An Roinn Cosanta
Department of Defence

Strategic Emergency Management

Guideline 3 - Critical Infrastructure Resilience (Version 2)

TABLE OF CONTENTS

List of Figures

List of Tables

SUMMARY

A modern State depends on multiple types of infrastructure, some of which are Critical Infrastructure (CI) .CI is defined as an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of the people and the disruption or destruction of which would have a significant impact in the State as a result of failure to maintain those functions. CI provides services and utilities in order to facilitate efficient functioning of the economy, the safety and wellbeing of its citizens and the continual functioning of government. Citizens of Ireland expect that CI of the State will function efficiently and when disrupted that those services will be restored as quickly as possible. The importance to a State of resilient CI is well understood. However, more recently there is an increasing complexity, dependency and interdependency within and between CI. This potentially poses risks to society that need to be identified and evaluated. This Guideline Document offers guidance to Government Departments and Agencies, and public and private operators of essential services, on how to identify what is CI, how to evaluate/quantify the criticality of the disruption or destruction of that CI and provides a framework of measures to improve resilience of CI. This Guideline adopts a risk based approach that is societal centric, and is focused on the impact of the loss of services to Irish society rather than on the losses incurred to the owner or operator of that service.

PART ONE outlines the background and purpose of this Guideline Document, including important terminology and definitions used throughout. It introduces the understanding of National Infrastructure and Lead Government Department (LGD) principles in relation to their responsibility to Sectors and Sub-Sectors. In addition, it also provides an explanation of the Irish, EU and international context with regard to Critical Infrastructure Resilience (CIR).

PART TWO outlines a methodology for identifying CI and the process for evaluating and quantifying disruption impacts, taking into account measures already in place to mitigate against risk. This methodology introduces the Criticality Metrics, the use of Impact Factors within the categories of Scope, Severity and Time Related, and finally the Criticality Score. This allows for the evaluation (based on the Criticality Score) of the impact of the disruption or destruction of a service provided by CI on Ireland's society. This Criticality Score facilitates Government Departments/Agencies to determine which national infrastructure is CI. Evaluations on the upper scale allows for the identification of Critical National Infrastructure (CNI).

PART THREE proposes a framework of measures to improve resilience of CI. This framework compliments the five stage systems approach to emergency management outlined in the Strategic Emergency Management (SEM): National Structures and Framework[1] document. It advises on resilience measures in eight (8) key areas to enable Government Departments, Agencies and owners and/or Operators of Essential Services (OES) to continuously improve the resilience of their specific CI.

1. SEM available at www.emergencyplanning.ie

PART ONE

Introduction

1. Fostering national resilience is identified as an important objective in the Strategic Emergency Management: National Structures and Framework (SEM) document in order to minimise the disruption to society and to facilitate quick recovery of essential services from emergency events.

2. The SEM, in paragraphs 4.20 to 4.36, outlines that improving national resilience requires continual improvement of the resilience of National Infrastructure.

Background

3. The SEM has identified the requirement to have a number of Guideline Documents published in specific areas. One specific area is Critical Infrastructure Resilience. Para 4.31 of the SEM states: "CI consists both of assets owned and operated by the State, and of those operated by the semi-state and private sectors, usually under the regulation of an independent regulatory authority. The primary responsibility for safeguarding a CI asset or system rests with its owner or operator". Also Para 4.32 of the SEM states: "There is also a responsibility on Government to put in place measures to support safer, more secure and more resilient CI. This puts an onus on Government Departments to foster links and work closely with the semi-state and private sectors, focusing on the protection of critical infrastructure from a wide variety of threats". Further to this, Para 4.33 of the SEM states: "The task of identifying measures to improve the resilience of CI will be undertaken by a Sub Group of the GTF". All essential services, upon which society depends for normal functioning, are included in the scope of this Guideline Document.

4. To facilitate the reading and understanding of this Guideline Document, terminology and definitions used throughout are outlined at Table 1.

Table 1: Essential Definitions and Terminology.

Term	Definition
Agency	An Agency can be defined as any organisation within a sector, for which a Department has a responsibility, or oversight role, or with which it has a relationship, that provides any service to society, the loss of which may have an impact on society.
Business Continuity Planning (BCP)	Business Continuity Planning can be defined as the process by which organisations of any size design plans and procedures to ensure that their critical functions are maintained during emergencies and are restored to acceptable levels after an event.
Business Continuity Plans	Business Continuity Plans can be defined as documented business continuity procedures. Organizations use these procedures to respond to disruptive incidents, to guide recovery efforts, to resume prioritized activities and to restore operations to acceptable levels.
Business Impact Analysis (BIA)	Business Impact Analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. A BIA is an essential component of an organisation's business continuity plan.
Criticality	Criticality can be defined as the impact level to the citizen or to government from disruption or destruction of infrastructure.
Criticality Assessment	Criticality Assessment can be defined as a process used in evaluating the criticality of identified infrastructure. Notably, employing a risk based approach, Criticality Assessment evaluates the impacts due to service loss on the State and/or society instead of the impacts on the service providers.
Critical Infrastructure (CI)	Critical Infrastructure can be defined as an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of the people and the disruption or destruction of which would have a significant impact in the State as a result of failure to maintain those functions.
Critical Infrastructure Community	Critical Infrastructure Community can be defined as all stakeholders, including Government Departments, Agencies, and Owners/Operators of Essential Services, affected by disruption or destruction to Critical Infrastructure.
Critical Infrastructure Protection (CIP)	Critical Infrastructure Protection can be defined as the ability to prevent or reduce the impact of an adverse event.
Critical Infrastructure Resilience (CIR)	Critical Infrastructure Resilience can be defined as a dynamic process that applies an 'all hazard' risk based methodology to reduce the magnitude/scope, severity, or duration of a disruptive shock to the State/society and facilitates the resultant recovery. This type of resilient approach employs a holistic set of procedures and measures that ensures the ability to risk assess, mitigate, prepare for, absorb/adapt to, and recover from a disruptive shock.

Term	Definition
Critical National Infrastructure (CNI)	Critical National Infrastructure can be defined as being of unique national importance, which if disrupted or destroyed would have significant national level effects and may impact across a number of sectors. CNI is evaluated as a level 5 on the Criticality Scale (Table 6). CNI is a subset of C I.
Dependency and Interdependency	Dependency and Interdependency can be defined as relationships which consider the cascading effect within sector/sub-sectors and/or across sectors/sub-sectors. Dependency can be defined as a singularly dependent relationship while Interdependency can be defined as a mutually dependent relationship.
Disruptive Shock	Disruptive Shock can be defined as any significant event which interferes with the availability, delivery or integrity of essential services.
Essential Services	Essential Services can be defined as those day to day services which are essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of the people.
National Infrastructure	National Infrastructure can be defined as those assets and systems necessary for the delivery of the essential services upon which daily life depends and which ensure the state continues to function effectively.
National Resilience	National Resilience can be defined as the ability of the state to withstand and recover from adversity.
Operators of Essential Services (OES)	Operators of Essential Services can be defined as those public or private entities which provide/operate day to day services which are essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of the people.
Partnership	A partnership may be defined as a cross-organisational group working together towards common goals which would be extremely difficult, if not impossible, to achieve if tackled alone.
Preventative Measures	Preventative Measures can be defined as a set of controls put in place to avoid any damage, disruption or destruction to critical infrastructure from any potential crisis or emergency.
Public-Private partnership	Public-Private Partnership, in terms of CIR, can be defined as the relationship between governing/legislative/regulatory structures and owner/operators of Essential Services, some of which may be private entities.
Security Measures	Security Measures can be defined as measures to prevent intentional and accidental incidents which would cause a disruption or destruction to essential services.
Significant Impacts	Significant Impacts can be defined as those impacts which threaten public safety, social wellbeing or public confidence; threaten our economic security or harm our international competitiveness; harm the environment; or impede the continuity of the government or its services.
Reasonable Worst Case Scenario	Reasonable worst case scenario is the most serious credible scenario which causes the greatest impact to the service being provided. It is assessed using historical and scientific data, modelling and trend surveillance and the professional judgements of experts.

Purpose

5. The purpose of this Guideline is to create a methodology for Government Departments, agencies, public sector and private sector OES, to identify CI. It introduces a Criticality Metric, which consists of three specific, yet different, scales to evaluate the impact of the loss of that infrastructure on Irish society. Within each of the three distinct scales there are internationally accepted Impact Factors. There is an ascending value on these Impact Factors which reflect the increased impact on Irish society. A formula gives the infrastructure a score, allowing its criticality be evaluated in terms of the societal impacts of the loss of the service provided.

6. This Guideline then outlines measures to improve the resilience of infrastructures. This process in turn will further inform other national level reviews e.g. A National Risk Assessment (NRA) for Ireland.

Infrastructure Protection and Resilience: EU Context

7. Internationally it is generally accepted that the risk to society, due to inadvertent or deliberate disruption or destruction to CI, is gradually increasing. There are many reasons for this, including urbanisation, increased use of ICT, increased dependencies, increased demand and awareness of the instability caused by the interruption of services.

8. In 2005, responding to these trends and their related risks to society, the EU adopted a green paper on a European programme for Critical Infrastructure Protection[2]. In 2008, the European Council (EC) issued Directive 2008/114/EC[3] requiring Member States to identify and designate European Critical Infrastructure (ECI) and assess the need for its protection.

9. Though Directive 2008/114/EC requires Member States to consider infrastructure at EU level, it has prompted individual Member States to develop a knowledge of what their national CI comprises of and what is their criticality to society in order to help focus the development of national level Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) strategies. This Directive will be replaced by European Commission's *Resilience of Critical Entities Directive* (at time of writing this EU directive is being developed).

10. Reducing the vulnerabilities of CI across all sectors and improving their resilience is identified as a key objective by the EC.

11. The European Programme for Critical Infrastructure Protection (EPCIP), which is coordinated by the EU Joint Research Centre, outlines an overall framework for protection of CI in the EU and provides for an 'all-hazards cross-sectorial approach'. This considers all threats (terrorism, cyber, natural, etc.) for all relevant sectors for economic activity.

[2] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576

[3] 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.

12. The term CIP, as used by the EU, embraces not only the need to protect CI in the physical sense but also the need to ensure the continued provision of the service or output of the CI by taking such other practical measures as might be required to mitigate the risk to the CI.

13. Based on this work, a new approach to the work of EPCIP was adopted by the EC under the three main themes of prevention, preparedness and response. This new approach was aimed at building common tools and methodology within the EU to CIP and more recently CIR. Notably there is a focus on taking better account of CI dependencies.

14. Following on from this, in terms of CI cyber resilience, the EU adopted Directive (EU) 2016/1148 concerning measures of a high common level of security of network and information systems across the EU, otherwise known as the NIS Directive[4]. This directive will be replaced by European Commission's directive on measures for a high common level of cyber security (NIS2) (at time of writing this EU directive is being developed).

Move to Critical Infrastructure Resilience

15. International and EU publications[5] show a shift from a focus on CIP only and more consideration towards CIR in terms of 'good practice' in ensuring CI functionality.

16. The shift towards CIR is a result of a recognition that protective measures in themselves cannot ensure speedy restoration of services. There is an acknowledgment that focusing on CIP, owners and operators of CI may have limited capacity to continue service delivery when essential services they require are disrupted.

17. Another causal reason towards a CIR approach is due to the adverse and changing landscape of hazards and threats to CI. It is not possible to foresee, prevent, prepare or mitigate for all threats to CI which may in some cases be a new emergent threat.

Critical Infrastructure Resilience

18. CIR is a dynamic process that applies an 'all hazard' risk based method to reduce the magnitude/scope, severity or duration of a disruptive shock to the State/society and the resultant recovery. A resilient approach is a holistic set of procedures and measures that ensures the ability to risk assess, mitigate, prepare for, absorb/adapt to, and recover from a disruptive shock or event. Building CIR is as much a process as it is a set of outcomes. If the operation of CI within Ireland is seen as essential for Irish society then the resilience of that CI is of paramount importance. Cognisance must also be given to infrastructure outside the state upon which CI within the country depends.

[4] Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[5] Refers to the EC Staff Working Document on a new approach to the EPCIP making European CI more secure. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

Table 2: Sectors and Sub-Sectors of National Infrastructure*

Sector	Sub-sector	LGD**
Energy	Electricity	DECC
	Gas	DECC
	Oil	DECC
Food and Water	Food Supply	DAFM
	Water *(Supplies and wastewater including the sewerage system.)*	DHLGH
ICT	Telecommunications	DECC
	Information Technologies	DECC
	Media	DTCAGSM
Finance, Financial Services	Banking (including payment delivery)	DFIN
	Insurance	DFIN
	Welfare Payments Systems	DSP
Transport	Aviation	DT
	Roads	DT
	Rail	DT
	Marine & Ports	DT, DAFM
Health	Hospitals	DH
	Laboratories	DH DAFM
Public Administration	Government	DoT
	Central and Local Government	All
	Justice and Legal System	DJ
	Revenue and Customs	Revenue
	Cultural Property	DHLGH OPW
	Diplomatic Representations and International HQs	DFA
National Security, Policing and Public Safety Infrastructure	An Garda Síochána	DJ
	Fire and Emergency	DHLGH
	National Ambulance Service	DH
	Irish Coast Guard	DT
	Prison Service	DJ
	Defence Forces	DoD
	Civil Defence	DoD
Industry	Hazardous Industries *(Pharma, chemical etc.)*	DHLGH DETE
	Agriculture/Marine Industries (*Farming/Fisheries*)	DAFM
	Manufacturing and Processing Industries	DETE
	Industrial and Domestic Waste Disposal	DHLGH
	Logistical supply chains	All

*This table is contained in the 'Strategic Emergency Management (SEM) National Structures and Framework' published in October 2017.

**Names of updated Government Departments 2020

Identification of National Infrastructure

19. Prior to embarking on any understanding and assessment of the criticality of Ireland's infrastructure, it is necessary to understand the entirety of the National Infrastructure.

20. In the context of Ireland's response to natural and technological hazards, security threats, and other threats, the understanding of National Infrastructure is focused around the concept of Essential Services. National Infrastructure is viewed as comprising of those assets and systems necessary for the delivery of the essential services upon which daily life in Ireland depends and which ensure the State continues to function effectively both socially and economically.

21. The sector, sub-sectors and respective LGDs, as outlined in SEM and as illustrated in Table 2, facilitate the identification of National Infrastructure and the components that are assessed as 'critical' to the functions of the sectors. A list of Agencies are available at the Office of Emergency Planning's website.[6]

Understanding Criticality in Ireland's National Infrastructure

22. Understanding the dynamics underlying infrastructure will allow for more effective planning, response, coordination and recovery in the event of an emergency. The failure or compromise of one piece of infrastructure can have a cascading effect on other infrastructure, e.g. the failure of the power supply can interfere with the function of a water treatment plant or a sewage treatment plant. Infrastructures are physically interdependent if the state of each is dependent on the supply or service provided by the other, i.e. bi-directional influencing. There may also be a spatial dimension to interdependency, where one CI is co-located with or in close geographical proximity to another.

23. Ireland's National Infrastructure may be comprised of one or more individual infrastructure assets, which collectively enable the provision of the service or output in question. Assets may be human (e.g. staff), physical (e.g. sites, installations equipment etc.) or logical (e.g. information networks, systems etc.).

24. Within Ireland's sectors and sub-sectors there are certain 'critical' elements of infrastructure. The loss or compromise of such infrastructure, would have a significant impact on the availability or integrity of essential services, leading to loss of life or severe economic social or other negative impact on society.

25. It is important to note that not everything within the National Infrastructure sector and sub-sectors will be CI. In addition, within the identified CI, some will be more critical than others to society in terms of impact due to the disruption or destruction of service provided. The methodology outlined in Part 2 to identify CI also provides a Criticality Scale (Table 6), which shows the levels of criticality from localised infrastructure up to CNI.

[6] www.emergencyplanning.ie

PART TWO

Understanding and Identifying Critical Infrastructure

26. This Part of the Guideline Document outlines a methodology to identify CI and to determine its criticality. Universal guidelines for establishing these criteria, scoring and application do not exist as many different methods are utilised. However, good practice suggests that criticality can be based on the evaluation of impact that the disruption or destruction of the infrastructure would inflict on the provision of an essential service. The Impact Factors used in this Guideline Document are considered in line with international good practice, but also take into account Ireland's geographical position, National Impact Criteria[7] and the European Commission guidelines[8].

Why Conduct a Criticality Evaluation?

27. A risk based approach is accepted internationally as an essential step to evaluating the criticality of National Infrastructure. In particular, this approach is taken to evaluate the impact on society caused by a disruption or destruction to essential services.

28. The approach, adopted in this Guideline Document, was derived from good practice in the sphere of CIR and:

- **Contributes** to creating a shared understanding of the national-level challenges to be addressed with regard to the resilience of Ireland's CI;
- **Provides** a basis for establishing priorities with regard to risk mitigation strategies for CI within the State;
- **Provides** a basis for assessing national risk management capability;
- **Informs** the inter-agency work at local and regional levels under the provisions of the "Framework for Major Emergency Management[9]" (MEM);
- **Underpins and compliments** the implementation of the "Strategic Emergency Management"[10] (SEM) document developed by the Government Task Force on Emergency Planning (GTF);
- **Informs** the development of enhanced national resilience.

[7] National Risk Assessment for Ireland 2020 Table 2 Available at: www.emergencyplanning.ie

[8] Communication from the Commission on a European Programme for Critical Infrastructure. COM (2006) 786

[9] National Steering Group on Major Emergency Management; "A Framework for Major Emergency Management", 2006. Available at: www.mem.ie

[10] Strategic Emergency Management: National Structures and Framework. Available at: www.emergencyplanning.ie

Categorising Infrastructure and the Criticality Scale

29. The effects of a disruption to identified National Infrastructure are evaluated to categorise the impact on society, the safety and wellbeing of its citizens, the economy and the continual functioning of Government. The methodology to evaluate infrastructure criticality is based on the loss of a service to society. Senior Management of relevant stakeholders should evaluate infrastructure criticality by following the six step process outlined below.

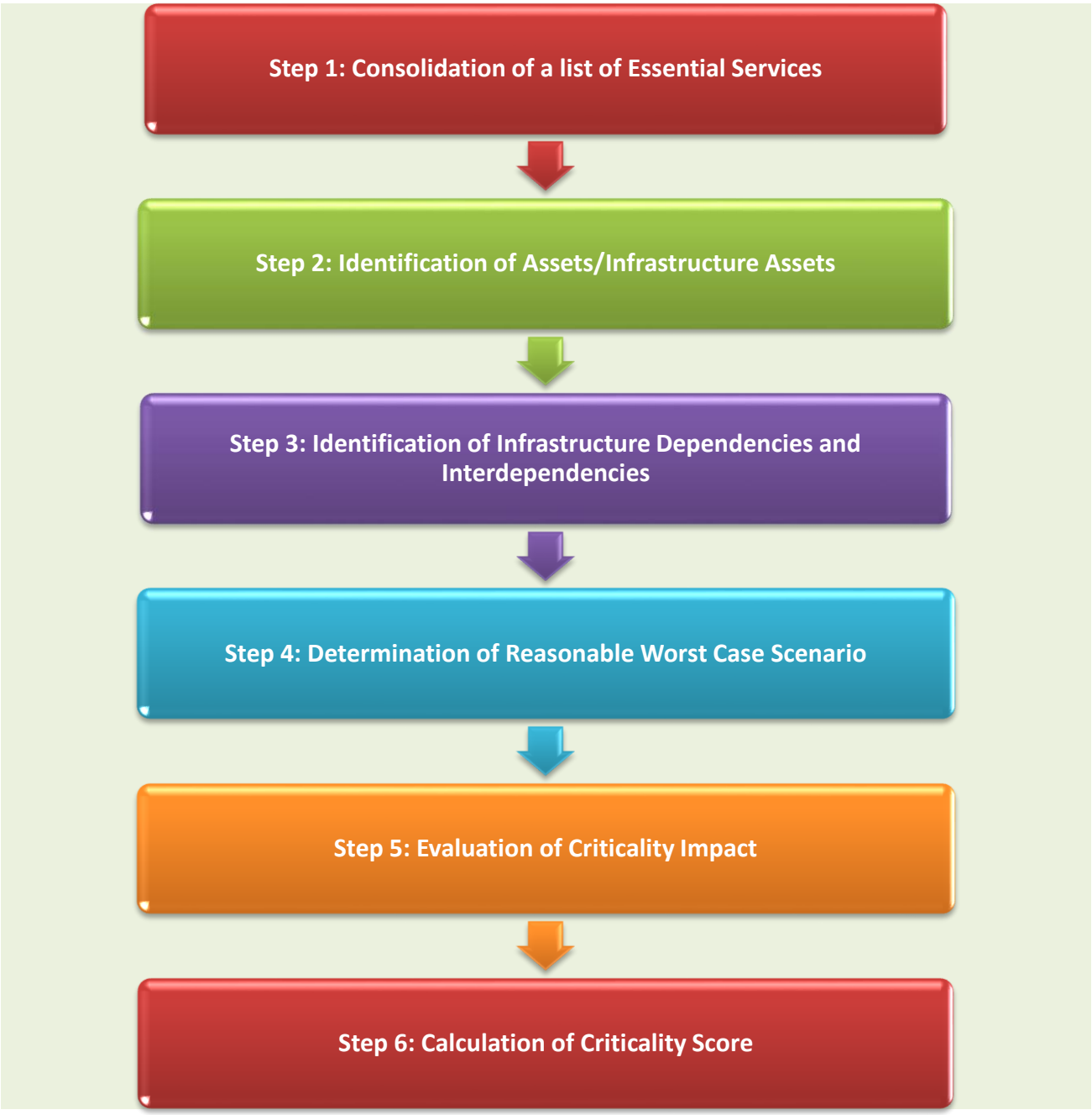


Figure 1. Six Steps for Evaluating Critical Infrastructure.

STEP 1: Consolidation of a list of Essential Services: Lead Government Departments (Table 2) and Agencies in consultation with Operators of Essential Services (OES) should consolidate a list of essential services which if disrupted or destroyed would, in their expert view, have the potential to have a significant impact on society.

STEP 2: Identification of Assets/Infrastructure Assets: Having identified essential services, document the assets essential for service provision, e.g. human (staff and expertise), physical (sites, installations, equipment etc.) or logical (Information networks, systems etc.). Each are now known as the Examined Infrastructure.

STEP 3: Identification of Infrastructure Dependencies and Interdependencies (Annex A and Annex B): Identify other infrastructures which are connected with the Examined Infrastructure.

30. These other infrastructures, as in Step 3, can be considered as two subcategories:

- **Dependent Infrastructures** include infrastructures that are dependent (one level up) on the Examined Infrastructure.
- **Required Infrastructures** include infrastructures that are required (one level down) by the Examined Infrastructure.

31. Where one asset requires support from a second asset, it is called Dependency. Where both assets require support from each other it is called Interdependency.

32. All identified dependencies and interdependencies within the Examined Infrastructure that imply any risk to society, must be considered. Furthermore for practicality, this identification process should be limited to one level up to Dependent Infrastructure and one level down to Required Infrastructure (Annex A).

STEP 4: Determination of a Reasonable Worst Case Scenario (RWCS): Using a Scenario based approach, determine a RWCS where a service is unavailable due to a disruptive shock.

33. To determine RWCS[11], an OES must list the possible scenarios which may impact the provision of their service, consider the mitigation measures already in place and determine which scenario is the RWCS. See Annex C.

STEP 5: Evaluation of Criticality Impact: Evaluate the criticality rating by assigning a score 1 to 5 for each impact factor. Ensure the score reflects the combined loss of dependent and interdependent services from Step 3.

34. The impact to society of the loss of service is evaluated using the categories of Scope, Severity and Time Related. All Impact Factors must be considered, however some impact factors may not be relevant to the scoring of a particular infrastructure.

[11] The term RWCS is derived from ISO 31010:2009, p85 "the most serious credible outcomes/consequence"

"The RWCS of a particular risk is based on historical and scientific data, modelling and trend surveillance and the professional judgements of experts" Keep the Country Running; P 22 Cabinet Office 2011

Table 3: Scope Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
People Affected	<75,000	>75,000	>150,000	>225,000	>350,000
Concentration of People	<10 pers/km2	>10 pers/km2	>50 pers/km2	>250 pers/km2	>1,250 pers/km2
Range	Rural	Urban/Town	County	Regional	National

35. **Scope Impacts**: This impact category has three factor for consideration (Table 3);

- People: This is a quantitative impact factor that measures the number of people that are affected by an event. It does not consider the severity of the impact.
- Concentration of people: This impact factor is a quantitative factor that highlights the greater the concentration of people, the increased potential for impact effects.
- Range: Finally this impact factor evaluates the geographical scope of an event. Range uses a qualitative or abstract representation in terms of geographical effect.

Table 4: Severity Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Public Impacts: including Loss of life, medical illness, serious injury	Deaths less than 1 in 250,000 people for population OR Critical injuries/illness less than 1 in 250,000 OR Serious injuries less than 1 in 100,000 OR Minor injuries only	Deaths greater than 1 in 250,000 people for population OR Critical injuries/illness greater than 1 in 250,000 OR Serious injuries greater than 1 in 100,000	Deaths greater than 1 in 100,000 people for population OR Critical injuries/illness greater than 1 in 100,000 OR Serious injuries greater than 1 in 40,000	Deaths greater than 1 in 40,000 people for population OR Critical injuries/illness greater than 1 in 40,000 OR Serious injuries greater than 1 in 20,000	Deaths greater than 1 in 20,000 people for population OR Critical injuries/illness greater than 1 in 20,000
Economic Impact: economic loss	Up to a 1% of Annual Govt Budget	Greater than 1 % of Annual Govt Budget	Greater than 2 % of Annual Govt Budget	Greater than 4% of Annual Govt Budget	Greater than 8% of Annual Govt Budget
Environmental Impact: including the surrounding environment	Simple, localised contamination.	Simple, regional contamination, effects of short duration	Heavy contamination localised effects or extended duration	Heavy contamination, widespread effects or extended duration.	Very heavy contamination, widespread effects of extended duration
Dependence: The dependencies on and between infrastructures	Very low impact on other infrastructures or other sectors	Low impact on infrastructures or other sectors	Moderate impact on infrastructures or other sectors	High impact on infrastructures or other sectors	Very high impact on infrastructures or other sectors
Political Impacts: including confidence in the Government	Perception of very low risk and high confidence to control risk	Perception of low risk and limited ability to control risk	Perception of moderate risk and low ability to control risk	Perception of high national risk and very low ability to control risk	High risk and lack of ability to control risk by national Government
Psychological Impacts: observed psychological effects on the population	Limited disruption to society	Society functioning with considerable inconvenience	Society functioning poorly	Society only partially functioning	Society unable to function without significant support
International Relations	Very low impact on international relations	Low impact on international relations	Moderate impact on international relations	High impact on international relations	Very high impact on international relations
Essential Services: Operators of Public or Private Services	Very low disruption to the delivery of public /private services	Low disruption to the delivery of public /private services	Medium disruption to the delivery of public /private services	High disruption to the delivery of public /private services	Loss of delivery of public /private services
Security: Cyber Security, State Security	Very Low disruption of operational effectiveness of security service	Low disruption of operational effectiveness of security service	Moderate disruption of operational effectiveness of security service	High disruption of operational effectiveness of security service	Loss of operational effectiveness of security service

36. **Severity Impacts**: This impact category has nine factors for consideration (Table 4);

- Public Impacts: This is a quantitative impact measurement that considers deaths and the extent of medical treatment required for illnesses and injuries.
- Economic Impact: This is a quantitative approach which is based on a percentage of annual government budget. This was adopted as the most suitable 'proxy' for economic impact.
- Environmental Impact: This is a quantitative impact measurement. Environmental criteria are based on the Environmental Protection Agency's environmental impact assessment criteria[12].
- Dependence: This is a qualitative impact measurement that considers the dependencies and interdependencies between CI elements. The cascading effects within and across sectors and sub-sectors should be considered.
- Political Impact: This is a qualitative impact measurement that considers public perceptions in relation to confidence in Local Authority and/or Government.
- Psychological Impacts: This is a qualitative impact measurement that considers psychological effects on the population.
- International Relations: This is a qualitative measure that considers relationships with the international community.
- Essential Services: This is a qualitative measurement that considers the disruption or destruction of services from either public or private services at a national level.
- Security: This is a qualitative measurement that considers state security and cyber security impacts only.

[12] Available at: www.epa.ie

Table 5: Time Related Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Recovery Time	Minutes	Hours	Days	Weeks	Months
Duration of Impact	Minutes	Hours	Days	Weeks	Months
Incident Impact Peak or Critical Point of Scale	Within Months	Within 4 Weeks	Within 7 Days	Within 24 Hours	Immediate

37. **Time Related Impacts:** This impact category has three factors for consideration (Table 5);

- Recovery Time: This quantitative factor measures the time required in order to recover from an incident until the service is restored to pre-event levels.
- Duration of Impact: This impact factor is not the same as Recovery Time. Although some services may recover and become fully functional at some point, the long term effects of an incident may still affect the infrastructure and its environment. For example, a service is lost but recovered in five days. However, its loss resulted in backlogs which take an additional three weeks before the service returns to pre event norms. Therefore it has a Duration of three weeks and five days.
- Impact peak: This impact factor is the point of time that an incident causes the most serious effect. For example, a service is lost on a Monday, however due to reserves, etc., this service loss impact peak is not realised until Thursday.

STEP 6: Calculation of Criticality Score: After evaluating and assigning a score from 1 to 5 for each Impact Factor, a Criticality Score can be calculated as follows:

a. Ensure all dependencies have been considered in the evaluation process before moving to the final calculation of Criticality Score.

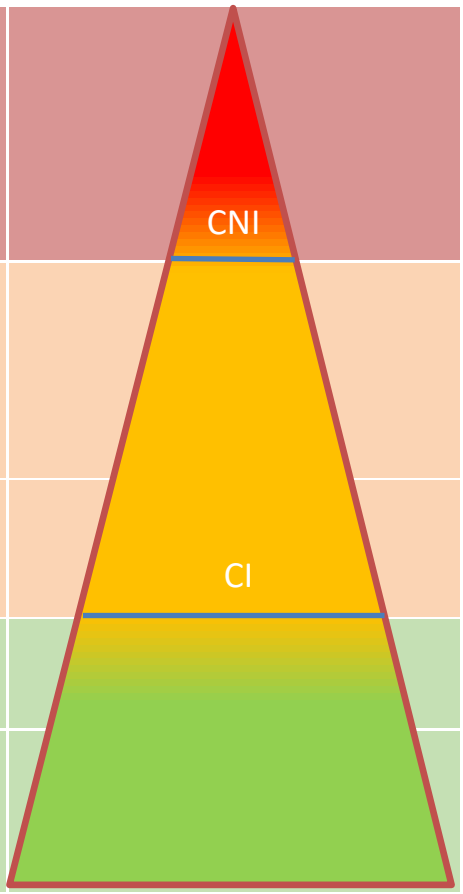
b. Select the single highest impact score from each Impact category (Scope, Severity and Time Related). Only one highest score from each category is necessary.

c. Multiply the highest score from each of the three Impact categories (i.e. Scope X Severity X Time Related). The calculated Criticality Score may range from 1 to 125. See Annex D.

d. Plot the Criticality Score on the appropriate level in Table 6 to determine the overall Criticality Level of the infrastructure.

38. A 'critical threshold' is set on the scale and is the level above which the impacts of loss are considered so severe that National Infrastructure falling into these levels should be considered CI. In this case, the base threshold is set at above Level 2 as illustrated on the National Infrastructure Pyramid in Table 6 below, with CNI for those few CI that fall into Level 5.

Table 6: Criticality Scale

Level	Description	National Infrastructure Pyramid
5	This is infrastructure the loss of which would have a very high impact on the State. These assets will be of national importance whose loss would have significant national effects and may impact across a number of sectors. Relatively few are expected to meet the Level 5 criteria known as CNI. (>80 Criticality Score)	
4	Infrastructure of high importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be high and may impact provision of essential services across Ireland. (>50 Criticality Score)	
3	Infrastructure of importance to the sectors, and the delivery of essential services, the loss of which would have a moderate impact. (>36 Criticality Score)	
2	Infrastructure whose loss would have a low impact on the delivery of essential services. (>27 Criticality Score)	
1	Infrastructure whose loss would cause very low disruption to service delivery, most likely on a localised basis. (<27 Criticality Score)	

PART THREE

Resilience

39. This part of the Guideline Document shares good practice and advice to enable Government Departments, Agencies and owners and/or operators of essential services to continuously improve their resilience to any disruption to services provided to society within the State. If the service provided by CI within Ireland is seen as essential for Irish society then the resilience of that CI is of paramount importance.

40. Resilience is the ability to risk assess, mitigate, prepare for, absorb, adapt to and recover from a disruptive shock. Building resilience is as much a process as it is a set of outcomes. The process of building resilience itself must also embody the characteristics of resilient systems (Figure 2).

- **Reflective:** Using past experiences to inform future decisions.
- **Resourceful:** Recognising alternative ways to use resources.
- **Robust:** Well-conceived, constructed and managed systems.
- **Redundant:** Spare capacity purposively created to accommodate disruption.
- **Inclusive:** Prioritise broad consultation to create a sense of shared ownership in decision making.
- **Integrated:** Bring together a range of distinct systems and institutions.
- **Flexible:** Willingness and ability to adopt alternative suggestions in response to changing circumstances.

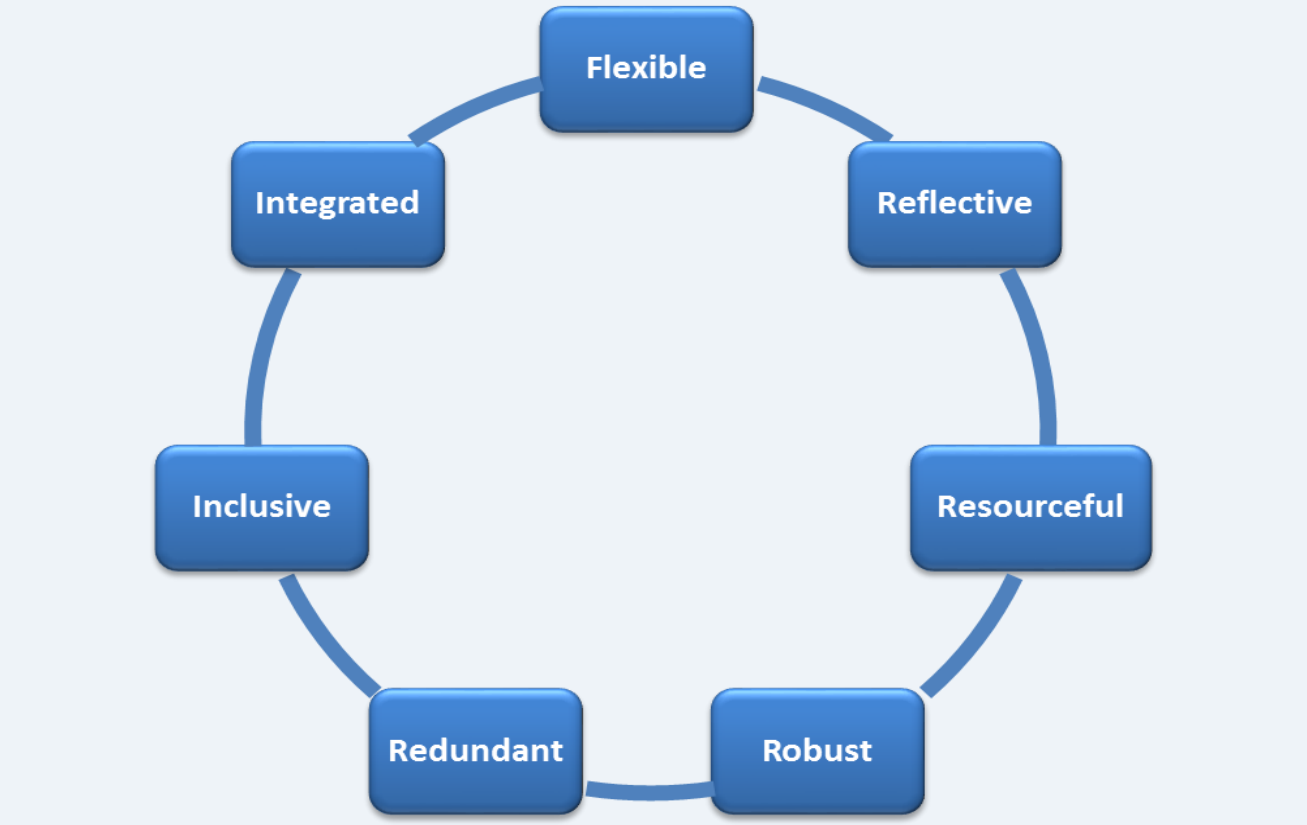


Figure 2. The Characteristics of Resilient Systems

41. Resilience is secured through a combination of activities or components; the four principle components are shown in Figure 3 below.

- **Resistance**: Concerns direct physical protection, e.g. fire walls, flood defences etc.
- **Reliability**: The capability of infrastructure to maintain services under a range of conditions, e.g. an asset being able to continue to operate in extremes of temperatures.
- **Redundancy**: the adaptability of infrastructure to maintain services (asset, network or system) e.g. back up data centres, alternative storage or spare capacity.
- **Response and Recovery**: An organisation's ability to respond to and recover from a disruptive shock.

42. The appropriateness and cost effectiveness of each component varies across the nine sectors of National Infrastructure (Table 2) owing to the differing circumstances involved. However each of the four components above can be utilised and adapted to all different levels of infrastructure.

Resilience of infrastructure is provided through:

- **good design** of the physical infrastructure and the associated systems to ensure it has the necessary resistance, reliability and redundancy.
- **establishing good organisational resilience** to provide the ability, capacity and capability to respond and recover from a disruptive shock.

Figure 3. The Components of Infrastructure Resilience

Measures to Improve Resilience of Critical Infrastructure

43. The following measures should be considered by all with responsibility for CI within the State. These measures are not hierarchical or mutually exclusive and may dovetail or complement each other. These measures are considered during all stages of the Five Stage Systems Approach to Emergency Management of Hazard Analysis, Mitigation, Planning and Preparedness, Response and Recovery. Examples of measures to improve resilience are given below and each sector should consider these in the context of their own CI. These measures can be used by organisations of any size.

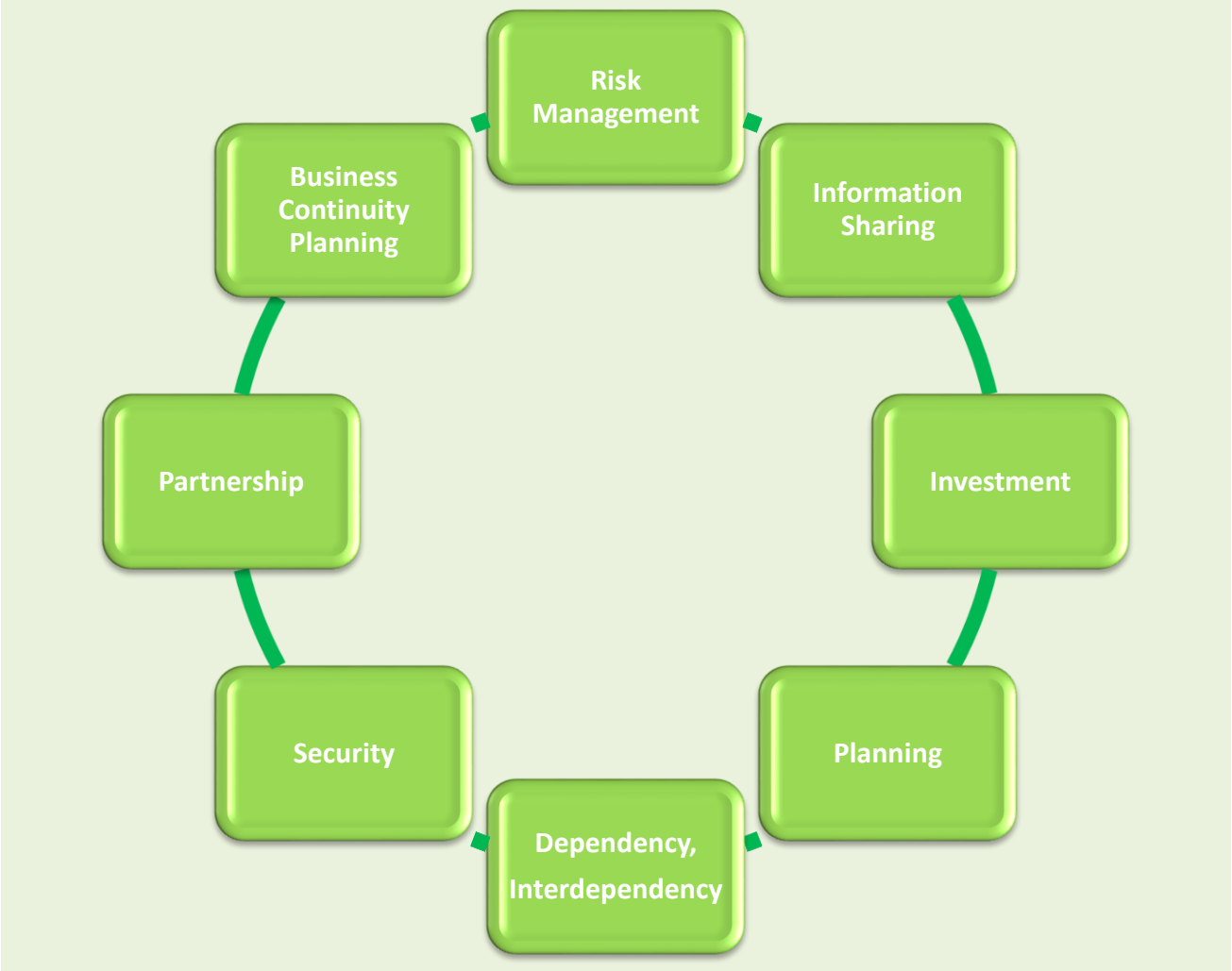


Figure 4. Measures to improve resilience

Risk Management

44. Risk Management is the process of identifying, assessing, evaluating, and treating risk. It also monitors, reviews, records, reports and communicates risk[13]. It ensures actions in resilience are considered across the range of options and choices and are proportionate to the risks. Effective risk management is the key to facilitating and building resilience, particularly when driven at the appropriate management level to create a culture where resilience and business continuity management is embedded in operations. This creates organisational resilience – the ability of an organisation to anticipate, plan and respond to uncertainties and disruptions to the business operations. Risk should be identified and managed in a coordinated and comprehensive way across the CI community to enable the effective allocation of security and resilience resources. Collectively managing risk requires the sharing of information and promoting more efficient and effective use of resources. It enables the development and execution of more comprehensive measures to secure against, disrupt /lessen, and prepare for threats, mitigate vulnerabilities, and reduce the consequences of loss of services to society. To ensure a comprehensive approach to risk management, the CI community should consider risk mitigation strategies as well as other ways to address risk, including acceptance, avoidance or transference of that risk.

45. **Risk Assessment:** A detailed risk assessment must be carried out to identify where the emphasis on resilient measures must be. Risk assessment must be carried out by a team, competent in this area to ensure the process is completed in a thorough and accurate manner. It must give a comprehensive picture to the decision makers of organisations. Risk Assessment is an iterative process and as such will identify opportunities for improving CI resilience.

46. **Risk Management Plan:** Risk Management Plans should be prepared and maintained by Owners/Operators of CI. These should contain as a minimum, identification and assessment of risks faced, existing and planned actions or activities to manage each of the risks and the arrangements, processes and procedures that implement these actions or activities.

47. **Critical Infrastructure Management Team:** Each OES should consider a Critical Infrastructure Management Team to maintain and manage all aspects and components of their CI. The infrastructure operator should develop and manage a risk register, which includes the vulnerability of, and threats to, all of its components such as, but not limited to; staff, resources, power/energy, physical structure, transportation, security, information security, cyber, dependencies and interdependencies.

[13] ISO 31000 Risk Management–Principles and Guidelines and ISO 31010 Risk Management- Risk Assessment Techniques

Critical Infrastructure Management Teams should consider not only the costs and current status of the CI itself but also the potential risks that the failure of CI could have on society. By mapping the risks, decisions can be made as to what measures should be performed based on a balance of performance, risk and cost.

Planning

48. The planning processes for management of various events, ranging from incidents to crises, will create the conditions that allow an event to be managed effectively. Learning gained and systems put in place during planning allow CI and services to society to be maintained or restored quickly. Lack of planning can translate very easily to serious situations that could have been avoided. Planning cannot be improved during emergencies.

49. As CI is built, refreshed or expanded, those involved in making design decisions, including those related to control systems, should consider the most effective and efficient ways to identify, deter, detect, disrupt and prepare for threats and hazards, mitigate vulnerabilities and minimise consequences. Building capacity and developing frameworks to improve all phases of preparedness, will have a positive impact on resilience.

50. In relation to the process of planning to enhance the resilience of CI, it is important to consider users' expectations. Planners should first determine the public's expectations with respect to the levels and resilience of services, and the investment required to maintain them. Planning should take cognisance of long term requirements and be prepared to horizon scan into the future.

51. It is crucial that the locked-in current impacts and the potential future impacts of climate change to critical infrastructure are considered in plans. Adaptation measures can have significant benefits and improve the reliability of service provision and the longevity of asset life as well as reduce the need for emergency responses. The most immediate risks associated with climate change to Ireland are predominantly those associated with changes in extremes, such as floods and storms. Further information on where to find data on the impacts of climate change on Ireland is available in SEM Guideline Document No 4 - Climate Change Adaptation[14].

52. All plans associated with enhancing the resilience of critical infrastructure should take full cognizance of advances in research, technology and innovation. It should encompass both cyber and physical concerns, and be strongly integrated in a layered security strategy.

[14] SEM Guideline Document No 4 - Climate Change Adaptation. https://www.gov.ie/en/collection/5ef65-publications/

53. **Preparedness:** The term preparedness refers to actions taken to reduce the impact of disasters when they are forecast or imminent. Raising awareness of potential threats and hazards among CI staff, ensuring the appropriate skillsets of staff and instilling a culture of risk awareness among staff will all ensure resilience within the CI.

54. Preparedness minimises hazards' adverse effects through effective precautionary measures that ensure timely, appropriate, and efficient organisation and delivery or response and relief action. Preparedness is usually defined and conducted through the use of pre-prepared plans. These may be referred to as emergency operations plans, contingency plans, continuity of operations plans, emergency response plans, or counter-disaster plans. These describe the people and agencies who will be involved in the response to events, the responsibilities and actions of these individuals and agencies, and when and where those responsibilities and actions will be called upon. Plans should include policy statements, procedures, checklists and information for decision makers.

55. A higher level of preparedness will enhance resilience and may not only protect the lives of citizens, but potentially lessen the amount of funding needed to rebuild/repair damage done to infrastructure and property following an event.

56. Preparedness plans are especially important for high hazard organisations, but often the most important benefit of preparing the plan is the growing of effective relationships and mutual understanding among those involved in the process of planning and preparation which in turn leads to a more mature and effective response when utilising those plans. Plans must be regularly tested, exercised and reviewed to ensure that they work efficiently when required.

Security

57. The protection of critical infrastructure involves activities that enhance the security of the organisation. This can relate to cyber and physical, public and private infrastructures that are essential to security, public health, safety and economic or social wellbeing. The security of these systems and data is essential to avoiding disruptions in critical operations.

58. **Preventative measures:** Preventative measures can be defined as a set of controls put in place to avoid any damage, disruption or destruction to critical infrastructure from any potential crisis or emergency. They help reduce the risk to CI, achieve operational protection and can reduce the number/intensity of emergency events. Plans/measures implemented in the Hazard Analysis, Mitigation and Planning and Preparedness phases of Emergency Management are used to reduce the likelihood of an incident occurring. Preventative measures aimed at reducing the risk should be subject to a cost

benefit analysis. This is done by comparing the potential expenditures and the direct and indirect costs resulting to society from a disruptive shock or extreme incident. Combining the result of a risk analysis with those of a cost benefit analysis leads to the selection of appropriate preventative measures.

59. **Security Measures:** Security measures can be defined as measures to prevent intentional or accidental incidents which would cause a disruption to or destruction of essential services.

60. Appropriate security controls and measures for staff working in particularly sensitive areas are essential for security. Organisations must take appropriate steps to mitigate the threat and/or reduce the possibility of an "insider threat" from staff working within the particular organisation or from external contractors.

61. Security of staff resources must also be emphasised and include appropriate succession planning and the spreading of expertise and knowledge to ensure services are not dependent on a small number of people.

62. Direct and robust physical protection should be utilised, where appropriate, to protect against known/suspected risks. Robust security includes well-conceived, constructed and managed systems. All OES must examine security measures appropriate to their particular area.

63. Given the ever increasing dependencies on information networks and systems, special consideration must be given to information and cyber security. All infrastructure is seriously threatened by persistent malicious attacks on multiple fronts, including networks, data and applications. Organisations must look at the development of several layers of security technologies. Critical assets that organisations need to protect include perimeter, as well as core systems. A cyber security program may be required to cover a wide range of areas that must be assessed and evaluated to protect the organisation.

64. Security risk assessment, like any other focused risk assessment scheme, requires the identification and quantification of threats, criticalities, and vulnerabilities of the organisation and its outputs. Mitigation includes identification and implementation of effective control, preventative, and corrective action. It is in executing control measures or mitigations that risk assessment becomes risk management, which is important if security measures are to improve resilience.

65. The integration of a security conscious mind-set must be present throughout the organisation. Without a similar approach, major security shortfalls may be present in areas of the utility, potentially exposing critical systems which operate core infrastructure.

66. Critical infrastructures can also be vulnerable to malicious attacks and hybrid attacks. The disruption of critical infrastructure can play an essential role in a hostile actor's hybrid activities. Therefore, an attack on critical infrastructure may just be a means to an end and part of a larger plan.

Business Continuity Planning

67. Business Continuity Planning (BCP) can be defined as the process by which organisations, of any size, design plans and procedures to ensure that their critical functions are maintained during emergencies and are restored to acceptable levels after an event.

68. A business continuity plan must be in place to ensure the continuation of essential services in the event of an incident or crisis. It facilitates the reliability of the infrastructure and the capability of that infrastructure to maintain operations under a range of conditions. It ensures that plans are in place to react to as wide a range of interruptions as possible to the service provided, and allows the service to be restored to full operating capacity as quickly as possible.

69. BCP should ensure there is redundancy built into the essential assets (human, physical and logical) within an infrastructure. The adaptability of CI assists in the quicker response and recovery from a disruptive shock.

70. Each owner/operator of CI should develop their own BCP with clear and defined actions to take place in the event of a disruptive shock. An important part of developing any BCP is the need to conduct a Business Impact Analysis (BIA). This is an evaluation of the effects of extended outages on the ability to continue service-critical functions. After reviewing the impact assessment, it is important to assess the maximum tolerable period of disruption to the service. A BCP should include a priority plan which identifies the parts, elements and sectors etc. which need to be restored first.

71. **Establish necessary Memorandum of Understanding:** Establishing a memorandum of understanding with other service providers may assist in restoration of essential services until CI is back to full operational capacity. Some CI have agreements to help with the recovery effort and get services back quicker or provide service while the original CI is being repaired.

72. **Robust Contracts**: Some CI is now owned and operated by private sector entities. Therefore, State authorities need to have robust contracts in place to ensure functionality and delivery of service capacity in times of crises. These contracts ensure the continuity or quick recovery of the service for the population. These relationships and their systems should be reviewed and tested regularly, in particular their communications, as communication plays a crucial role in BCP in order to keep recovery times for businesses to an absolute minimum.

73. **Training and Exercises:** Owners/operators must ensure that robust plans are in place to manage emergencies and restore service to customers. All staff should be appropriately trained and exercised in their various roles within the response and recovery phases of an incident. These plans must be tested to ensure their effectiveness. Owners/Operators should develop, conduct and evaluate exercises to test their planning, preparedness, prevention, response or recovery capability in respect of an emergency.

74. Government Departments have a role in the coordination of exercises in areas under their remit, providing a platform for inter-agency cooperation between State bodies and private sector owners/operators. Crisis communication is vital to this. Business Continuity Plans rely heavily on various methods of communication to disseminate information on a large scale within organisations.

75. **Lessons Learned:** Owners/operators of CI must be reflective and use past experiences to inform future decisions. Resilient CI is achievable only through the collective efforts of numerous partners grounded in continuous learning and adaptation to changing environments.

The CI community can better realise the opportunities for learning and adaptation during and after exercises and incidents through collaborative exercise design, coordinated lessons learned, corrective action processes and streamlined sharing of best practices.

Sharing of lessons learned and corrective actions from exercises and incidents and rapidly incorporating them into technical assistance training and education programs will improve future security and resilience efforts.

76. Business Continuity Plans need to be considered, implemented, monitored, and continually reviewed and improved upon.

Investment

77. Early Investments in resilience can deliver savings in the future. Any investment should be determined after risk analysis and cost effectiveness is analysed. Investments in critical infrastructure can require a significant initial outlay, take a long time to build and have long economic consequences.

78. **Adding Resilience:** A cost benefit analysis centered round the mitigation of any identified risk should be conducted and, where appropriate, investment made in adding robustness to CI. Such measures should address the entire infrastructure life-cycle from planning to operations, maintenance and renewal or retrofitting.

79. **Build Back Better:** It should be the aspiration of all owners/operators to use an opportunity, within financial constraints, to replace or expand CI with new and robust technologies which have greater resilience to envisaged threats. These allow a CI to withstand a higher level of impact in the future.

The concept behind Build Back Better-based recovery may present an opportunity subsequent to the recovery phase to rejuvenate the operation along with rebuilding to create a more resilient and sustainable organisation.

80. **Reconstruction**: Suitable plans should be in place to finance the temporary restoration of infrastructures in the immediate response to an emergency and the reconstruction of CI to recover and resume the pre-event or better level of service. Disaster or disruption recovery is a critical function within an organisation. Whether it is an external natural disaster or an unexpected internal systems failure, either can severely disrupt an organisation and the service it provides. Despite its importance, disaster recovery presents a difficult challenge, especially in a constrained spending environment, because it is aimed at avoiding the future cost of a breakdown. Disaster recovery spending typically does not translate to an immediate bottom-line financial benefit with a measurable return but a long term outlay on future security.

81. Conducting criticality assessments allow organisations to classify human, physical and logical assets that are truly critical. After criticality assessments are completed, stress tests and resilience analysis should be conducted in order to identify weak points where potential failures may occur. This allows organisations to set priorities for resilience investment and the allocation of resources.

Dependency and Interdependency

82. Understanding and addressing risks from cross sector dependencies and interdependencies is essential to enhancing CI security and resilience. All CI sectors rely on functions provided by energy, communications and transportation among others. It is important for the CI community to understand and appropriately account for dependencies and interdependencies when managing risk.

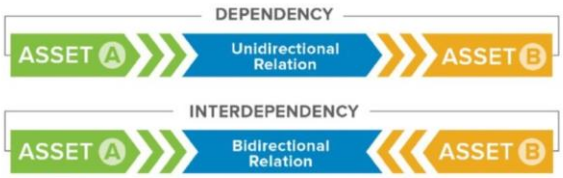


Figure 5. Dependency and Interdependency Model.

83. Modern Critical Infrastructures (CIs) are becoming increasingly more interdependent locally, regionally and globally, constituting a system of systems. The high degree of dependency (unidirectional) and interdependency (bidirectional) that exists between all sectors of infrastructure requires that the whole system be considered when assessing any impacts of an event.

84. Global investments in infrastructure, along with the deployment of global value chains, as well as the rise of information and communication technologies, have increased interconnectedness and interdependencies between sectors and countries around the world. Critical infrastructures are the hubs, nodes and networks of an increasingly complex web of interdependencies and interconnectedness, through which threat agents can navigate and the impact of disruptions can cascade. Therefore, the failure or disruption of one critical infrastructure system can have far-reaching consequences, in other sectors, or in other locations, sometimes globally (OECD, 2019).

Partnership

85. A partnership may be defined as a cross-organisational group working together towards common goals which would be extremely difficult, if not impossible, to achieve if tackled alone. There are benefits of both institutional partnerships at a strategic level and also at lower levels between organisations dealing with particular events or providing a particular service.

86. Partnership between Government and individual owners and operators of CI, all of them promoting collaboration, information sharing and risk management, is important and must be encouraged in order to ensure highest levels of resilience. Partnership between Government and individual owners and operators of CI also facilitates capitalising on the collective problem-solving acumen and creativity of the CI community, by leveraging advances in data and research, to address emerging challenges.

87. **Partnership approach:** A partnership approach is central to maintaining CIR. A well-functioning partnership depends on a set of attributes, including trust; a defined purpose for its activities; clearly articulated goals; measurable progress and outcomes to guide shared activities; leadership involvement; clear and frequent communications; and flexibility and adaptability. Recognising the value of different perspectives helps the partnership more distinctly understand challenges and solutions related to CI resilience. All levels of Government and the private and non-profit sectors bring unique expertise, capabilities and core competencies to the national effort.

88. The building of trust is clearly of supreme importance. The central function of trust is to develop long-term inter-organisational relationships and “closeness”. The key ingredients to building of trust are those of dialogue and communications.

89. **Collaboration across borders**: Ireland benefits from, and depends upon, a global network of infrastructure (e.g. oil distribution, transport systems for exports etc.). This is increasingly the case as services provided by critical infrastructure are often dependent on information gathered, stored and processed in highly distributed locations.

It is imperative that the public sector, the private sector and international public and private partners work together. This includes collaborating to fully understand supply chain vulnerabilities and implementing coordinated and not competing global security and resilience measures. The cognitive and cooperative skills of the individuals working in concert toward the same goals will ultimately determine the success of such collaboration which in turn improves resilience.

90. **Regional or sector partnerships:** These are crucial to develop shared perspectives on gaps and actions to improve infrastructure and resilience. The same shared perspective could be included in sector partnerships where a number of organisations share a common service function.

Information Sharing

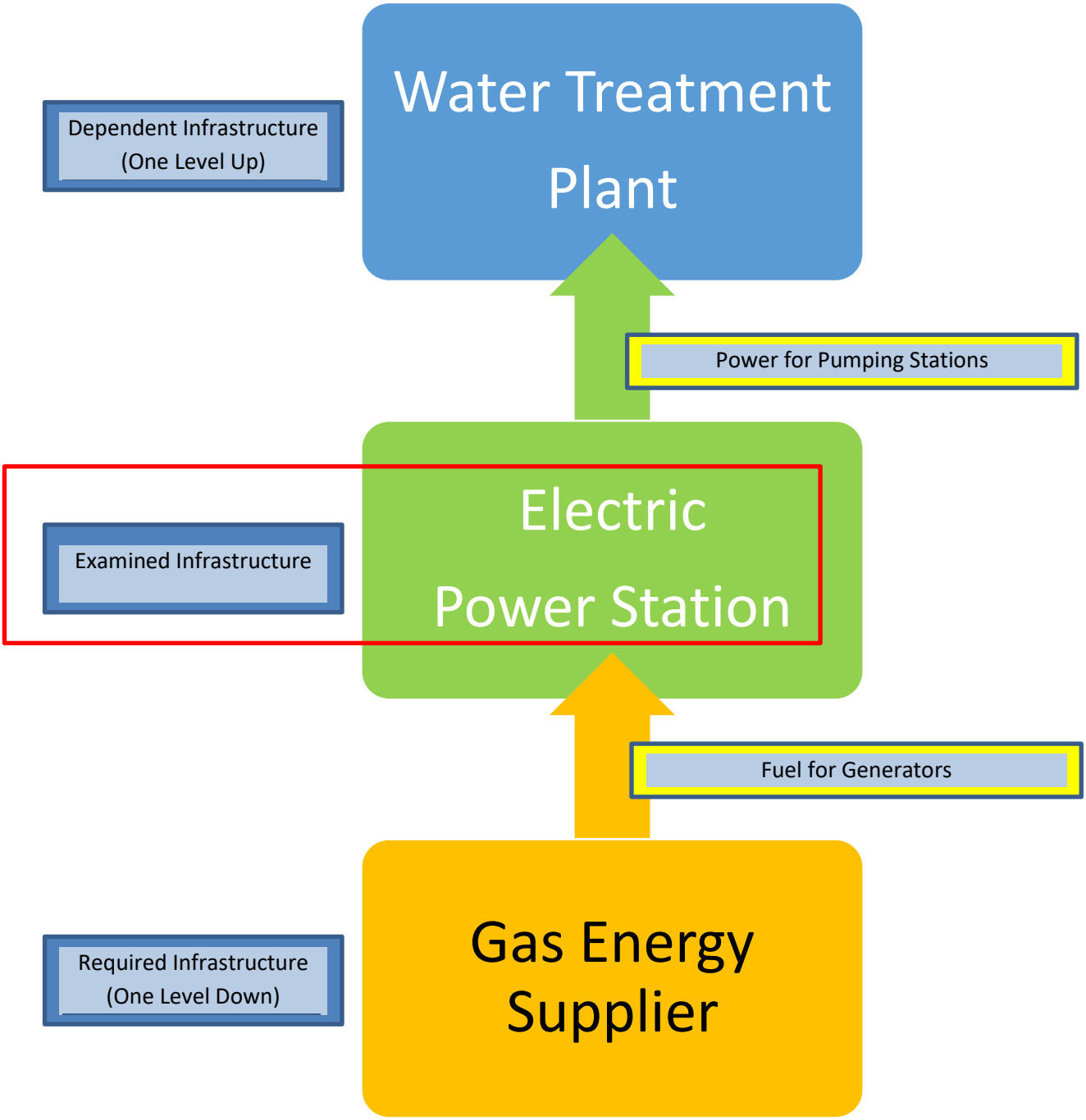
91. Stakeholders across the CI community possess and produce diverse information useful to the enhancement of critical infrastructure resilience. Sharing and joint planning based on this information is imperative to comprehensively enhance CI resilience in an ever evolving environment. For that to happen, appropriate legal protections, trusted relationships, enabling technologies and consistent processes should be in place.

Effective implementation of any information sharing frameworks require that all involved parties understand that organisations need to agree on joint response standards, responsibilities and protocols as well as on how to share data/information in order to efficiently respond to events.

92. To improve resilience across the CI community, it is important to encourage open and collaborative communication and information sharing between an organisation and its external partners. Public and private sector information sharing is also regarded as a bridge to improve performance. Strengthening these communication relationships between organisations and their external partners leads to enhanced information sharing.

93. In general, information sharing offers the opportunity to improve information infrastructure, data management integration, information quality, business process enhancement, and strengthens the relationship among participating organisations. Despite many expected benefits, there may be operational/natural barriers in adopting such initiatives. These should be overcome once relationships and trust is built up.

ANNEX A – EXAMPLE OF DEPENDENCY MODEL



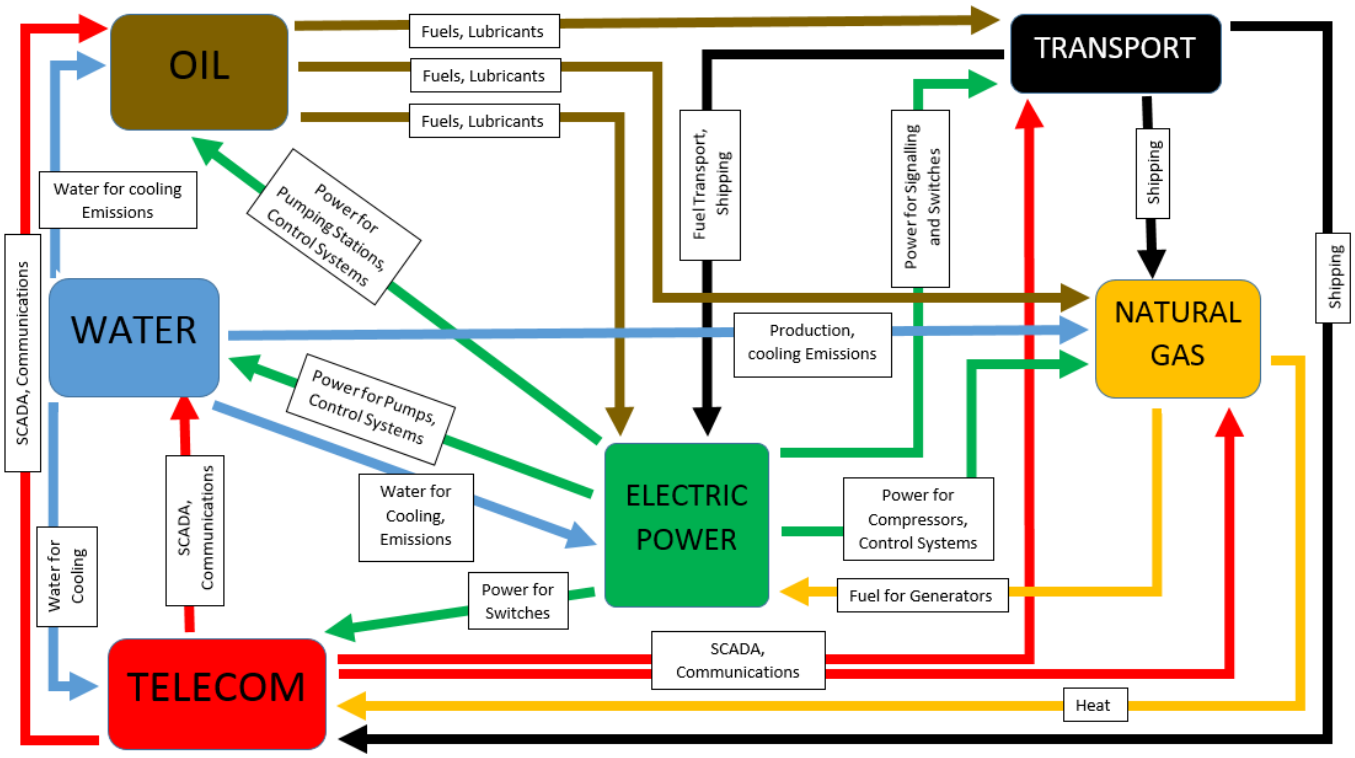
The **ELECTRIC POWER STATION** is the Examined Infrastructure.

The **ELECTRIC POWER STATION** requires **GAS** to produce power. Therefore, the **GAS ENERGY SUPPLIER** is the "Required Infrastructure" (one down) from the Examined Infrastructure.

The **ELECTRIC POWER STATION** produces power for **WATER** production, therefore, the **WATER TREATMENT PLANT** is a "Dependent Infrastructure" (one up) from the Examined Infrastructure.

When considering the impact of the loss of the **ELECTRIC POWER STATION** you must also consider the impact of the loss of the **WATER TREATMENT PLANT.**

ANNEX B – EXAMPLES OF INFRASTRUCTURE DEPENDENCIES AND INTERDEPENDENCIES



This diagram is hypothetical and illustrates the complexity of dependencies and interdependencies amongst infrastructures. It highlights the relationship between critical infrastructures in areas such as shipping, fuel supply and SCADA[15]

[15] SCADA - Supervisory Control And Data Acquisition, is a computer system for gathering and analyzing real time data. These systems are used to monitor and control industrial plants or equipment.

ANNEX C. – REASONABLE WORST CASE SCENARIO ASSESSMENT SHEET

Service Provided: ***From Step 1***	**Asset :** ***From Step 2***
Scenario	**Mitigation Measures Already in Place**
A	1. 2.
B	1. 2.
C	1. 2.
Having listed a wide range of reasonable scenarios and considered the mitigation measures already in place, OES should select one of these scenarios as the Reasonable Worst Case Scenario (RWCS) i.e. the one which would have the greatest impact on the service being provided if it were to occur.	
RWCS	**Justification and Narrative**
SCENARIO **B**	This scenario has been selected as the Reasonable Worst Case Scenario (RWCS) based on expert judgement of the risk managers, those who know the organisation best and the service it provides. Based on this, should this scenario happen, it would have the greatest impact on the service provided by the OES.

The following are possible scenarios and mitigation measures. These examples are for illustrative purposes only.

EXAMPLES OF SCENARIOS		
Supply chain issues	Loss of essential employees	IT systems failure
Disruption to energy supply	Severe weather- Flooding	Insider threat
Terrorism threat	Severe Weather – Snow/ice	Climate change
Severe Weather - Storm	Severe weather - Drought	Financial issues
Pandemic	Loss of water Supply	Accidental damage

EXAMPLES OF MITIGATION MEASURES		
Robust Systems	Succession Planning	Robust Supply Chains
Adequate reserves held	Several sources of raw material	Sufficient levels of security
Sufficient training of staff	Protocols in place	Strong IR relationships

ANNEX D. - CRITICALTY SCORE CALCULATION - EXAMPLE

A hypothetical piece of Infrastructure is evaluated through the three scales:

Scope Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
People Affected	<75,000	>75,000	>150,000	>225,000	>350,000
Conc. of People	<10 pers/km2	>10 pers/km2	>50 per/km2	>250 pers/km2	>1,250 pers/km2
Range	Rural	Urban/Town	County	Regional	National

Severity Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Public Impacts: including Loss of life……..	Deaths less than 1 in 250,000……	Deaths greater than 1 in 250,000 …….	Deaths greater than 1 in 100,000…….	Deaths greater than 1 in 40,000 people …….	Deaths greater than 1 in 20,000 people for …….
Economic Impact: economic loss.	Up to a 1% of Annual Budget	Greater than 1 % ……	Greater than 2 % of Annual ……	Greater than 4% of Annual …….	Greater than 8% of Annual ……
Environment Impact……..	Simple……,.	Simple, regional……	Heavy contamination …	Heavy contamination……	Very heavy contamination,
Interdependence, namely the…….	Very low impact…..	Low impact on infrastructures…	Moderate impact……	High impact on infrastructures…	Very high impact…….
Political Impacts:	Perception of very low risk …	Perception of low risk…..	Perception of moderate risk…	Perception of high national risk ……	High risk and lack of ability to….
Psychological Impacts,	Limited disruption…	Society functioning…….	Society functioning ……..	Society only partially ……	Society unable to function…..
International Relations	Very low impact on	Low impact on int. relations	Moderate impact on	High impact on int. relations	Very high impact on int. relations
Essential Services (Operators of ……	Very low disruption to….	Low disruption to the….	Medium disruption to…….	High disruption to the delivery……	Loss of delivery of public /private ……
Security…….	Very Low disruption…..	Low disruption of ……	Moderate disruption……..	High disruption of operational……..	Loss of operational effectiveness……

Time Related Scale

Impact Factor	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Recovery Time	Minutes	Hours	Days	Weeks	Months
Duration of Impact	Minutes	Hours	Days	Weeks	Months
Incident Impact Peak	Within Months	Within 4 Weeks	Within 7 Days	Within 24 Hours	Immediate

The highest score from each scale is taken. Even though there are two scores of four in Severity Scale, only one is taken. To work out the Criticality Score Calculation, multiply the highest score from each scale. The Criticality Score is then placed on the Criticality Scale (Table 6).

Scope Scale = 5 Severity Scale = 4 Time Related Scale = 4

5 X 4 X 4 = 80

Therefore the Criticality Score of this piece of hypothetical infrastructure is 80

TABLE OF ACRONYMS

Acronym	Title	Acronym	Title
BCP	Business Continuity Planning	EC	European Council
BIA	Business Impact Analysis	ECI	European Critical Infrastructure
CI	Critical Infrastructure	EPCIP	European Programme for Critical Infrastructure Protection
CIP	Critical Infrastructure Protection	EPA	Environmental Protection Agency
CIR	Critical Infrastructure Resilience	EU	European Union
CNI	Critical National Infrastructure	GTF	Government Task Force on Emergency Planning
DAFM	Department of Agriculture, Food and the Marine	ICT	Information and Communications Technology
DETE	Department of Enterprise, Trade and Employment	ISO	International Standards Organisation
DECC	Department of Environment, Climate and Communications	LGD	Lead Government Department
DSP	Department of Social Protection	MEM	Framework for Major Emergency Management
DFA	Department of Foreign Affairs	NIS	Network and Information Systems
DFIN	Department of Finance	NRA	National Risk Assessment
DH	Department of Health	OECD	Organisation of Economic Co-operation and Development
DHPLG	Department of Housing, Local Government and Heritage	OES	Operators of Essential Services
DJ	Department of Justice	OPW	Office of Public Works
DoD	Department of Defence	RWCS	Reasonable Worst Case Scenario
DoT	Department of an Taoiseach	SCADA	Supervisory Control And Data Acquisition
DT	Department of Transport	SEM	Strategic Emergency Management: National Structures and Framework

BIBLIOGRAPHY

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

Australian Government (2015) *Critical Infrastructure Resilience Strategy: Plan.* pp.1 - 11. Canberra: Commonwealth of Australia

Bowman, R. and Newman, A. (2016). A model to improve preparedness and strategically enhance resiliency at a community level: The Garden State approach, Journal of Business Continuity & Emergency Planning, 10 (2), pp.124-131.

Canadian Government (2014) *Action Plan for Critical Infrastructure (2014 - 2017)*. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-en.aspx

Canadian Government (2014) Critical 5: Forging a Common Understanding for Critical Infrastructure. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx

Canadian Government (2018) *Enhancing Critical Infrastructure Resiliency*. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/nhncng-rslnc-en.aspx

Canadian Government (2018) *National Strategy for Critical Infrastructure*. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

Canadian Government (2018) *The Regional Resilience Assessment Program*. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx

Center for Security Studies, Switzerland (2008) *CRN Report: Critical Infrastructure Protection.* Zurich: Center for Security Studies

Coppola, D. P. (2015). *Introduction to International Disaster Management.* Oxford: Butterworth-Heinemann.

Department of Defence (2017). Strategic Emergency Management: National Structures and Framework. Dublin: Office of Emergency Planning.

European Commission (2006) *Communication from the Commission on a European Programme for Critical Infrastructure Protection.* Brussels: Commission of the European Communities.

European Commision (2013) *A New Approach to the European Programme for CIP: Making European CI more secure.* Brussels: Commission of the European Communities.

European Commission (2017) *Science for Disaster Risk management 2017.* Brussels: Commission of the European Communities.

Federal Office for Civil Protection FOCP (2009). *The Federal Council's Basic Strategy for Critical Infrastructure Protection.* Bern: Federal Department of Defence, Civil Protection and Sports DDPS, Switzerland.

European Commission (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. (2008). *Official Journal of the European Union*, L 345, pp.75 - 82.

Granot, H. (1997) Emergency inter-organisational relationships. Disaster Prevention and Management, 6 (5), pp. 305-310.

Haddow, G., Bullock, D. & Coppola, D. (2011) Introduction to Emergency Management. 4th ed. Burlington: Elsevier.

Hiles, A. (2011) The definitive handbook of business continuity management, 3rd ed. Chester: John Wiley & Sons.

Izuakor, C and White, R. (2016) Critical Infrastucture Asset Identification: Policy, Methodology and Gap Analysis., in Rice, M and Shenoi S. (eds) *Critical Infrastructure Protection X,* Arlington, VA: Springer, pp. 27 - 41.

Kapucu, N., Arslan, T., and Demiroz, F. (2010) Collaborative emergency management and national emergency management network. Disaster Prevention and Management, 19(4), pp.452-468.

Laing, A.W. and Lian, P.C.S. (2005) Inter-organisational relationships in professional services: Towards a typology of service relationships. Journal of Services Marketing, 19 (2), PP. 114-128.

ISO (2009) *ISO 31000. Risk Management - Principles and Guidelines.* Retrieved from International Standards Organisation: http://www.iso.org/iso/home/standards/iso31000.htm

ISO (2009) *IEC 31010:2009 Risk Management - Risk assessment Techniques.* Retrieved from International Standards Organisation: http://www.iso.org/iso/home/standards/iso31000.htm

ISO (2012) *ISO 22301:2012 Societal security -- Business continuity management systems -- Requirements.* Retrieved from International Standards Organisation: https://www.iso.org/standard/50038.html

ISO (2018) *ISO 31000:2018 Risk Management - Principles and Guidelines.* Retrieved from International Standards Organisation: http://www.iso.org/iso/home/standards/iso31000.htm

Mannakkara, S and Wilkinson, S. (2013) Build back better principles for economic recovery: Case study of the Victorian bushfires , Journal of Business Continuity & Emergency Planning , 6(2), pp.164-173.

OECD (2013) Governing effective Prevention and Mitigation of Disruptive Shock. *Risk Management Policy Issues Paper*. Paris: OECD Publishing

OECD (2014) *Boosting Resilience through Innovative Risk Governance.* Paris: OECD Publishing doi:10.1787/9789264209114-en

OECD (2015) Policy Evaluation Framework on The Governance of Critical Infrastructure Resilience in Latin America. Paris: OECD Publishing.

OECD - JRC (2018) 'System-thinking for critical Infrastructure Resilience and Security'. 7th OECD High-Level Risk Forum, Paris, 24-25 September 2018.

OECD - JRC (2018) 'Good Practice Framework for the governance of Critical Infrastructure Resilience'. 8th OECD High-Level Risk Forum Paris, 12- 14 December 2018.

OECD (2019), Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies, Paris: OECD Publishing. https://dx.doi.org/10.1787/02f0e5a0-en.

Praditya, D. and Janssen, M (2015) Benefits and Challenges in Information Sharing between the Public and Private Sectors. Journal of Proceedings of the European Conference on e-Government, ECEG, 2015, pp.246-253.

Petit, F. D. et al. (2013) Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Argonne, Illinois: Argonne National Laboratory, Global Security Sciences Division.

Petit, F. D. et al. (2015) Analysis of Critical Dependencies and Interdependencies. Argonne, Illinois: Argonne National Laboratory, Global Security Sciences Division.

Phelps, R. (2017) The true value and return on investment of business continuity, Journal of Business Continuity & Emergency Planning, 11(3), pp.216-222.

Razetti, E.A. (2018) Disaster Preparedness in DoD. Hurricanes and Terrorist Attacks Require the Same Preparations. Defence AT& L., 47(1), pp.12-18.

Rehak, S., Senovsky, P. and Slivkova, S.(2018) Resilience of Critical Infrastructure Elements and Its Main Factors. *MDPI*, pp. 1 - 11. doi: 10.3390/systems6020021

Rinaldi, S., Peerenboom, J. and Kelly, T. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control System Magazine, 21, 11–25.

Santella, N., Steinberg, L.J, and Parks, K. (2009) Making for Extreme Events: Modeling Critical Infrastructure Interdependencies to Aid Mitigation and Response Planning. Review of Policy Research, 26(4), pp.409-422.

Sarriegi, J.M., Finn, F.O, and Torres, J.M. 2008. Towards a research framework for critical infrastructure interdependencies, International journal of emergency management , 5(3), pp235-249.

Shuster, L.A. (2009) Report Urges New Framework for Planning Critical Infrastructure, Civil Engineering, pp.20-21.

Setola, R, Luiijf, E. and Theoharidou, M. (2016) Managing the Complexity of Critical Infrastructures, Studies in Systems, Decision and Control 90, pp . 1 - 15. doi: 10.10007/978-3-319-51043-9_1

Swedish Civil Contingencies Agency (MSB) (2014). Action Plan for the Protection of Vital Societal Functions and Critical Infrastructure. https://www.msb.se/en/Products/Publications/Publications-from-the-MSB/Action-Plan-for-the-Protection-of-Vital-Societal-Functions--Critical-Infrastructur

Theoharidou, M., Kotzanikolaou, P. and Gritzalis, D. (2009) 'Risk-Based Criticality Analysis; Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection', in Palmer, C. and Shenoi, S. (eds.) 3rd IFIP International Conference on Critical Infrastructure Protection. USA: Springer, pp.35-50.

U.K. Cabinet Office (2010) *Strategic Framework and Policy Statement on improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.* London: Cabinet Office.

U.K. Cabinet Office (2011) *Keeping the Country Running: Natural Hazards and Infrastructure.* London: Cabinet Office.

U.K. Cabinet Office (2014) A summary of the 2014 Sector Resilience Plans. August 2014. London: Cabinet Office.

U.S. Dept. of Homeland Security (2013) National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. Retrieved from *https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience*

State of Victoria (Emergency Management Victoria) (2015) *Critical Infrastructure Resilience Strategy.* Melbourne: Victorian Government.

Title:	**Strategic Emergency Management Guideline 3, Critical infrastructure Resilience (Version2)**		
Prepared by:	**Office of Emergency Planning (OEP) and Government Information Service (GIS)**		
Adopted by:	**Government Task Force on Emergency Planning**		
Version:	**2.0**	**Date of Approval**	**14/07/2021**

An Roinn Cosanta
Department of Defence

Approved by the Government Task Force on Emergency Planning – 14 July 2021.

An Oifig um Pleanáil Éigeandála **An tIonad Náisiúnta Comhordaithe Éigeandála** **Teach Talmaíochta (2 Thoir)** **Sr. Chill Dara Baile** **Átha Cliath 2** **R-Phost: oep@defence.ie** **Teileafón: 00353 1 237 3800** **Láithreán Gréasáin: www.emergencyplanning.ie**	**Office of Emergency Planning** **National Emergency Coordination Centre** **Agriculture House** **Kildare Street** **Dublin 2** **Email: oep@defence.ie** **Telephone: 00353 1 237 3800** **Web Site: www.emergencyplanning.ie**

DFPP **Printed by Defence Forces Printing Press**

An Roinn Cosanta
Department of Defence