 provides conclusions and recommendations.

2 Critical Infrastructures and Extreme Weather Events

As part of the INFRALINC project, the main CIs and EWEs in Ireland were identified. The review of international and national documents provided a good background on the relevant CIs and EWEs in Ireland, but direct communication with stakeholders provided useful insights on their concerns and priorities. This direct communication was facilitated through the first project workshop: "Critical Infrastructure and Extreme Weather Events". An inventory of CIs and associated EWEs was also developed, highlighting the impacts and consequences of various past events on elements of infrastructure, including cascading failures (Appendix A).[1] The inventory primarily focused on the Irish context but also included some Europe-wide events, which could be very relevant to Ireland.

2.1 Critical Infrastructures

Several national and international documents were reviewed during the project to gain an overview of how CIs are defined and identified. Relevant documents included EU Council Directive 2008/114/EC (EU, 2008); Strategic Emergency Management: National Structures and Framework (Department of Defence, 2017); Strategic Emergency Management – Guideline 3 (Department of Defence, 2021a); A National Risk Assessment for Ireland 2020 (Department of Defence, 2021b); and the National Adaptation Framework (Department of Communications, Climate Action and Environment, 2018a).

EU Council Directive 2008/114/EC (EU, 2008) defines a CI as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". In Ireland,

Table 2.1. Sectors and lead departments

Theme	Sector level	Lead department for sectoral adaptation plans
Natural and cultural capital	Seafood Agriculture Forestry	Department of Agriculture, Food and the Marine
	Biodiversity Built and archaeological heritage	Department of Culture, Heritage and the Gaeltacht (now Department of Tourism, Culture, Arts, Gaeltacht, Sports and Media)
Critical infrastructure	Transport infrastructure	Department of Transport, Tourism and Sport (now Department of Transport)
	Electricity and gas network Communication network	Department of Communications, Climate Action and Environment (now Department of the Environment, Climate and Communications)
Water resource and flood risk management	Flood risk management	Office of Public Works
	Water quality Water services infrastructure	Department of Housing, Planning and Local Government (now Department of Housing, Local Government and Heritage)
Public health	Health	Department of Health

Source: Department of Communications, Climate Action and Environment (2018a).

1 The appendices are included in the full version of this report, available on the INFRALINC project page on the Roughan & O'Donovan website (https://www.rod.ie/projects/infralinc).

Table 2.2. Critical infrastructures for the Irish context

Sector	Subsector
Energy	Electricity network Gas network Oil network Waste network Wind farms
Water	Water network (supplies and wastewater, including the sewerage system)
Food	Food supply
Information and communications technology (ICT)	Telecommunication network Information technology Media
Finance and financial services	Banking (including payment delivery) Insurance Welfare payments systems
Transport	Aviation Road network Rail transport Marine and ports
Health	Hospitals Laboratories
Public administration	Government Central and local government Justice and legal system Revenue and customs Cultural property Diplomatic representation and international headquarters
National security, policing and public safety infrastructure	An Garda Fire and emergency National Ambulance Service Irish Coast Guard Prison service Defence forces Civil defence
Industry	Hazardous industries Agriculture and marine industries Manufacturing and processing industries Industrial and domestic waste disposal Logistical supply chains
Infrastructures	Bridges Culverts Tunnels Slopes/embankments Quays/retaining walls

the National Adaptation Framework (Department of Communications, Climate Action and Environment, 2018a) defines the key sectors concerned with developing sectoral adaptation plans, divided into four key thematic areas (Table 2.1). Based on the review of available documents and the feedback of relevant stakeholders during workshops, a list of relevant CIs was identified for the Irish context (Table 2.2).

Modern urban infrastructure is highly interdependent, formed of multiple connections, feedback loops and "feedforward" paths. Figure 2.1 shows an example of infrastructure interdependencies from *Strategic Emergency Management – Guideline 3: Critical Infrastructure Resilience (Version 2)* (Department of Defence, 2021a).

2.2 Extreme Weather Events

Strategic Emergency Management: National Structures and Framework (Department of Defence, 2017) defines an emergency as "an event which, usually with little or no warning, causes or threatens to cause death, serious injury, serious disruption to essential services, the economy or critical infrastructure, significant damage to property or the environment, and which requires the activation of National resources to ensure an effective coordinated response and recovery". The National Adaptation

Box 2.1. Extreme weather events for the Irish context

Flooding

Rainfall

First flush

Snowfall

Hail

Cold weather

Freezing events

Strong wind

Storms

Thunder and lighting

Heat wave

Drought

Landslides

Sea level rise

Coastal erosion

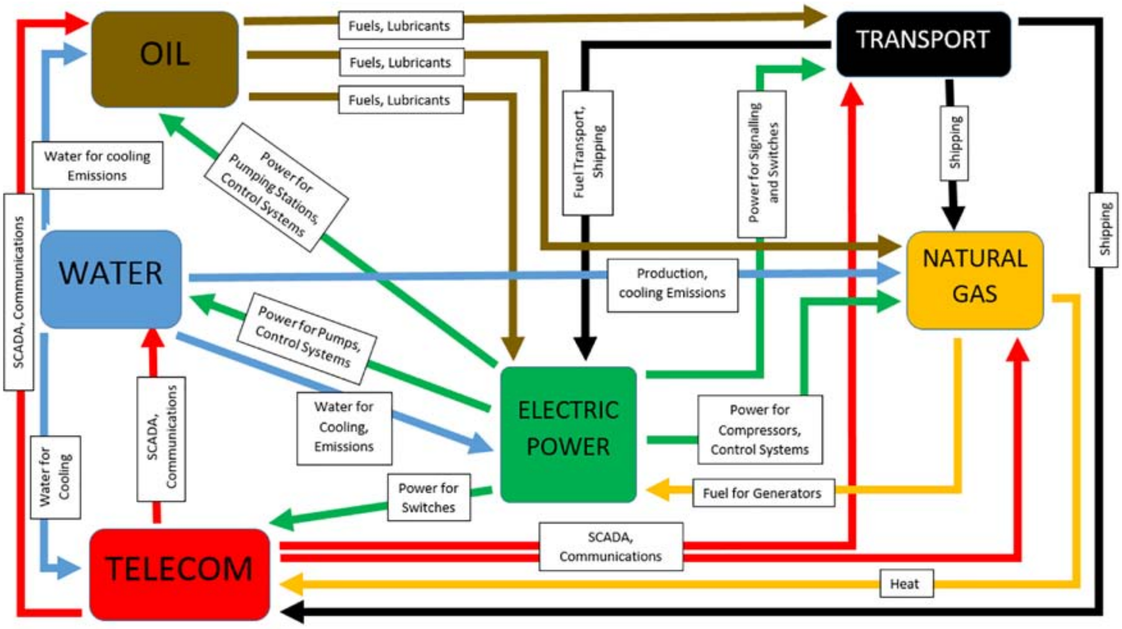

Figure 2.1. Examples of critical infrastructure interdependencies. Source: Department of Defence (2021a).

Framework (Department of Communications, Climate Action and Environment, 2018a) defines an EWE as "an event that includes unusual, severe or unseasonal weather or weather at the extremes of the range of weather observed in the past". EWEs are often short lived and include events such as heat waves, freezes, heavy downpours and floods.

Through the review of available documents, such as Strategic Emergency Management (Department of Defence, 2017), National Risk Assessment 2021/2022 (Department of the Taoiseach, 2018) and A National Risk Assessment for Ireland 2020 (Department of Defence, 2021b), and based on stakeholder interaction during workshops, a list of relevant EWEs (Box 2.1) for the Irish context has been identified. The National Risk Assessment, published in 2023 (Department of the Taoiseach, 2023), has been updated with significant risks that may arise for Ireland over the short, medium and long terms.

Based on the National Adaptation Framework (Department of Communications, Climate Action and Environment, 2018a) and the Sectoral Planning Guidelines for Climate Change Adaptation (Department of Communications, Climate Action and Environment, 2018b), each sector listed above (Table 2.2) has developed a sectoral adaptation plan. Each plan provides a list of the key climate impacts relevant to the sector, which are summarised in Table 2.3. However, it is worth noting the recently published Climate Action Plan (Government of Ireland, 2023a) and associated Annex (Government of Ireland, 2023b), to be updated annually, which outline the actions required to address climate change up to 2035 and beyond. Specifically, action number AD/25/1 requires the development of new sectoral adaptation plans in line with updated sectoral adaptation guidelines, while AD/25/2 requires the development and implementation of the delivery and publication of Ireland's first dedicated Climate Change Risk Assessment, setting out the priority impacts of climate change for Ireland. These actions are due for completion in Q1 and Q2 of 2025, respectively.

Table 2.3. Key sectoral climate impacts

Sector	Key climate impacts
Agriculture, forestry and seafood (Department of Agriculture, Food and the Marine, 2019)	Changes in air temperature Changes in precipitation patterns and hydrology Increase in intensity and frequency of extreme events Changes in ocean temperature Sea level rise
Biodiversity (Department of Culture, Heritage and the Gaeltacht, 2019a)	Changes in phenology Changes in the geographical ranges of species Increased degradation of habitats and changes in ecosystem processes Increased occurrence of invasive species
Built and archaeological heritage (Department of Culture, Heritage and the Gaeltacht, 2019b)	Increased flood and storm intensity and frequency Sea level rise Greater wave energy Increased high tidal levels Changes in salinity and saline intrusion Rainfall and wind-driven rainfall Changes in moisture content of soil Long and dry summers Floods Prolonged periods of wetness Air temperature rise Increased occurrence of invasive species

Table 2.3. Continued

Sector	Key climate impacts
Energy sectors: communications, electricity and gas networks (Department of Communications, Climate Action and Environment, 2019)	Flooding Changes in precipitation Changes in extreme events Temperature rise Sea level rise Changes in wind speeds
Flood risk management (Office of Public Works, 2019)	Increased average temperature Wetter winters and drier summers Increased intensity of storms Sea level rise Increased sea surface temperature
Health (Department of Health, 2019)	Air pollution UV radiation Windstorms Extreme cold snaps Increase in precipitation and flooding events Extreme heat and heat waves
Transport sector (Department of Transport, Tourism and Sport, 2019)	High priority: • Changes in precipitation • High winds/storm surges • Sea level rise Moderate priority: • High temperature extremes • Low temperature extremes • Coastal erosion
Water quality and water services (Department of Housing, Planning and Local Government, 2019)	Variation in temperature Changes in precipitation intensity and frequency Changes in storm driving parameters Sea level rise

3 Risk Assessment Framework

In recent years, climate change has led to an increase in the severity and frequency of EWEs, impacting infrastructure and environmental and socio-economic systems. In order to be properly prepared for EWEs and to be able to effectively deal with a potential emergency, the risk posed by these events needs to be assessed and estimated. In general, *risk* can be defined as “the chance that an event will occur with how large its impact could be, in social, economic or environmental terms” (Department of Communications, Climate Action and Environment, 2018a) or “the combination of the likelihood of a hazardous event and its potential impact” (Department of Defence, 2017). *Hazard* is defined as “any phenomenon with the potential to cause direct harm to members of the community, the environment or to the physical infrastructure, or being potentially damaging to the economic and social infrastructure” (Department of Defence, 2017). *Impact* and *likelihood* are respectively defined as “the consequences of a risk expressed in terms of a negative outcome for people, the environment, economic activity or societal structures” and “the probability (or frequency) of a risk occurring” (Government of Ireland, 2020). In the case of climate change and its effect on CI, risk can be calculated by a high-level generalised formula (equation 3.1). It must be noted, however, that the concept and representation of risk are much more complex, as shown, for example, in IPCC (2022) and explained in subsequent sections of this report.

$$\text{Risk} = \text{Likelihood of the EWE} \times \text{Vulnerability} \quad (3.1)$$

As part of the INFRALINC project, an extensive literature review of frameworks for risk management was carried out from past projects, such as Sventekova *et al*. (2015) and Adey *et al*. (2014), at both the international level, such as IPCC (2022) and ISO (2018), and the national Irish level, such as Department of Housing, Local Government and Heritage (2010) and Department of Communications, Climate Action and Environment (2018b). While more focus is given to the existing Irish frameworks, some aspects of the international frameworks might contribute to the improvement of the Irish frameworks. The most relevant Irish frameworks identified are *Framework for Major Emergency Management – A Guide to Risk Assessment in Major Emergency Management* (Department of Housing, Local Government and Heritage, 2010), which consists of a five-step planning cycle, and *Sectoral Planning Guidelines for Climate Change Adaptation* (Department of Communications, Climate Action and Environment, 2018b), which is based on a six-step planning cycle. It is also worth mentioning *Strategic Emergency Management – Guideline 3* (Department of Defence, 2021a), which provides a methodology to assess the criticality of infrastructures and, if criticality is high, can identify infrastructures for which the application of a detailed risk assessment is appropriate.

Based on the review of the existing frameworks in the literature and in the Irish context, an overarching methodology was developed for the INFRALINC project. The proposed methodology evaluates the risk associated with multiple infrastructure networks and can be used for different hazards. The methodology considers a generic definition of networks and objects of networks, the effect of different types of hazards on networks and cascading processes, the propagation of effects through networks, and the modelling of interdependencies between multiple objects in networks.

Through the workshops that took place during the project, feedback was obtained from relevant stakeholders in Ireland. The importance of preserving the framework currently available and being used by the different sectors in the country was often emphasised. Therefore, the framework proposed ensures that the risk assessment methodology currently implemented in Ireland, which is based on Department of Communications, Climate Action and Environment (2018b) and Department of Housing, Local Government and Heritage (2010) guidance, is taken into account.

The methodology proposed can be subdivided into three main phases, as shown in Figure 3.1:

- **Risk identification.** Initial thought is given to the problem, potential scenarios to be analysed are identified and information and data relevant to the system is gathered, including hazards, infrastructures, social factors, environmental factors.

- **Risk assessment.** Based on the data available, hazard and vulnerability assessments are carried out through qualitative, semi-quantitative or quantitative processes.
- **Adaptation planning and risk treatment.** The risk calculated is analysed and compared with the risk of other potential scenarios; possible actions to reduce and treat the risk are then evaluated and the best option can be identified, often using a cost–benefit analysis (CBA) process.

After relevant risks have been identified, several approaches can be used in the risk assessment phase to evaluate each risk. An exhaustive review and description of these methodologies is provided in ISO 31010:2019 (ISO, 2019), including pros and cons for each of them. During the INFRALINC project several methodologies were analysed and mainly subdivided into qualitative, semi-quantitative and quantitative methodologies. The selection of the best method depends on different factors, such as data availability, the level of detail desired/required, available resources, cost and the accessibility of expert knowledge. Based on the literature review carried out, three main approaches are recommended for the Irish context and for the purpose of the proposed INFRALINC framework, but other approaches might be more suitable depending on the output desired. The three recommended methods are:

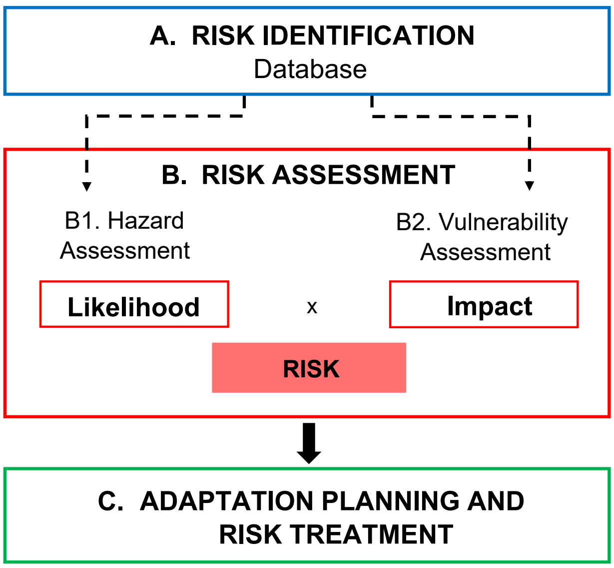

Figure 3.1. INFRALINC's overarching risk assessment methodology.

- **Risk matrix.** This method is intuitive and flexible, since it can be implemented qualitatively, semi-quantitatively or quantitatively; the risk matrix is also often used in the various climate change sectoral adaptation plans, which makes this method already well known among relevant stakeholders in Ireland.
- **Bow tie analysis.** This method enables a more detailed process while still being applicable qualitatively and maintaining a level of flexibility; it enables graphical representation of the pathways from the causes to the consequences of an event. However, a limitation is that it cannot take into account a situation where the pathways from causes to event are interdependent.
- **Bayesian network.** This method is the most complete, though complex, of the three proposed, while still being intuitive, thanks to its graphical representation of the events. Being a quantitative methodology, it requires a certain level of data availability, but it enables the consideration of different scenarios, taking into account interdependencies and cascading events.

The current approach taken in Ireland to a risk management framework is to use a more qualitative procedure using a risk matrix in accordance with the sectoral adaptation plan, to be updated as per the Climate Action Plan 2023 (Government of Ireland, 2023a), for each sector. In the context of the INFRALINC project, focus was then put on the implementation of a risk matrix technique with more semi-quantitative features. A risk matrix, also referred to as a consequence/likelihood matrix or heat map, is a way of displaying risk based on the combination of consequences and likelihood, which are shown on the axes of the matrix (Figure 3.2). Customised scales are separately defined to evaluate and assign a score to consequences and likelihood. The score scales can be of any dimension and can be qualitative or quantitative, depending on what is required by, or is best for, the stakeholder. By combining the two values, a final risk score is obtained. The consequences and likelihood values can be obtained based on a combination of different factors influencing them, with the use of weighting factors if desired. The final

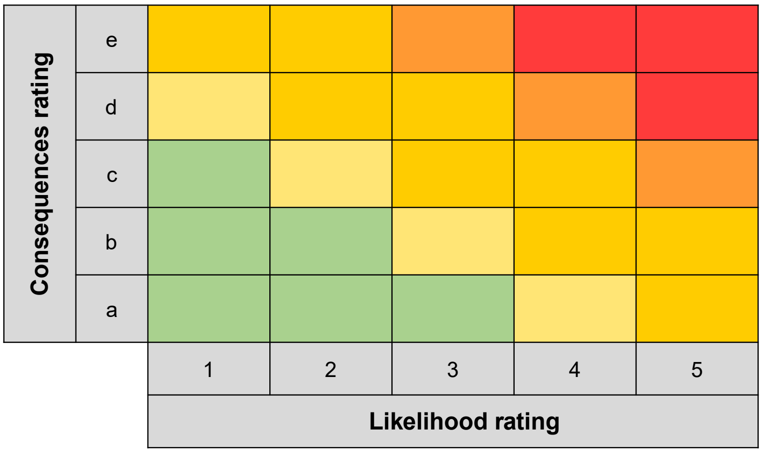

Figure 3.2. Example of consequence/likelihood matrix.

combined value is then standardised to the respective customised scale.

In Figure 3.2 a colour-coded scale is adopted to allow an easier understanding of the level of the risk for the particular hazard: light yellow represents a tolerable risk, whereas red represents a risk requiring immediate action. More details on the risk matrix and scales can be found in ISO (2019).

3.1 Risk Identification

The risk identification phase involves giving initial thoughts on the problem being analysed, identifying the boundaries and characteristics of the problem, determining potential scenarios and gathering relevant information and data, which will build a solid base for the risk assessment. This phase aims initially to identify risks, causes, events, vulnerabilities and consequences/impacts, and subsequently to create a database based on the initial considerations. The dataset can be more or less detailed depending on the type of approach taken for the risk assessment, the analysis outcomes desired and the data available. The data will be used in subsequent phases to evaluate hazards and vulnerability (exposure, susceptibility and adaptive capacity), and consider risk treatments and adaptation planning. The information should be collected in relation to the overall system, including hazards, infrastructures and the surrounding area. Data to be gathered might refer to, but not be limited to, environmental factors, triggering factors, cascading events, hazard inventory, climate change scenarios and social elements at risk. More details on data are provided in Chapter 4. In this phase, several scenarios/pathways might be taken into account, which are not necessarily mutually exclusive. These could include:

- different climate scenarios and current and future climate predictions;
- different mitigation measures, currently implemented and potential future measures;
- different EWEs that are relevant for the system being considered and related cascading hazards;
- different interdependent infrastructures and potential disruption/failure scenarios.

3.2 Risk Assessment

The risk assessment phase provides an estimation of the risk to the CI under consideration depending on the hazards being analysed. This phase consists of two sub-phases: hazard assessment and vulnerability assessment. The information obtained in the risk identification phase feeds into these two sub-phases to obtain an estimation of risk. For example, environmental factors, hazard inventory and elements at risk contribute to the evaluation of vulnerability, and triggering factors, cascading events, hazard inventory and climate change scenarios influence the hazard assessment. It must be noted that the risk assessment and the data used are very dependent on the approach chosen, the level of detail desired and data availability, and that this process should be adapted based on the outputs required. The hazard and vulnerability assessments result in an estimation of the likelihood of the event and of the vulnerability of the system, respectively, and these estimations are combined to obtain the risk value. In the risk identification phase, as explained above, various scenarios can be identified. For each of them, a risk assessment process should be carried out, which will result in a series of risk values that can be analysed and compared. Based on the risk values obtained and the purpose of the implementation of the framework, the best actions to be undertaken can be identified.

3.3 Hazard Assessment

The hazard assessment provides a measure of the likelihood of the EWE analysed occurring in the area of interest. This measure can be based on a more or less quantitative approach. If the data available is limited or more general, or if the level of detail desired is relatively low, a qualitative approach might be sufficient, for example using hazard maps. In a more quantitative approach, more detailed data is required, and models for the specific hazard and area of interest can be developed. For example, the present-climate frequency of occurrence of EWEs may be estimated using reanalysis datasets (e.g. ERA-Interim/ERA5), model simulation ensembles of the current climate (hindcasts), observational datasets (e.g. E-OBS) and approaches based on a geographical information system (GIS). Predicted scenarios are also available to analyse future climate scenarios, such as greenhouse gas concentration scenarios of representative concentration pathway (RCP) 4.5, RCP 6.0 and RCP 8.5 for the period until the year 2100. Significant information relevant to the Irish context is available from Met Éireann's project TRANSLATE (Met Éireann, 2022a,b). Met Éireann is also leading the development of Ireland's National Frameworks for Climate Services (NFCS), which aims to coordinate, facilitate and strengthen the collaboration between climate information providers and users. The final likelihood measure obtained can depend on several factors that can be combined, such as the hazard itself and cascading hazards. For the risk matrix, both approaches can be used, and the measure obtained can then be standardised and assigned a likelihood score.

3.4 Vulnerability Assessment

Vulnerability encompasses susceptibility, exposure, coping and adaptive capacity as well as different thematic areas, such as physical, social, political, economic, environmental and institutional factors (Luskova *et al*., 2015). Vulnerability in this case can be seen as a state that exists within a system before it encounters a hazard event. Biophysical vulnerability can then be introduced, which considers both a physical component, related to the nature of the hazard and its physical impacts, and a biological/ social component, associated with the properties of the affected system that act to amplify or reduce the damage resulting from these impacts (Brooks, 2003). In particular, social vulnerability is taken into account and has been analysed considerably more in recent years as a crucial part of the vulnerability assessment. A general and widely applicable definition is provided in IPCC (2022), where vulnerability is defined as the "propensity or predisposition to be adversely affected and encompasses a variety of concepts and elements, including sensitivity or susceptibility to harm and lack of capacity to cope and adapt".

The concept of vulnerability is composed of three key factors:

- **Exposure (E):** the presence of people, livelihoods, environmental services and resources, infrastructure, economic, social or cultural assets in places that could be adversely affected (IPCC, 2012).
- **Susceptibility (S):** the deficiencies that indicate the likelihood of suffering harm and loss due to an adverse event (Luskova *et al.,* 2015); in this regard susceptibility is related to personal factors driving vulnerability, such as age and health.
- **Adaptive capacity (AC):** the combination of the strengths, attributes and resources available to an individual, community, society or organisation that can be used to prepare for and undertake actions to reduce adverse impacts and moderate harm, or exploit beneficial opportunities (IPCC, 2012). Specifically, adaptation capacity has a triple nature: ability to prepare, ability to respond and ability to recover.

Social vulnerability is part of the wider concept of vulnerability, which measures the potential adverse effects of climate change impacts on the environment and society. Social vulnerability describes those characteristics of the population that influence the capacity of the community to prepare for, respond to and recover from hazards and disasters. It helps to explain why some communities experience the hazard differently, despite experiencing the same level of flooding or storm surge inundation. Specifically, there will be certain categories of the population that will be more affected than others because of their personal status and well-being. Some of the main domains to consider are socioeconomic status (e.g. income, poverty, employment, education), household composition and disability (e.g. age, gender, single parenting, disability), minority status and language (e.g. race, ethnicity, language proficiency) and housing and transport (e.g. housing structure, crowding, vehicle access).

There are several ways to calculate and assess vulnerability, but one of the most common representations is in the form of a vulnerability index (VI). A VI is obtained through the definition and combination of a set of vulnerability indicators, which are representations of variables and characteristics decided at the beginning of the process. As defined in Cutter *et al*. (2008), vulnerability indicators are "quantitative measures intended to represent a characteristic or a parameter of a system of interest" using a single value, which are usually grouped into three categories related to exposure, susceptibility and adaptive capacity. Depending on, for example, the context, data availability, data reliability, expertise and level of detail, a number of vulnerability indicators can be identified for each category. The process of constructing VIs is described in Tate (2012).

Depending on data availability, level of detail desired and type of risk assessment, the vulnerability assessment can be based on a more or less quantitative approach. For the risk matrix approach, the vulnerability can be measured quantitatively, for example using a VI, or qualitatively, where more qualitative characteristics are analysed. Both processes result in a vulnerability value that can be standardised and assigned a vulnerability score. The final measure obtained can depend on several factors that can be combined, such as measures of exposure, susceptibility and adaptive capacity, social vulnerability factors and interdependencies.

3.5 Adaptation Planning and Risk Treatment

The last phase of the risk assessment framework focuses on decisions and actions to be taken based on the results obtained in the previous risk assessment phase. As mentioned above, different scenarios can be identified and analysed in the risk assessment process. For each scenario, a risk evaluation is carried out and results can then be compared. Scenarios with higher risk values are clearly of more concern than those with lower risk values. For example, when comparing the likelihood of two EWEs and their impact on a CI, the hazard that results in the higher risk value is the one that should be prioritised when planning actions. Similarly, when comparing the impact of the same hazard on different CIs or infrastructure elements, the scenario with the higher risk value identifies the most vulnerable CI. The focus will then be on analysing adaptive measures required to treat the risk and reduce the score to an acceptable risk value. Those scenarios with an acceptable risk value might not require any action. The categorisation of a risk value as acceptable or not will depend on the stakeholder who is implementing the risk assessment framework. A risk value that is considered acceptable by one organisation might not be acceptable to another, depending on the sensitivity of the infrastructure considered. The risk assessment framework also allows the comparison of scenarios where different adaptive measures are implemented, which helps the identification of the best and most efficient measure for the system being considered. It must be noted that, when comparing different adaptive measures, the measure resulting in the lowest risk value might appear to be the best one to be adopted. However, other factors must be considered. For example, costs and benefits are important aspects to take into account, since an adaptive measure might be very effective in reducing the risk but not cost efficient for the system considered. It is then recommended to perform a CBA to select the best adaptive measures. In addition, maladaptation needs to be considered, that is, when adaptation to climate change is actually harmful. This appears to be mainly caused by poorly designed adaptation strategies, for example because of a lack of awareness of what drives vulnerability to climate change or not understanding the wider development context (Schipper, 2020).

4 Data Availability, Requirements and Monitoring Regime

This chapter provides an overview of the identification of data currently available and the data required ideally and as a minimum to perform a climate impact risk assessment for Irish CIs. The current data availability is presented based on the findings of a literature review and stakeholder interaction, such as workshops and correspondence. The data requirements for the proposed framework are then presented, considering the data currently available and not available based on a gap analysis. At two workshops, “Data Availability and Data Requirements” and “Data Ongoing Monitoring and Security”, and through a survey distributed (Appendix B – Data Requirements) stakeholders were asked about various aspects of relevant and available data, such as hazard data, infrastructure data and spatial and temporal data of both hazards and infrastructures. In particular, queries were focused on relevant data and data requirements to evaluate hazard likelihood and assess vulnerability; data currently available, both within and outside the organisation; data currently not recorded, missing data or data gaps; data sharing issues; and sources of data.

4.1 Data Availability

In the development of a design for a full-scale study to assess the risk posed to CIs by climate change, gaining an understanding of the data that is currently available is an important step. Based on the data availability, a particular risk assessment methodology can be chosen. In fact, the development of a complex framework might not be suitable for organisations if the data required is too specific and not accessible. An overview of the data available allows a common framework suitable for the Irish sectors to be proposed, so it can be easily, accurately and successfully implemented by multiple organisations. The primary data of interest is related to three main categories, which include all the information required to implement a risk assessment (Chapter 3):

- **Hazard information:** general and detailed data on the hazard considered in order to estimate the probability of occurrence of the event and any potential cascading hazards.
- **Infrastructure characteristics:** general and detailed data on infrastructure characteristics, including current adaptation measures in place and interdependencies, in order to evaluate its vulnerability.
- **Features of the surrounding area:** surrounding area characteristics, such as topography and hydrology, that might influence the hazard and the infrastructure vulnerability, in addition to demographic data to consider social vulnerability aspects.

Feedback received during workshops and through responses from the survey distributed (Appendix B – Data Requirements) was important to understand the current data availability among stakeholders. However, for some data categories, it was not clear whether the data was available or not. In these cases, project partners used their engineering knowledge and judgement to draw conclusions.

4.1.1 Extreme weather events

Another survey (Appendix B – Extreme Weather Events) requested detailed information on EWEs and was subdivided into three sections: general information on the EWE, detailed data on the EWE and information on the surrounding area. Based on the responses and stakeholder interaction, it appears that most of the data related to EWEs is available, either openly or on request. A vast amount of data (on hourly, daily, monthly and annual scales) on EWEs and stations is openly provided on websites and portals, such as those listed in Table 4.1. EWE data can also be found in the form of hazard maps, which provide an estimate of the probability of hazard occurrence in certain areas.

Based on the responses obtained from the survey, the EWEs with the most detailed data available are storms, rainfall/first flush, snowfall, heat waves, cold weather and droughts. Data on landslides, sea level

Table 4.1. Extreme weather event data availability

Source	Available data
Met Éireann	Data related to EWEs such as rain, storms, snowfalls, heat waves, hail, cold events, strong wind, droughts, and data related to air flow, air pressure, temperature and humidity
Office of Public Works (OPW)	Data related to, for example, flood events, hydrometric stations, coastal tidal monitoring, hazard maps
Climate Ireland	Information on climate change and future projections
Geological Survey Ireland (GSI)	Data on, for example, coastal tidal monitoring, landslides, surrounding areas topography and hydrology, vegetation, deforestation, urbanisation, land use, soil properties and conditions
Teagasc – Agriculture and Food Development Authority	Data on, for example, surrounding areas topography and hydrology, vegetation, deforestation, soil properties and conditions
Marine Institute	Data related to, for example, ocean currents, sea level rise, waves and wind, coastal erosion
National Parks & Wildlife Service (NPWS)	Data on, for example, surrounding areas topography and hydrology, vegetation, deforestation, soil properties and conditions
Environmental Protection Agency (EPA)	Data from, for example, hydrometric stations and rain gauges

rise and coastal erosion appears to be more general, not readily available or not recorded at all. The other EWEs considered have an average availability of such data. It must be noted that some of these events can be difficult to record and predict. In general, hazard maps are a useful tool as an overall measure of the probability of occurrence of an event, but it is recognised that these are relatively difficult to develop for some events.

An interesting Met Éireann project currently ongoing is TRANSLATE (Met Éireann, 2022a,b). This project aims to standardise national climate projections for Ireland and develop climate services to meet the Irish adaptation sector's climate information requirements. The TRANSLATE project also looks into the problem of sector-specific data, analysing how and if this data is useful or applicable to other sectors.

4.1.2 Critical infrastructures

Based on the stakeholders' interaction and direct communication with some organisations, the findings can be summarised as follows:

- Data related to infrastructures is usually recorded by the responsible organisation and stored within the organisation.
- Data is internally available, although the data might be saved in different datasets using different software for different departments within the organisation; there might be duplication of data between different departments, potentially causing inconsistencies; data might be incomplete and have gaps.
- Desired data from other organisations might be obtained, or not, depending on the related organisation: public bodies share most of their data, whereas private bodies share limited or no information and mainly only on request.

The survey distributed requested detailed information in relation to CIs and their surroundings. In particular, the data referred to general information on the CI; detailed information on the CI; information on location and surroundings; and data on maintenance and monitoring. The responses were limited and at times incomplete, so conclusions on the availability of CI data are provided from a more general point of view. It is important to highlight that a key barrier to a cross-sectoral risk assessment is the lack of data sharing among organisations. Therefore, it is important to recognise that, although data might be available, it is not often accessible, and some data is not recorded and available at all. In relation to CIs, data that is currently limited appears to be related to quay walls and retaining walls, ICT networks and waste energy. For other infrastructure sectors, it is unclear how much and what data is recorded, for example for ports and airports, emergency infrastructures and services, industries, supply chains, oil networks and wind farms. It must be noted that it was often highlighted during stakeholder interactions that emergency infrastructures, emergency services and supply chains are quite important infrastructures/services during an emergency, so data related to these would be considered particularly relevant.

For the infrastructures where data is recorded and available, it is worth noting that:

- Although most of the data is available, it might be not properly organised and might be recorded in different software for different departments, include gaps and be inconsistent.
- Some information is available but might be difficult to retrieve for some infrastructures, for example data on adaptation measures in place.
- Although some information is known by stakeholders, it is not actively recorded, for example the redundancy of an infrastructure, or the relevance of the infrastructure in the event of disruption.

These findings are summarised in Table 4.3 at the end of this chapter, and additional details on the data included in the survey are available in Appendix B – Critical Infrastructure.

4.2 Data Requirements

To properly implement a design for a full-scale study to assess the risk posed to CIs it is important to possess the necessary data. After assessing the data that is currently available to stakeholders, it is possible to adapt the methodology proposed so that it can be applied by stakeholders in the Irish context. Based on the methodology, a list of data required was developed and through gap analysis the missing data was identified. New monitoring systems or data sources should be implemented to gather the missing data.

An overview of the potential data requirements was developed and distributed to the stakeholders as a survey. The data requirements can be divided into three main categories: hazard information, infrastructure characteristics, and features of the surrounding area. For both EWEs and CIs, subcategories can also be identified, as listed in Table 4.2. Data related to aspects of the surrounding area contributes to both EWE and CI categories.

The categorisation aims to help stakeholders to easily identify the data required on a case-by-case basis. Each of these subcategories consists of various input data, which depends on the EWE and CI being considered. The specific data required may also vary depending on the level of detail of the risk assessment, which can be more qualitative or quantitative. For a qualitative risk assessment, more general data might be sufficient. For a quantitative assessment, the methodologies applied usually require specific types of detailed data.

Table 4.2. General data requirements for extreme weather events and critical infrastructures

Category	Subcategory
EWE	General data
	Detailed data
	Surrounding area data
CI	Infrastructure general data
	Infrastructure detailed data
	Data on location and surroundings
	Data on maintenance and monitoring

The list of data required was based on a literature review, engineering judgement and feedback received from stakeholders. The data required might be more or less detailed depending on the stakeholder and the purpose of the risk assessment, so it is recommended that the list of data required is revised and adapted by stakeholders as needed. In order to obtain a significant and relevant outcome from the process, however, a minimum amount of data is required. In general, a qualitative risk assessment requires more general and qualitative data, which is often available or easily accessible. The minimum data required for an EWE might be hazard maps and future climate change predictions, which might be sufficient to carry out a qualitative risk assessment. For a quantitative risk assessment, relevant measured data and/or historical data, together with information on the surrounding area, are required to be able to properly model the event. Regarding CI data, the minimum data required is mostly available within the organisation responsible for the infrastructure. However, if interdependencies are taken into account, access to other organisations' data is usually necessary. For both qualitative and quantitative risk assessments, the minimum amount of data would be the amount sufficient to properly assess the criticality and vulnerability of the infrastructure, together with social vulnerability.

4.3 Monitoring Regime

In this section, stakeholders' feedback on the proposed monitoring regime is presented, with particular focus on the data not available. A review of existing monitoring systems was also carried out to establish how to obtain the data required. Analysis of the data suggested that most of the data required to perform a risk assessment is currently available to stakeholders, with some exceptions. In addition, based on the outcome of stakeholder interaction, it appears that stakeholders are satisfied with their current level of monitoring and would not consider adopting new systems, unless they would lead to a substantial benefit for the infrastructure and reduce the related risk. The following conclusions on the monitoring regime proposed for infrastructure owners can be made:

- Data available should be reviewed and audited by data owners to determine what data is actually available, in what format and its arrangement
- Although most data appears to be available, gaps and inconsistencies are still a concern in the datasets of infrastructure owners, so efforts should be made to close these gaps and rearrange the dataset to a more unified dataset in order to avoid data repetition and inconsistencies.
- Where data is unavailable, it is recommended that monitoring systems are implemented to collect the data or to process data already collected to make it readily available.
- For most EWEs, it appears that most of the general data required is recorded, so it is recommended that the current efficient and up-to-date systems are maintained. Data available for EWEs can often be more general and might not be accurate for a particular location of interest. If a more precise and quantitative assessment is desired, monitoring specific to the area of interest might be required to develop accurate models.
- Some EWEs (e.g. landslides) might not have much data recorded or directly accessible. If these hazards are particularly relevant to the infrastructure considered, additional monitoring might need to be considered.
- For CIs, it appears that stakeholders have sufficient data within their organisations to perform a risk assessment, although at times some information might not be recorded. If a more detailed risk assessment is desired, additional monitoring might be required.
- A key issue is data sharing, the lack of which could prevent the performance of a cross-sectoral risk assessment. It is recommended that potential solutions, as presented in Chapter 5, are discussed and that infrastructure owners in Ireland reach an agreement to share relevant data.

Table 4.3. Stakeholders' feedback on critical infrastructures

CI	Relevant organisation	Data availability	Data sharing arrangement	Comments
Bridges/ culverts	Local authorities Irish Rail TII DoT	Most or all data available	Local authorities – openly shared, some data shared on request Irish Rail – limited data shared on request TII – limited data shared on request[a] DoT – limited data shared on request[a]	Each organisation possesses data on its own assets Not clear what and how much data can be shared by Irish Rail, TII and DoT**
Tunnels	Local authorities TII	Most or all data available	Local authorities – openly shared, some data shared on request TII – limited data shared on request[a]	Not clear what and how much data can be shared by TII[b]
Quays and retaining walls	Local authorities	Data limited but being collected	Local authorities – openly shared, some data shared on request	
Road network	Local authorities TII DoT	Most or all data available	Local authorities – openly shared, some data shared on request TII – limited data shared on request[a] DoT – limited data shared on request[a]	Not clear what and how much data can be shared by TII and DoT[b]
Railway network	Irish Rail TII	Most or all data available	Irish Rail – limited data shared on request[a] TII – limited data shared on request[a]	Not clear what and how much data can be shared by TII and Irish Rail[b]
Slopes/ embankments	Local authorities Irish Rail TII	Most or all data available	Local authorities – openly shared, some data shared on request Irish Rail – limited data shared on request[a] TII – limited data shared on request[a]	Not clear what and how much data can be shared by TII and Irish Rail[b]
Ports	Port companies	Amount of data available not clear[b]	Limited data shared on request[a]	Dublin Port Company Shannon Foynes Port Port of Cork
Airports/ heliports	Airport companies	Amount of data available not clear[b]	Limited data shared on request[a]	Dublin Airport Authority Cork Airport Shannon Airport Ireland West Airport Knock
Emergency infrastructure and services	Not applicable[c]	Not applicable[c]	Not applicable[c]	Potentially available to Department of Defence and Department of Housing
Buildings	Local authorities	Data partially available	Local authorities – openly shared, some data shared on request	Local authorities possess data only on their own assets. Data might be incomplete
Water network	Irish Water OPW Waterways Ireland	Data partially available	Irish Water – limited data shared on request[a] OPW – openly shared, some data shared on request Waterways Ireland – not applicable[c]	Some data is incomplete and shared data requires assessment

Table 4.3 Continued

CI	Relevant organisation	Data availability	Data sharing arrangement	Comments
Electricity	EirGrid ESB	Not applicable[c]	Not applicable[c]	
ICT network	Local authorities Eir	Data limited	Local authorities – openly shared, some data shared on request Eir – not applicable[c]	Local authorities possess data only on their own assets. Data might be very limited
Gas network	Gas Network Ireland	Most or all data available	Mostly not shared, only some general data shared on request	
Waste energy	Local authorities Covanta	Data limited	Local authorities – openly shared, some data shared on request Covanta – not applicable[c]	Local authorities possess data only on their own assets
Industries	Not applicable[c]	Not applicable[c]	Not applicable[c]	Not applicable[c]
Supply chains	Not applicable[c]	Not applicable[c]	Not applicable[c]	Not applicable[c]
Oil network	Not applicable[c]	Not applicable[c]	Not applicable[c]	Not applicable[c]
Wind farms	Not applicable[c]	Not applicable[c]	Not applicable[c]	Not applicable[c]

[a]Limited data shared on request: data is not publicly available but shared only on request; not all data requested is shared but data is usually filtered and selected on a case-by-case basis.

[b]Not clear: the information obtained during the project on this data was limited, so conclusions are uncertain.

[c]Not applicable: not enough information was provided during the project to make conclusions on this data.

DoT, Department of Transport; ESB, Electricity Supply Board; OPW, Office of Public Works; TII, Transport Infrastructure Ireland.

5 Cross-sectoral Data Sharing Issues

This chapter provides an overview of the data sharing issues, potential existing methodologies to overcome security issues and security concerns of cross-sectoral data usage. In the context of this project, the objective is to provide recommendations for reducing and potentially removing any safety concerns that could affect the implementation of a multi-sectoral risk assessment in Ireland. Based on the literature review, engineering judgement and stakeholder interaction, a series of concerns related to data sharing have been identified (Table 5.1) but there are also many reasons why data sharing should be taken into consideration by stakeholders, so a series of benefits are listed in Table 5.2.

Data can be shared in different ways, such as through direct contact between organisations, or indirectly through a platform. In the case where a

Table 5.1. Main data sharing concerns for the Irish context

Data sharing concern		Description
Misuse and misinterpretation of data	Misuse of data	Data might be used by third parties that are not aware of the type, assumptions, accuracy, restrictions or reasons for the collection of such data
	Misinterpretation of data shared	Data might be misinterpreted if shared without proper clarifications and explanatory documentation (e.g. inaccurate data as a result of a sensor malfunction)
	Improper reuse of data	Data might be duplicated for secondary use. This behaviour, even if not deliberate, leads to decreased reliability of and level of confidence in the decision made
Effort and costs	Effort to have reusable data	Particular effort is required before sharing data in order to have reusable data (e.g. management of the data and production of explanatory documentation)
	Compatibility of data	Different available formats and non-interoperability of software might make data unusable/not shareable. Particular effort is required to make data compatible
	Collection process	The collection process can vary case by case, making it difficult to have consistent and standardised data
	Storage	The increasing amount of data collected as a result of the number/typology of sensors along with IT sector improvements has increased the need for storage
	Platform for sharing	Building a platform to share data can be expensive, in terms of protocols, framework, infrastructure and costs associated with the maintenance of the platform, equipment, personnel and training
	Funding	Lack of funding can obstruct effective data sharing
Advantages and recognition	Maintaining competitive advantages	Shared data might represent an advantage to competitors
	Protecting future publications	Data shared at earlier stages of the project might influence future publications
	Ownership of data collected/elaborated	Stakeholders spend time and resources on collecting data and processing it, so data might not be shared because of the lack of acknowledgement
	Incorrect or insufficient citation	Incorrect or insufficient citation/acknowledgement represents another obstacle to data sharing
	Expectation of future collaboration	Sharing data might be dependent on the expectation of future collaboration or receiving data in return
Regulations	Regulations/law/ internal policies	Regulations and policies on data sharing can sometimes be unclear in terms of practices
Sensitive information	Disclosure of sensitive and private information	One of the biggest issues is sharing sensitive and private information that could cause security issues

IT, information technology.

Table 5.2. Data sharing benefits

Data sharing benefit	Description
Scientific and educational benefits	Data sharing makes large amounts of data available, which can lead to progress in the research field
Re-analysis of data by others	Researchers and scientists can re-analyse previously collected data to improve data quality and can use different approaches/techniques to discover new knowledge or make breakthroughs
Access to data from other organisations	Access to data made available by others allows a more complete and exhaustive set of data for a more accurate analysis. Data would ideally be publicly available so that any researcher or scientist could use it freely
Time and cost reduction	Data sharing helps to reduce costs and the time related to collection of data, specifically if the data has already been collected by other organisations
Elimination of data gaps and duplicated data	Data collected and processed by others can be accessible, avoiding duplication of data. Integration of data from different organisations might help eliminate data gaps
Verification, reproduction and refinement of data	By sharing and comparing data that has already been collected by others, data can be verified, reproduced and refined
Guarding against research fraud	The adoption of a unified framework/platform reduces the chance of fraud, from malpractice to falsification of data, which impacts data validity
Building trust in other agencies	Some data could be useful to other agencies/organisations, and sharing it would help build trust among them and lead to new collaborations
Formulation of policies	Data sharing helps reduce costs, which can help the private and public sectors to formulate long- and short-term policies (Chawinga and Zinn, 2019)

platform is used, there might be different settings and configuration options, for example the adoption of:

- an open-source cloud system/platform so that all data is available and freely accessible;
- an open-source cloud system/platform where only non-sensitive data is available and accessible freely; sensitive data can be accessed through requests and based on signed agreements and disclaimers;
- a restricted access cloud system or platform where all or some data is available for a limited group of organisations/bodies, subject to agreements and disclaimers;
- a restricted access cloud system or platform where some data can be accessed through requests and based on signed agreements and disclaimers; sensitive data is not shared through the platform.

The best option for the group of platform users should be based on a consultation with the various stakeholders and data owners through, for example, a Delphi panel or a brainstorming session, so that all relevant stakeholders would be involved in deciding what data is to be restricted. In the case of restricted access, the adoption of a system to control the access is required, for example through a formal request/email or through a more restricted implementation of privileged access management (or PAM). The control of access might be implemented with role-based access control (or RBAC), where the access is based on the user's role in order to restrict their potential use of the data, or with the adoption of electronic signatures/IDs. Where different users can access the platform, the access to data and any other kind of usage can also be monitored. In addition, security concerns can also be addressed by encrypting data to make it unreadable, for example when data is obtained illegally. From a cybersecurity perspective, such as for personal and sensitive data, encryption of data is highly recommended. Encryption or two-step authentication, which has already been adopted by some applications and cloud services, is typically the best solution to adopt to ensure the safe transfer of data.

Frameworks and processes to build a safe data sharing structure, however, come with costs in terms of time and resources, such as those related to staff training. Unfortunately, there is no easy solution to reducing the costs and time required to implement a suitable data sharing system. Yet, the development of the IT sector provides many solutions for data sharing. Many are storage solutions for collecting data, for example a physical–cloud or cloud-only system, which have huge storage options and capacity ranges.

Concerns about and the benefits of data sharing and possible solutions for a safe sharing system were introduced to relevant stakeholders through a workshop. The following findings are based on stakeholders' comments recorded during the workshop:

- Public bodies have an open view on data sharing and already share most or all of the data available. Data on weather events is publicly available online and can be obtained from different websites. Local authorities share any type of data on request.
- Private bodies have more control over what data they can and want to share and usually tend to restrict data sharing. On request, some data might be shared with individuals or for construction works, but that is limited to only the minimum necessary.
- Data might be requested in general by private owners (e.g. for insurance purposes), consultants and designers, other organisations (e.g. universities for research projects) and journalists.
- Data sharing concerns are mostly related to sensitive data, such as infrastructure criticality or personal information. In particular, the concerns centre around the potential security issues resulting from sensitive data being shared, the misuse and misinterpretation of data and the potential legal consequences of data sharing.
- Usually, agreements and disclaimers would be signed by the data receiver to protect the data provider from any responsibility if the data is not accurate (e.g. in the case of a sensor malfunction), and information related to the assumed use of the data is also provided. The GDPR (General Data Protection Regulation) is also considered when it comes to individual private owners and related elements.
- A key point for data sharing is knowing the reason why the data needs to be shared. In general, there is a certain level of security risk in sharing all data. Sharing is usually not a problem for general information, but organisations might not want to share more sensitive data: for example, organisations might not want to highlight certain assets of a critical nature. Often, the amount and type of data being shared by organisations are dependent on its assumed use and the subsequent potential risk of its use. Answering the question "Why gather critical information and what is its use?" might help find common ground and agreement on how data security concerns might be addressed. So, the reasons why the information needs to be brought together and the uses that it would be put to could potentially lead to changes in what, where and how data is shared.
- An achievable and common solution for the future requires agreements between organisations on what and how data should be used and shared. Agreements and disclaimers should be put in place to protect the organisations from any potential misuse of data and legal consequences and to make sure that data is not shared with third parties. For private bodies, sharing data publicly or on an open-source platform is not a feasible option. A platform giving limited access to a selected group of users, such as asset owners, would be a more acceptable solution. Before sharing data, especially if sensitive, the reasons for sharing and the uses of the data need to be made clear and agreed. For example, a suitable data sharing agreement could be found in the case of government task forces coordinating emergency planning on a national level, which are subject to increased levels of security.
- Overall, a platform including all information, general and sensitive, necessary to implement a cross-sectoral risk assessment framework for a full-scale study needs to be recognised as safe and reliable by stakeholders. In addition, the reasons for and uses of data available on the platform need to be made clear and agreed. Ideally, a platform accessible to all stakeholders would be preferable, overseen and managed by central government, with a stakeholder group representing all relevant government departments set up to oversee its development and implementation.

6 Cost Estimation

Implementing a risk assessment for a full-scale study can certainly provide benefits in identifying the most critical infrastructures and the most threatening hazards, and potential actions to be taken to reduce their risk. However, the implementation of the framework itself will incur costs for the infrastructure owner/manager. These costs could be related to:

- **data:** the purchase/installation/maintenance of monitoring systems to record data, software to process data, software for the organisation and management of data, and the recovery of data internally and from other organisations;
- **labour:** the time spent by the organisation in implementing the framework, which would include the time taken to gather/process/organise/manage data and to carry out each step of the risk assessment framework (Chapter 3), the resources required (whether in-house or from external providers) and the time spent interacting with other organisations and sectors.

The cost associated with the implementation of a full-scale study could vary a lot depending on the type of risk assessment being carried out. The costs involved are mainly influenced by the level of detail that is sought. A simpler, qualitative and more general risk assessment would involve more general data that is often already available, limited data processing, reduced labour time and simplified scenarios. A quantitative and more detailed risk assessment would instead involve more accurate and specific data, which might require the installation of monitoring systems, more complicated data processing, with potentially the need for specific modelling and additional software, hiring independent professionals with specific expertise, interactions with other organisations/sectors, and a greater amount of and more complex risk assessment scenarios.

An estimation of the cost associated with the implementation of a full-scale study is a task that would depend on several factors and information that was not available during the INFRALINC project. It is, however, recommended that, before commencing the framework implementation, the organisation should carry out a cost estimation to assess the potential costs involved. This would allow the organisation to adjust the level of detail of the risk assessment being carried out to match the budget available. It is also recommended to carry out the risk assessment in accordance with the forthcoming National Climate Change Risk Assessment, as referred to in the Climate Action Plan 2023 (Government of Ireland, 2023a), in order to avoid duplication of effort and make more efficient use of resources.

7 Conclusions

This report summarises the work done for the INFRALINC project. The findings, conclusions and recommendations of the project are listed below:

- It is expected that the frequency and intensity of EWEs will increase as a result of climate change.
- The effects of cascading hazards and the interdependencies between infrastructure assets should be considered in the risk assessment framework.
- Social vulnerability, in addition to infrastructure vulnerability, should be considered in the risk assessment process.
- An overarching methodology was proposed, based on an extensive literature review and by taking into account what is currently used by relevant stakeholders in Ireland and what features are best suited to the Irish context.
- The risk assessment approach adopted should consider the ease of implementation of the method and the necessary flexibility of the approach, considering the existing potential limitations to carrying out an assessment (e.g. data availability, available resources).
- While a quantitative risk assessment approach is recommended, it requires more detailed data than is typically available at present. Equally, a lot of the data is stored in disparate locations and formats, and it would be beneficial to standardise approaches to data formats and storage across organisations.
- A cross-sectoral framework to be used by multiple sectors would allow the comparison of risk values between sectors and would need to be standardised and agreed among stakeholders.
- The data necessary to perform the risk assessment approach is more or less available depending on the type of data, its ownership and sharing limitations and the organisation of the data itself.
- Monitoring regimes need to be specific to the data required and the level of detail desired.
- Data sharing is an issue because of concerns that sensitive data could be misused and/or misinterpreted.
- A common platform including all the data necessary to implement a cross-sectoral risk assessment framework for a full-scale study would require the involvement of central government and related departments to ensure that the platform is secure and offers users no commercial advantage.
- Before commencing the implementation of the framework, the organisation should carry out a cost estimation to assess the potential costs involved, in order to adjust the level of detail of the risk assessment carried out to match the budget available.

References

Adey, B., Hackl, J., Heitzler, M. and Iosifescu, I., 2014. *INFRARISK Deliverable D4.1: Preliminary Model, Methodology and Information Exchange*. INFRARISK.

Brooks, N., 2003. *Vulnerability, Risk and Adaptation: A Conceptual Framework*. Tyndall Centre for Climate Change Research, Norwich, UK.

Chawinga, W.D. and Zinn, S., 2019. Global perspectives of research data sharing: a systematic literature review. *Library and Information Science Research* 41(2): 109–122.

Cutter, S.L. *et al*., 2008. A place-based model for understanding community resilience to natural disasters. *Global Environmental Change* 18(4): 598–606.

Department of Agriculture, Food and the Marine, 2019. *Agriculture, Forest and Seafood – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

Department of Communications, Climate Action and Environment, 2018a. *National Adaptation Framework*. Government of Ireland.

Department of Communications, Climate Action and Environment, 2018b. *Sectoral Planning Guidelines for Climate Change Adaptation*. Government of Ireland.

Department of Communications, Climate Action and Environment, 2019. *Electricity & Gas Networks Sector – Climate Change Adaptation Plan*. Government of Ireland.

Department of Culture, Heritage and the Gaeltacht, 2019a. *Biodiversity – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

Department of Culture, Heritage and the Gaeltacht, 2019b. *Built & Archaeological Heritage – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

Department of Defence, 2017. *Strategic Emergency Management: National Structures and Framework* Government of Ireland.

Department of Defence, 2021a. *Strategic Emergency Management – Guideline 3: Critical Infrastructure Resilience (Version 2)*. Government of Ireland.

Department of Defence, 2021b. *National Risk Assessment for Ireland 2020*. Government of Ireland.

Department of Health, 2019. *Health – Climate Change Sectoral Adaptation Plan 2019–2024*. Government of Ireland.

Department of Housing, Local Government and Heritage, 2010. *A Framework for Major Emergency Management – A Guide to Risk Assessment in Major Emergency Management*. Government of Ireland.

Department of Housing, Planning and Local Government, 2019. *Water Quality and Water Services Infrastructure – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

Department of the Taoiseach, 2018. *National Risk Assessment 2021/2022 – Overview of Strategic Risks*. Government of Ireland.

Department of the Taoiseach, 2023. *National Risk Assessment 2023 – Overview of Strategic Risk*. Government of Ireland.

Department of Transport, Tourism and Sport, 2019. *Transport – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

EU (European Union), 2008. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345, 23.12.2008, p. 75–82.

Government of Ireland, 2020. A National Risk Assessment for Ireland 2020. Office of Emergency Planning, Government of Ireland.

Government of Ireland, 2023a. *Climate Action Plan 2023 (CAP23) – Changing Ireland for the Better*. Government of Ireland.

Government of Ireland, 2023b. *Climate Action Plan 2023 – Annex of Actions*. Government of Ireland.

IPCC (Intergovernmental Panel on Climate Change), 2012. *Managing the Risks of Extreme Events and Disasters to Advance Climate.* Cambridge University Press, Cambridge, UK.

IPCC (Intergovernmental Panel on Climate Change), 2022. *Climate Change 2022: Impacts, Adaptation and Vulnerability*. Cambridge University Press, Cambridge, UK.

ISO (International Organization for Standardization), 2018. ISO 31000:2018. Risk Management – Guidelines. International Organization for Standardization, Geneva, Switzerland.

ISO (International Organization for Standardization), 2019. *ISO 31010:2019.* Risk Management – Risk Assessment Techniques. International Organization for Standardization, Geneva, Switzerland.

Luskova, M., Titko, M., Bianchizza, C. and Prak, P., 2015. *RAIN D3.4: Methodology for Measuring Societal Vulnerability due to Failure of Critical Land Transport Infrastructure Elements*. RAIN Project.

Met Éireann, 2022a. TRANSLATE – Introduction to TRANSLATE. Available online: https://www.met.ie/science/translate (accessed 8 February 2023).

Met Éireann, 2022b. TRANSLATE project to standardise future climate information for Ireland. Available online: https://www.met.ie/translate-project-to-standardise-future-climate-information-for-ireland (accessed 8 February 2023).

Office of Public Works, 2019. *Flood Risk Management – Climate Change Sectoral Adaptation Plan*. Government of Ireland.

Schipper, E.L.F., 2020. Maladaptation: when adaptation to climate change goes very wrong. *One Earth* 3(4): 409–414.

Sventekova, E. *et al*., 2015. *RAIN D3.2: Defining Critical Land Transport Infrastructure Protection Methods*. RAIN Project.

Tate, E., 2012. Social vulnerability indices: a comparative assessment using uncertainty and sensitivity analysis. *Natural Hazards* 63(2): 325–347.

Abbreviations

CBA	Cost–benefit analysis
CI	Critical infrastructure
EPA	Environmental Protection Agency
EU	European Union
EWE	Extreme weather event
ICT	Information and communications technology
INFRALINC	Infrastructure Climate Change Risk Considering Interdependencies and Cascading Hazards
IT	Information technology
TII	Transport Infrastructure Ireland
VI	Vulnerability index

An Ghníomhaireacht Um Chaomhnú Comhshaoil

Tá an GCC freagrach as an gcomhshaol a chosaint agus a fheabhsú, mar shócmhainn luachmhar do mhuintir na hÉireann. Táimid tiomanta do dhaoine agus don chomhshaol a chosaint ar thionchar díobhálach na radaíochta agus an truaillithe.

Is féidir obair na Gníomhaireachta a roinnt ina trí phríomhréimse:

Rialáil: Rialáil agus córais chomhlíonta comhshaoil éifeachtacha a chur i bhfeidhm, chun dea-thorthaí comhshaoil a bhaint amach agus díriú orthu siúd nach mbíonn ag cloí leo.

Eolas: Sonraí, eolas agus measúnú ardchaighdeáin, spriocdhírithe agus tráthúil a chur ar fáil i leith an chomhshaoil chun bonn eolais a chur faoin gcinnteoireacht.

Abhcóideacht: Ag obair le daoine eile ar son timpeallachta glaine, táirgiúla agus dea-chosanta agus ar son cleachtas inbhuanaithe i dtaobh an chomhshaoil.

I measc ár gcuid freagrachtaí tá:

Ceadúnú

- Gníomhaíochtaí tionscail, dramhaíola agus stórála peitril ar scála mór;
- Sceitheadh fuíolluisce uirbigh;
- Úsáid shrianta agus scaoileadh rialaithe Orgánach Géinmhodhnaithe;
- Foinsí radaíochta ianúcháin;
- Astaíochtaí gás ceaptha teasa ó thionscal agus ón eitlíocht trí Scéim an AE um Thrádáil Astaíochtaí.

Forfheidhmiú Náisiúnta i leith Cúrsaí Comhshaoil

- Iniúchadh agus cigireacht ar shaoráidí a bhfuil ceadúnas acu ón GCC;
- Cur i bhfeidhm an dea-chleachtais a stiúradh i ngníomhaíochtaí agus i saoráidí rialáilte;
- Maoirseacht a dhéanamh ar fhreagrachtaí an údaráis áitiúil as cosaint an chomhshaoil;
- Caighdeán an uisce óil phoiblí a rialáil agus údaruithe um sceitheadh fuíolluisce uirbigh a fhorfheidhmiú
- Caighdeán an uisce óil phoiblí agus phríobháidigh a mheasúnú agus tuairisciú air;
- Comhordú a dhéanamh ar líonra d'eagraíochtaí seirbhíse poiblí chun tacú le gníomhú i gcoinne coireachta comhshaoil;
- An dlí a chur orthu siúd a bhriseann dlí an chomhshaoil agus a dhéanann dochar don chomhshaol.

Bainistíocht Dramhaíola agus Ceimiceáin sa Chomhshaol

- Rialacháin dramhaíola a chur i bhfeidhm agus a fhorfheidhmiú lena n-áirítear saincheisteanna forfheidhmithe náisiúnta;
- Staitisticí dramhaíola náisiúnta a ullmhú agus a fhoilsiú chomh maith leis an bPlean Náisiúnta um Bainistíocht Dramhaíola Guaisí;
- An Clár Náisiúnta um Chosc Dramhaíola a fhorbairt agus a chur i bhfeidhm;
- Reachtaíocht ar rialú ceimiceán sa timpeallacht a chur i bhfeidhm agus tuairisciú ar an reachtaíocht sin.

Bainistíocht Uisce

- Plé le struchtúir náisiúnta agus réigiúnacha rialachais agus oibriúcháin chun an Chreat-treoir Uisce a chur i bhfeidhm;
- Monatóireacht, measúnú agus tuairisciú a dhéanamh ar chaighdeán aibhneacha, lochanna, uiscí idirchreasa agus cósta, uiscí snámha agus screamhuisce chomh maith le tomhas ar leibhéil uisce agus sreabhadh abhann.

Eolaíocht Aeráide & Athrú Aeráide

- Fardail agus réamh-mheastacháin a fhoilsiú um astaíochtaí gás ceaptha teasa na hÉireann;
- Rúnaíocht a chur ar fáil don Chomhairle Chomhairleach ar Athrú Aeráide agus tacaíocht a thabhairt don Idirphlé Náisiúnta ar Ghníomhú ar son na hAeráide;
- Tacú le gníomhaíochtaí forbartha Náisiúnta, AE agus NA um Eolaíocht agus Beartas Aeráide.

Monatóireacht & Measúnú ar an gComhshaol

- Córais náisiúnta um monatóireacht an chomhshaoil a cheapadh agus a chur i bhfeidhm: teicneolaíocht, bainistíocht sonraí, anailís agus réamhaisnéisiú;
- Tuairiscí ar Staid Thimpeallacht na hÉireann agus ar Tháscairí a chur ar fáil;
- Monatóireacht a dhéanamh ar chaighdeán an aeir agus Treoir an AE i leith Aeir Ghlain don Eoraip a chur i bhfeidhm chomh maith leis an gCoinbhinsiún ar Aerthruailliú Fadraoin Trasteorann, agus an Treoir i leith na Teorann Náisiúnta Astaíochtaí;
- Maoirseacht a dhéanamh ar chur i bhfeidhm na Treorach i leith Torainn Timpeallachta;
- Measúnú a dhéanamh ar thionchar pleananna agus clár beartaithe ar chomhshaol na hÉireann.

Taighde agus Forbairt Comhshaoil

- Comhordú a dhéanamh ar ghníomhaíochtaí taighde comhshaoil agus iad a mhaoiniú chun brú a aithint, bonn eolais a chur faoin mbeartas agus réitigh a chur ar fáil;
- Comhoibriú le gníomhaíocht náisiúnta agus AE um thaighde comhshaoil.

Cosaint Raideolaíoch

- Monatóireacht a dhéanamh ar leibhéil radaíochta agus nochtadh an phobail do radaíocht ianúcháin agus do réimsí leictreamaighnéadacha a mheas;
- Cabhrú le pleananna náisiúnta a fhorbairt le haghaidh éigeandálaí ag eascairt as taismí núicléacha;
- Monatóireacht a dhéanamh ar fhorbairtí thar lear a bhaineann le saoráidí núicléacha agus leis an tsábháilteacht raideolaíochta;
- Sainseirbhísí um chosaint ar an radaíocht a sholáthar, nó maoirsiú a dhéanamh ar sholáthar na seirbhísí sin.

Treoir, Ardú Feasachta agus Faisnéis Inrochtana

- Tuairisciú, comhairle agus treoir neamhspleách, fianaise-bhunaithe a chur ar fáil don Rialtas, don tionscal agus don phobal ar ábhair maidir le cosaint comhshaoil agus raideolaíoch;
- An nasc idir sláinte agus folláine, an geilleagar agus timpeallacht ghlan a chur chun cinn;
- Feasacht comhshaoil a chur chun cinn lena n-áirítear tacú le hiompraíocht um éifeachtúlacht acmhainní agus aistriú aeráide;
- Tástáil radóin a chur chun cinn i dtithe agus in ionaid oibre agus feabhsúchán a mholadh áit is gá.

Comhpháirtíocht agus Líonrú

- Oibriú le gníomhaireachtaí idirnáisiúnta agus náisiúnta, údaráis réigiúnacha agus áitiúla, eagraíochtaí neamhrialtais, comhlachtaí ionadaíocha agus ranna rialtais chun cosaint chomhshaoil agus raideolaíoch a chur ar fáil, chomh maith le taighde, comhordú agus cinnteoireacht bunaithe ar an eolaíocht.

Bainistíocht agus struchtúr na Gníomhaireachta um Chaomhnú Comhshaoil

Tá an GCC á bainistiú ag Bord lánaimseartha, ar a bhfuil Ard-Stiúrthóir agus cúigear Stiúrthóir. Déantar an obair ar fud cúig cinn d'Oifigí:

1. An Oifig um Inbhunaitheacht i leith Cúrsaí Comhshaoil
2. An Oifig Forfheidhmithe i leith Cúrsaí Comhshaoil
3. An Oifig um Fhianaise agus Measúnú
4. An Oifig um Chosaint ar Radaíocht agus Monatóireacht Comhshaoil
5. An Oifig Cumarsáide agus Seirbhísí Corparáideacha

Tugann coistí comhairleacha cabhair don Ghníomhaireacht agus tagann siad le chéile go rialta le plé a dhéanamh ar ábhair imní agus le comhairle a chur ar an mBord.