Keeping Scotland Running

RESILIENT ESSENTIAL SERVICES
SCOTTISH GOVERNMENT'S STRATEGIC FRAMEWORK
2020-2023

Scottish Government
Riaghaltas na h-Alba
gov.scot

www.readyscotland.org

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Scottish Government
Riaghaltas na h-Alba
gov.scot

www.readyscotland.org

CONTENTS Page

FOREWORD

In Scotland, our experience over many years has taught us the importance of Critical Infrastructure Resilience (CIR), whether the challenges we face include severe weather, pandemic disease, or man made threats from crime or terrorism.

I am pleased to say that since the publication of our CIR strategy 'Secure and Resilient' in 2011, we have come a very long way indeed. One of the key developments I would like to single out is the way in which we have become much more pro-active in our collaborative approach to mitigating the impacts of the challenges we face.

So whilst we are in a much stronger place than we were only a few short years ago, there is still a long way to go and we should never lose sight of the fundamental reason why we need to commit our time, effort and resources to build effective Critical Infrastructure Resilience – to ensure that Scotland is a safe, strong and resilient Country where our communities feel safe and are safe so that our economy can flourish.

This is why we are refreshing our strategic approach to CIR. Continuous improvement is at the heart of everything we do in Government and 'Keeping Scotland Running' is an example of this. There are four key elements within the new strategy and guidance, which I personally believe will make a significant contribution to resilience in Scotland.

Mainstreaming

The truth of the matter is that when a crisis strikes, we are all in it together – Government, Industry, local and national Responders – Resilience is everyone's business. We all need to be fully engaged from the outset to ensure that our arrangements are effective and that we all bounce back stronger from disruptive events.

Prevention

Planning, Responding and Recovering from disruptive events will continue to be key to our resilience effort in Scotland. However, I believe that a new focus on the Preventative elements of our resilience approach – Assessment of risk and Prevention activity to mitigate risk – will help to improve and enhance our already World Class resilience arrangements and ensure that Scotland remains a leader in this field.

Collaboration

Resilience involves a diverse range of stakeholders across Government, Industry, Responder Organisations, Academia and Communities at Scottish, UK and International levels. It is a highly complex field of work that requires a high level of

coordination and collaboration. In order to achieve this, we will continue to work hard to build strong relationships and to establish effective networks across Scotland. Information sharing and removing barriers to effective communication will remain a key aspect of this work.

Investment

This will be a key aspect of the Critical Infrastructure Resilience Programme as we go forward. I recently received the first Ministerial Summary of Critical Infrastructure Resilience in Scotland, which highlighted the need for a greater level of connectivity between the Prevention activity of CIR and our Infrastructure Investment programme in Scotland. This I believe, is an area where we can realise huge benefit in the future and exploit the opportunities that are available to us in understanding and mitigating our essential services vulnerabilities.

While real progress has been made over the last few years, we must never allow ourselves to become complacent. By working effectively across Government, Resilience Partnerships and Industry, we can make a significant difference together in making Scotland a Safe and Strong place to live and work.

John Swinney
Deputy First Minister

Introduction

In recent years we have been reminded of the potential for disruption to our essential services through a whole range of events both malicious and natural.

Building resilience across all aspects of our essential services and enhancing the security and resilience of the critical infrastructure that supports and under-pins these services is vital. This can only be achieved through the implementation of appropriate enhanced protective security measures and mitigating the risks from natural hazards through improving our resilience and contingency planning arrangements. Increasing our understanding of the threats and hazards, and developing our awareness of the interdependency issues across all 13 sectors of critical infrastructure will also assist in terms of moving the resilience agenda forward in Scotland.

'Keeping Scotland Running' has been designed to support critical infrastructure owners and operators, emergency responders, resilience partnerships (RPs), industry groups and relevant government departments in working together to improve the resilience of critical infrastructure and essential services provision in Scotland. It seeks to support the delivery of national strategies in Scotland, including the National Security Strategy and Strategic Defence and Security Review 2015 (SDSR 2015)[1] and the UK Counter Terrorism Strategy – CONTEST.[2] 'Keeping Scotland Running' is not intended to duplicate or conflict with existing UK Government critical infrastructure resilience work streams or other regulatory requirements in this area.

Background

In March 2011, the Scottish Government published its first ever strategy for Critical Infrastructure Resilience (CIR) in Scotland – 'Secure and Resilient – A Strategic Framework for Critical National Infrastructure in Scotland.'[3] The strategy was based on a clearly defined purpose, a common vision and a set of established principles that provided an excellent foundation on which to build our Critical Infrastructure Resilience (CIR) programme in Scotland. Indeed, the strategy and the wider delivery programme has also helped to establish Scotland as a world leader in the field of CIR.

'Keeping Scotland Running' seeks to build on the success of 'Secure and Resilient' by refreshing our strategic aims in the light of some significant developments that have taken place over the last few years. Much of the policy articulated in 'Secure and Resilient' however, remains valid and as such, CIR stakeholders should continue to refer to the document for guidance.

---

1 https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

2 https://www.gov.uk/government/publications/counter-terrorism-strategy-contest

3 https://www2.gov.scot/Resource/Doc/346469/0115308.pdf

Significant Developments in Critical Infrastructure Resilience (CIR)

In September 2014, the UK National Security Council (NSC) instigated a comprehensive review of Critical Infrastructure Resilience (CIR) strategy and policy. The review resulted in a new definition of Critical National Infrastructure (CNI) and an increase in the designated CNI Sectors from 9 to 13. A comprehensive governance and delivery programme has also been established under the UK NSC, coordinated by the Cabinet Office at a UK level and delivered in Scotland through the Critical Infrastructure Resilience Partnership (CIRP).

New Definition of Critical National Infrastructure (CNI)

- *'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*
    - *major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*
    - *significant impact on national security, national defence, or the functioning of the state.'*

Designated Critical National Infrastructure (CNI) Sectors

The following table provides a list of the 13 designated CNI sectors following the 2014 review and highlights the agreed split between Reserved and Devolved responsibilities.

Reserved Sectors	Devolved Sectors
Energy – Electricity, Gas, Fuel/Oil **Communications** – Telecommunications, Public Broadcast, Postal Services, Internet **Government** – UK **Transport** – Aviation, Rail and Ports **Finance** **Emergency Services** – HM Coastguard **Civil Nuclear** **Defence** **Space**	**Government** – Scottish Government, Scottish Parliament, NDPBs and other agencies, Local Authorities **Health** **Food** **Water** – Drinking Water, Waste Water **Transport** – Roads and Bridges **Emergency Services** – Police, Fire and Ambulance **Chemicals**

Critical Infrastructure Resilience (CIR) Coordination and Delivery

At a UK level, the Cabinet Office coordinates delivery of Critical Infrastructure Resilience (CIR) through the Infrastructure Resilience and Security Working Group – IRSWG, which in turn reports to the Threats, Hazards, Risk and Contingencies Group – THRC (O) and the National Security Committee (NSC).

In Scotland, the Scottish Government coordinates delivery at a national and regional level through the Critical Infrastructure Resilience Partnership (CIRP) and reports directly into the UKG arrangements. Delivery of the CIR work programme is driven through sector specific resilience groups and three regional critical infrastructure resilience groups covering the North, East and West Resilience Partnership areas (See Annex A).

Progress in delivering CIR in Scotland since 2011

Since 2011, the Scottish CIR programme has matured and evolved using recognised continual improvement methodologies. The following highlights four significant areas where progress has taken place resulting in an overall improvement in Critical Infrastructure Resilience (CIR) in Scotland (see Annex B for an overview of how this process works in practice).

A Scottish Approach to CIR

- A move from a protective security approach to an all risks approach, which has subsequently been endorsed as good practice at a UK level
- A move from a UK CNI approach to a Scottish Essential Services and Sector Resilience approach
- Evolution from a centralised focus in Scotland to a regional and local approach in relation to CIR
- Enhanced engagement and influence on UK Government, the Centre for the Protection of National Infrastructure (CPNI), the National Cyber Security Centre (NCSC) and CIR operators and owners

A Collaborative Approach to CIR

- A move from silo working to a holistic approach to critical infrastructure resilience
- A move from a culture of secrecy to a culture of sharing information appropriately between partners
- Improved relationships with critical infrastructure owners and operators
- Enhanced engagement with essential services owners and operators during disruptive events, resulting in improved response arrangements

- Enhanced engagement and influence with international critical infrastructure stakeholders, including Governments, Responders and Owner/Operators
- Enhanced engagement and influence with academia

An Empowered Approach to CIR

- Geographic Information System (GIS) Mapping Project for critical infrastructure resilience in Scotland
- Flood risk assessments for Critical Infrastructure sites in partnership with SEPA and Local Authorities
- Three Critical Infrastructure Resilience groups established as part of Resilience Partnership (RP) engagement
- The establishment of a critical infrastructure resilience governance structure in Scotland that uses existing resources, assets and arrangements (CIRP)
- Improvements to the resilience of critical infrastructure by owners and operators

An Improvement Approach to CIR

- The establishment of a Continuous Improvement approach to drive delivery of CIR across the CNI Sectors
- Stakeholder Impact Assessment (SIA) methodology established to assist sectors, owners and operators to consider their response to the 4 Big Questions – Criticality, Vulnerability, Preparedness and Mitigation
- Synergy with the future Infrastructure Investment planning arrangements
- Providing Ministers and the Scottish Resilience Partnership (SRP) with a Biennial report on Critical Infrastructure Resilience in Scotland

New CIR Strategic Vision

Our new Critical Infrastructure Resilience (CIR) Strategic Framework seeks to build on the successes of 'Secure and Resilient' by expanding our focus from Critical National Infrastructure (CNI) to the resilience of the wider Critical Infrastructure (CI) affecting Scotland. Building the resilience of Scotland's critical infrastructure is the responsibility of Government, Industry and the Responder Communities. We believe that this can be best achieved through a **Team Scotland** approach that seeks to **Keep Scotland Running** and **Keep Scotland Informed** before, during and after CIR related emergencies. This is why Scottish Government has worked with public and private CIR stakeholders across Scotland to develop this CIR Strategic Framework (see Annex C).

Purpose

Safeguarding Critical Infrastructure in Scotland through an all risks approach to Resilience in order to create sustainable economic growth and realise a Scotland where people are safe and feel safe.

Vision

To create a Scotland where our critical assets, systems and networks are resilient to all threats and hazards.

Guiding Principles

Mainstreaming - Provide leadership and direction to Critical Infrastructure Resilience (CIR) stakeholders promoting the message that Resilience is everyone's business.

Collaboration - Support and encourage stakeholder arrangements based on collaboration, cooperation and a shared commitment to enhance CIR in Scotland.

Prevention - Promote the assessment of risk and place preventative strategies at the forefront of our CIR continuous improvement approach.

Investment - Drive the delivery of CIR arrangements that seek to minimise disruption to the continuity of essential services in Scotland.

Strategic Priorities

Build on our 'All Risks' CIR model

- Taking a national and local risk assessment approach to CIR
- Includes all malicious threats and natural hazards
- Identifying the main risks and mitigating these in line with good business continuity principles
- Mitigation will be proportionate, realistic and achievable

Build on our existing CIR stakeholder arrangements

- Through a Cross-Sector approach
- Taking a collaborative, cooperative and shared commitment approach to the delivery of effective CIR in Scotland
- Building strong partnership engagement within the UK

Further enhance our 'Integrated' CIR approach

- Develop and implement a CIR delivery plan/programme to align with Ministerial expectations and Keeping Scotland Running – CIR Strategic Framework
- Identifying criticality, vulnerabilities, resilience levels and gaps
- Understanding Dependencies and Interdependencies between Sectors
- Developing coordinated and joined up solutions to address identified vulnerabilities
- Removing 'silo working' and breaking down the barriers between protective security and resilience work streams

Develop a culture of CIR Continuous Improvement

- Provision of a biennial Ministerial CIR Summary
- Establish an assurance framework that recognises the contribution of all CIR stakeholders
- Take an evidence-based, outcome-focussed approach to work programme delivery, which can measure success through effective governance
- Promote the concept of Business Resilience

Continue to influence CIR development Globally

- Collaborate with other CIR Stakeholders at home and abroad
- Providing a positive CIR vision for the future
- Engage in the International CIR Network (CIRINT.NET) in order to share best practice and learn from CIR initiatives - http://www.cirint.net/

New Guidance

Introduction

The 'Keeping Scotland Running' Guidance Suite seeks to support the delivery of Scotland's Critical Infrastructure Resilience (CIR) Strategy. It aims to provide operational guidance and advice for **Policy Leads**, **Responders** and **Operators** on key issues identified during consultation with key CIR stakeholders in Scotland, the UK and abroad. The Guidance Suite comprises seven separate guidance documents designed to equip and enable CIR stakeholders to work together in order to build resilience across the critical infrastructure sectors in Scotland.

Purpose and Format

The guides have been written and prepared in a common format for ease of reference. The intention is that stakeholders can refer to individual guides where the subject matter is of relevance to their needs. In turn, this will assist stakeholders in the development of common policy and best practice. The guides are designed to fill the gaps in existing guidance and to supplement existing business processes and industry guidance used by organisations to build resilience across their sectors. The guidance is not intended to duplicate or conflict with existing UK Government Critical National Infrastructure (CNI) work streams or other regulatory requirements in the area of critical infrastructure resilience.

Overview of the Guides

Guide 1 Critical Infrastructure Resilience (CIR) Stakeholder Collaboration

To encourage and enable effective partnership working and information sharing on critical infrastructure so that information is shared with the right people at the right time, identifying interdependencies and understanding vulnerabilities is improved, effective mitigation and response is delivered.

Guide 2 Identifying Significant Local Infrastructure

To set out practical approaches that can be used to identify significant local infrastructure, in order to inform the resilience preparedness assessment process and contribute to achieving the long term resilience of significant infrastructure through better understanding of Physical, Logical and People assets at a local level.

Guide 3 Dependencies and Interdependencies

To outline practical approaches that can be used to assess dependencies and interdependencies at site specific, regional and sector level, thus gaining a better understanding of vulnerabilities, impacts on other infrastructure and consequences when things do go wrong, which in turn will realise the benefit of more effective and proportionate mitigation action and multi-agency response to disruptive events.

Guide 4 Cyber Security and Critical Infrastructure

To establish a common cross-sector approach to Cyber Resilience and Critical Infrastructure and includes information on the key risks for Scotland, the impact that these may have on infrastructure, as well as information on the resources and support available to organisations.

Guide 5 Resilience to Natural Hazards

To establish a common cross-sector approach to building resilience to Natural Hazards through integration into existing collaborative risk management and planning processes, which are reviewed, and monitored to engender continuous improvement.

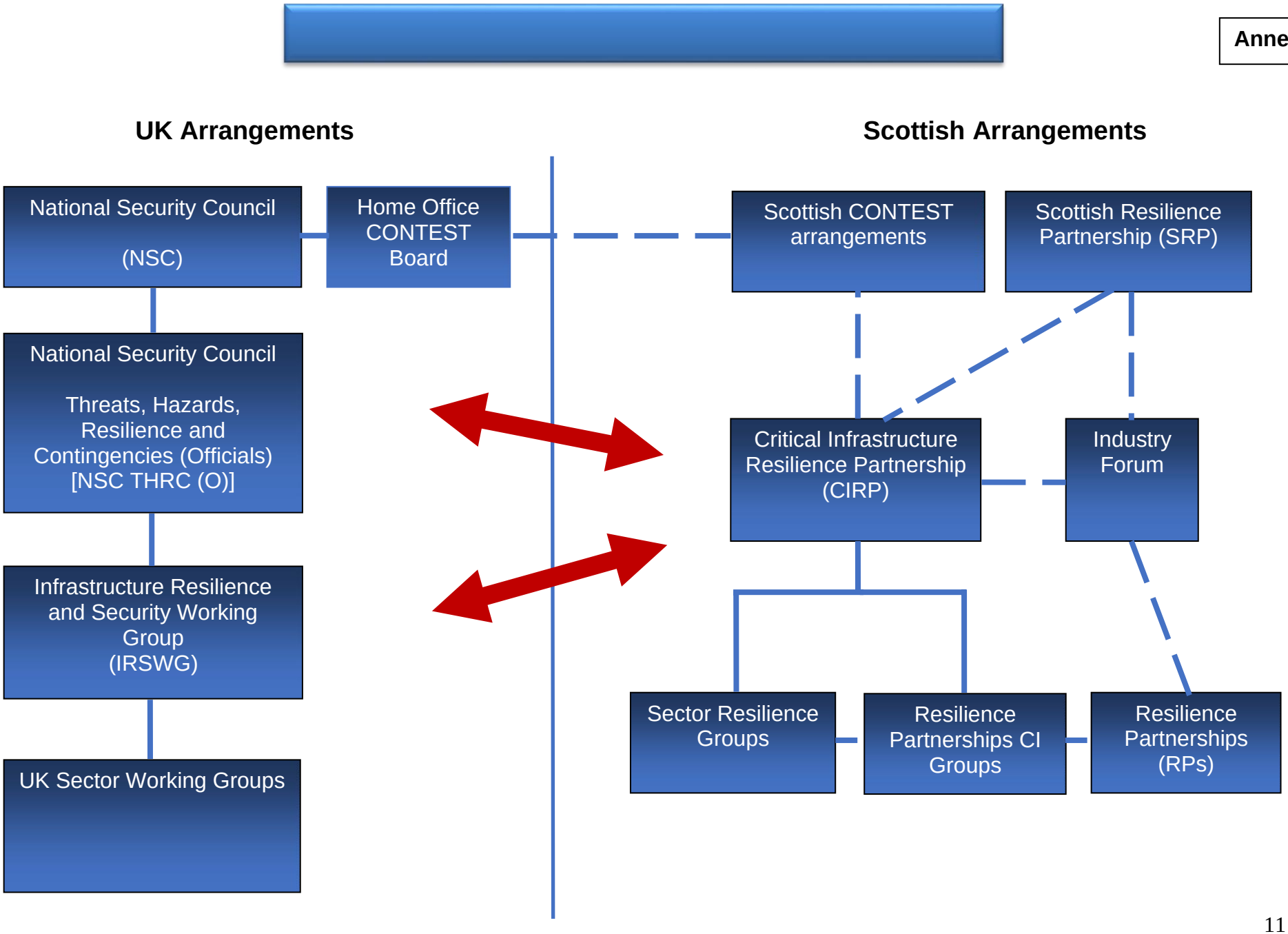
Guide 6 Building Resilience to a Changing Climate (Adaptation)

To provide relevant information to those responsible for critical infrastructure in Scotland to help build resilience to the impacts of the changing climate through, retrofitting existing infrastructure, adding redundancy into infrastructure networks, reducing future mitigation costs, use of more efficient technologies and ensuring that infrastructure organisations and professionals have the necessary skills and capacity to implement adaptation measures.

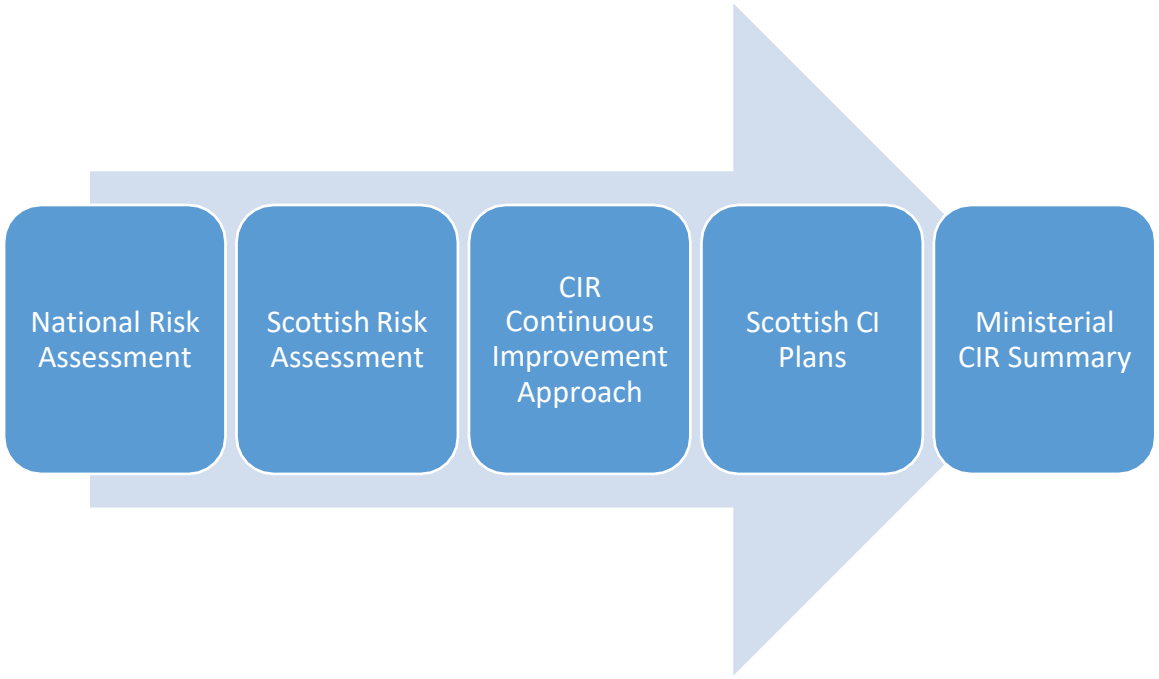
Guide 7 CIR Continuous Improvement Model

To establish a common cross-sector approach to continuous Critical Infrastructure Resilience (CIR) improvement in Scotland to realise the benefits that common standards, assessment and monitoring bring to the drive for enhanced organisational resilience.

Annex A


UK Arrangements
Scottish Arrangements
National Security Council
(NSC)
Home Office CONTEST Board
Scottish CONTEST arrangements
Scottish Resilience Partnership (SRP)
National Security Council
Threats, Hazards, Resilience and Contingencies (Officials) [NSC THRC (O)]
Critical Infrastructure Resilience Partnership (CIRP)
Industry Forum
Infrastructure Resilience and Security Working Group (IRSWG)
Sector Resilience Groups
Resilience Partnerships CI Groups
Resilience Partnerships (RPs)
UK Sector Working Groups

Annex B


National Risk Assessment
Scottish Risk Assessment
CIR Continuous Improvement Approach
Scottish CI Plans
Ministerial CIR Summary

Annex C

Purpose	**Safeguarding Critical Infrastructure in Scotland through an all risks approach to Resilience in order to create sustainable economic growth and realise a Scotland where people are safe and feel safe.**				
Vision	Create a Scotland where our critical assets, systems and networks are resilient to all threats and hazards.				
Principles	Leadership: 'We will seek to provide leadership through the provision of clear guidance and direction on Critical Infrastructure Resilience (CIR) in Scotland'	Collaboration: 'We are committed to developing stakeholder arrangements based on collaboration, cooperation and a shared commitment to enhance CIR in Scotland'	Improvement: 'Establish an assurance framework that seeks to monitor and support the continuous improvement of CIR in Scotland'	Delivery: 'Drive the delivery of CIR arrangements that minimise disruption to the continuity of essential services to the people of Scotland'	
Strategic Priorities	Build on our 'All Risks' CIR model: Taking a national and local risk assessment approach to CIR Includes all malicious threats and natural hazards Identifying the main risks and mitigating these in line with good business continuity principles Mitigation will be proportionate, realistic and achievable	Build on our existing CIR stakeholder arrangements: Through a cross-sector approach Taking a collaborative, cooperative and shared commitment approach to the delivery of effective CIR in Scotland Building strong partnership engagement within the UK	Further enhance our 'Integrated' CIR approach: Develop and implement a CIR delivery plan to align with ministerial expectations Identifying criticality, vulnerabilities, resilience levels and gaps Understanding Dependencies and Interdependencies between Sectors Developing coordinated and joined up solutions to address identified vulnerabilities Removing 'silo working' and breaking down the barriers between protective security and resilience work streams	Develop a culture of Continuous Improvement: Provision of a biennial Ministerial CIR Summary Establish an assurance framework that recognises the contribution of all CIR stakeholders Take an evidence-based, outcome-focussed approach to work programme delivery, which can measure success through effective governance Promote the concept of Business Resilience	Continue to influence CIR development Globally: Collaborate with other CIR stakeholders both at home and abroad Providing a positive CIR vision for the future Engage in the International CIR Network in order to share best practice and learn from CIR initiatives

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Guide 1
Critical Infrastructure Resilience (CIR) Stakeholder Collaboration

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 1

Critical Infrastructure Resilience (CIR) Stakeholder Collaboration

Overview

What	This guide seeks to: • Encourage and enable effective partnership working and information sharing on critical infrastructure resilience
Who	This guide is aimed at: • **Government** – CI Resilience Policy leads in Scottish Government • **Critical Infrastructure (CI) Operators** – Strategic Management, Resilience and Business Continuity Management (BCM) leads • **Responder Communities** – Regional Resilience Partnerships (RRPs), Local Resilience Partnerships (LRPs)
Why	Stakeholder Collaboration is a Guiding Principle of the CIR Strategy. Stakeholder collaboration promotes and helps: • CI information being shared with the right people at the right time • Identify interdependencies • A better understanding of vulnerabilities • Mitigation action to be taken • Provide a better understanding of the consequences when things do go wrong • More effective multi-agency response
How	Ensure that information on CI is shared with the right people at the right time, taking into account commercial sensitivities and protective markings. Available tools include: • Resilience Direct (RD) – https://collaborate.resilience.gov.uk/ • Information Sharing Protocols (ISPs) (see **Annex A**) • Non-Disclosure Agreement (see **Annex B**) • HMG Personnel Security Controls – Right Issue, Right Time, Right Level, Right Assessment (see **Annex C**) • Cabinet Office Guidance "Keeping the Country Running" – Critical Infrastructure Owner/Operator – Categories of Information for lead category 1 Responders (see **Annex D**)

KEEPING SCOTLAND RUNNING

Case Study

Establishing a Local Multi-agency Critical Infrastructure Resilience Group

With the approval of Scottish Government, a local multi-agency 'Critical Infrastructure' Group was established in the West of Scotland. Membership was drawn from local authority areas, emergency services, utility companies, the Scottish Environmental Protection Agency, Scottish Government, Police, the Centre for the Protection of National Infrastructure and the Ministry of Defence.

The primary focus was to make better use of local knowledge, particularly Counter Terrorist Security Advisors (CTSAs) and local industry/critical site owners, to improve the resilience and protective security of critical sites and Critical National Infrastructure (CNI) in the local area.

The group encouraged greater partnership working at a local level, in order to develop a better multi-agency approach to address crises or serious incidents occurring.

A significant challenge for the group was developing an environment where both security related and commercially sensitive information could be shared safely and appropriately.

Key to the process was the development of an Information Sharing Protocol for members (see Annex A).

The protocol proved to be extremely useful in live situations, where members of the group were able to exchange sensitive information due to the existing relationship and trust that had already been developed.

The group also participated in a Cabinet Office Pilot Project which looked at information sharing and understanding interdependencies at a Critical Infrastructure asset belonging to the Police.

Key to this process was the development of a non-disclosure document to ensure sensitive commercial information was not distributed or made available inappropriately to competitor organisations involved in the project (See Annex B).

The group also utilised:

- HMG Personnel Security Controls – Right Issue, Right Time, Right Level, Right Assessment (see Annex C)
- Cabinet Office Guidance "Keeping the Country Running" – Critical Infrastructure Owner/Operator – Categories of Information for Lead Category 1 Responder (see Annex D)

KEEPING SCOTLAND RUNNING

Background

Scotland's critical infrastructure is a complex interconnected number of assets, systems and networks, providing essential services to the People of Scotland. This Guide has been developed to support infrastructure owners and operators, emergency responders, and government departments to work together to improve the resilience and security of critical infrastructure and essential services in Scotland. This document supports the framework provided by the Civil Contingencies Act 2004[4] (CCA), which forms the legal basis for emergency preparedness in Scotland and across the UK and the duty to share information for the purposes of improved emergency planning.

For detailed information on the obligations for information sharing and cooperation that underpin the normal day to day exchange of information between those involved in resilience planning, reference should be made to:

- The Civil Contingencies Act (CCA) 2004 (Contingency Planning) (Scotland) Regulations 2005[5];
- Ready Scotland, which is the Scottish Government civil emergencies website containing a suite of guidance and useful resources[6];
- Preparing Scotland[7], a Scottish Government publication containing a hub of guidance to assist Scotland plan, respond and recover from emergencies. While produced by the Scottish Resilience Development Service (ScoRDS) there is a core emphasis on coordination as a successful Preparing Scotland is one that is developed and owned by the resilience community.

To achieve successful long term enhancement of CIR, it is crucial that effective Stakeholder Collaboration (partnership working and information sharing) is one of the guiding principles applied by Government, Industry and Responder Communities during the Integrated Emergency Management (IEM) process of 'Anticipation', 'Assessment', 'Prevention', 'Planning', 'Response' and 'Recovery'.[8] The aim of IEM is to develop flexible and adaptable arrangements for dealing with emergencies, whether foreseen or unforeseen. It is based on a multi-agency approach and the effective co-ordination of those agencies. Whilst an individual commitment to this process is important, experience shows that working together greatly increases effectiveness. All involved should therefore ensure that you have explored fully the benefits of collaborative working, training and exercising. In doing this you will gain the benefits of partnership working, maximise effectiveness and, in large part, meet you duty of cooperation under the CCA.

---

[4] https://www.legislation.gov.uk/ukpga/2004/36/contents
[5] http://www.legislation.gov.uk/ssi/2005/494/contents/made
[6] https://www.readyscotland.org/
[7] https://www.readyscotland.org/
[8] See Chapter 3, *Integrated Emergency Management: Guidance and Principles* for further reading at: https://www.readyscotland.org/media/1457/preparing-scotland-hub-updated-published-version-august-2018.pdf

It is therefore the principles of collaboration and partnership working which the present guide seeks to foster.

Guidance

General – All Stakeholders

Protection vs Sharing: Striking a balance

A pragmatic balance needs to be struck between the protection and sharing of CI information to ensure security does not become a major barrier to effective stakeholder collaboration.

If the security of CI information is compromised this could increase the vulnerability of an asset or assets to attack. Therefore, sensitive information which may help identify the significance or importance of an asset, its vulnerabilities or security arrangements should be appropriately protected. Applying too high a protective marking to CI information on the other hand will create barriers to legitimate access to the information, adversely impacting on the efficiency and effectiveness of those involved in CI resilience work.

How is this tension resolved? Useful guidance on the key principles, classification definitions, handling and storage instructions as well as protecting assets and infrastructure, can be found in the Cabinet Office publication 'Government Security Classifications May 2018', available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

A proportionate approach to the security classification of sensitive information can also be found in the UK Government's framework for protectively marking sensitive information, contained in the Cabinet Office publication HMG Security Policy Framework (SPF).[9] The framework is impact driven in that it takes account of the likely consequence of the information being compromised. In applying this guidance, all government departments and agencies must adhere to the SPF.

The UK Government operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. This comprises three levels: OFFICIAL, SECRET and TOP SECRET for which there are distinct security arrangements. OFFICIAL covers most of the day-to-day business of government, service delivery, commercial activity and policy development. SECRET and TOP

[9] HMG Security Policy Framework: www.cabinetoffice.gov.uk/resource-library/security-policy-framework

SECRET information will typically require bespoke, sovereign protection, but OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation. In this way government can deliver securely and efficiently, and shape its services to meet the user needs.

This system is designed to ensure that access to information is correctly managed and safeguarded to an agreed and proportionate level throughout its lifecycle from creation, processing, storage and transmission through to destruction. It is designed to protect information (and other assets) from accidental or deliberate compromise and CI information must be classified, handled and stored in line with its requirements.

One other way of enabling the discussion is to declassify the information, by either removing or summarising particularly sensitive information such as information about asset vulnerabilities. This may still enable key information/messages to be included and shared but at a lower protective marking.

'Sanitising' information in this way respects the principle of 'Right issue, Right time, Right level' (as outlined in **Annex C**), in line with the Civil Contingencies Act and Preparing Scotland.

Overall, success of the balanced approach to the protection and sharing of CI information is dependent upon establishing effective relationships between Government, CI Operators and Responders.

Government - CI Resilience Policy Leads

The Scottish Government Directorates with policy lead for the CNI sectors have a leadership role to play in delivering effective stakeholder arrangements based on collaboration, cooperation and a shared commitment to enhance CIR in Scotland.

CI Operators – Strategic Management, Resilience and BCM LeadS

Upon request from a lead Category 1 responder within a Regional Resilience Partnership (RRP) Critical Infrastructure group, owners of critical infrastructure should collaborate and provide information from their BCM process on any critical infrastructure that provides essential services within the RRP area (whether the infrastructure is located within or out with the area). This should include sites where a response or support may be needed from emergency responders to manage

the consequences of civil emergencies. See **Annex D** for further guidance on the categories of information to provide to a Category 1 responder.

CI operators/owners should give consideration to facilitating visits for the police and Fire & Rescue Service (and other Category 1 responders as appropriate) to the most critical sites, to establish familiarisation of access to the site; location of critical components/equipment, site operators and their actions in a crisis; and back-up arrangements, to understand the recovery process and timetables. This aligns to similar good practice for civil nuclear and chemical sites under the Radiation (Emergency Preparedness and Public Information) Regulations 2001 (REPPIR) and the Control of Major Accident Hazards Regulations 2015 (COMAH). For those sites that are part of the CNI and have not previously had engagement with police and Fire & Rescue Service planners, any proposed initial contact and visit must only be conducted after consultation with the local CTSA.

Responder Communities – RRPs, LRPs and RRP CI Groups

This guidance outlines a process for Category 1 and 2 responders[10] that is intended to support their statutory information sharing obligations and to enable the Responder Communities to receive the necessary information on critical infrastructure to carry out their duties to best effect.

To achieve this, there is a need to share information on critical infrastructure prior to an event in order to ensure that appropriate plans are in place to respond and recover from a CIR related emergency.

It is therefore necessary to understand:

(a) What infrastructure provides essential services in an area, and its dependencies
(b) The risks (likelihood and impact) of disruption to that infrastructure from natural hazards and threats
(c) The assumptions being made about assistance from emergency services and other RRP partners e.g. pumping of flood waters by the Scottish Fire and Rescue Service (SFRS)

An agreed lead Category 1 Responder from the RRP Critical Infrastructure group may request information on critical infrastructure within the area from Category 2 responders (and other owners of critical infrastructure who are prepared to provide information under these arrangements).

[10] Schedule 1, CCA 2004: https://www.legislation.gov.uk/ukpga/2004/36/schedule/1

It should be noted that ***labelling infrastructure as 'CNI' within emergency plans is not permitted.*** Plans will be shared with relevant Lead Government Body[11] so they can be assured key sites have been prioritised appropriately.

RRPs/LRPs will also produce their local 'Risk and Preparedness Assessments' based on the Scottish Government, Ready Scotland Guidance[12] and the National Risk Assessment (NRA), a classified assessment of the risks of civil emergencies facing the UK. The National Risk Register of Civil Emergencies[13] (NRR) is an unclassified version of the National Risk Assessment (NRA) and useful resource. This process should also identify the hazards and threats that could affect the RRP/LRP area and the potential consequences of these (including the impact on the provision of essential services in the area).

Critical infrastructure groups (RRP-CI) have been established in each of the Regional Resilience Partnership (RRP) areas to ensure that Regional Resilience Partnerships have effective liaison with Critical Infrastructure operators and owners and arrangements to prevent or minimise impacts resulting from loss or disruption to critical infrastructure.

Whilst detailed delivery may vary between RRP-CI groups, the above aim is generally achieved through the following four work-streams:

What is critical?

- Identify and collate information relating to Significant Local Infrastructure sites in each of the RRP areas, feeding into RRP Communality Risk Register processes for strategic context.

What are the vulnerabilities?

- Develop work streams to improve our understanding of the vulnerabilities and interdependencies for key Significant Local Infrastructure sites

How Resilient are they?

- Utilising the tripartite approach[14] explore and understand resilience issues

What do we need to do?

- Maintain an overview of critical infrastructure resilience within the RRP area and develop capabilities to assess and understand the impacts and consequences of

[11] Reserved Sectors / Sub-Sectors – UK Government Department, Devolved Sectors / Sub-Sectors – Scottish Government

[12] https://www.readyscotland.org/media/1444/are-we-ready_-december-2017.pdf

[13] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

[14] A three way relationship between Government (Scottish Government and/or UK Government), CPNI/NCSC (as the security advice specialist) and Critical Infrastructure owners and operators

the wider loss of essential services affecting organisations and communities
- Understand human behaviour responses to the consequences of loss of critical infrastructure and essential services
- Oversee preparedness of the RRP for CI disruptions in terms of Category 1 and 2 responder communities
- Provide reassurance to the RRP that Critical Infrastructure issues are being addressed
- Identify areas of work which require cross regional cooperation
- Develop a suitable Information Sharing Protocol

Police Counter Terrorist Security Advisors (CTSAs) are represented in the RRP CI groups and provide regular briefings to RRPs and LRPs, on the CI within their area. Information on Critical Infrastructure should be provided at the RRP/LRP during civil emergencies for the purpose of enabling an effective emergency response in line with the 'need to know' principle that access to sensitive information must be shared no wider than necessary to provide for the efficient conduct of an emergency response and limited to those with an identified need and the appropriate personnel security control[15].

Delivery

The following tools may assist in the delivery of the collaborative relationship which this Guide seeks to foster.

Critical Infrastructure Resilience International Network (CIRINT.NET)

Between 2013 and 2015 the Scottish Government Resilient Essential Services Team and Police Scotland participated in an EU funded project together with EU partners, to promote collaboration and the development of good practice on Critical Infrastructure Resilience (CIR) in Europe.

During the course of the project a vast range of CIR stakeholders, within Government, CI Operators (both public and private sector organisations), responders and academia from throughout Europe and farther afield, collaborated with the partners to deliver the project objectives and for mutual CIR benefit.

The overwhelming opinion of those who collaborated in the project was that there was a pressing need within the CIR community for a Critical Infrastructure Resilience International Network and consequently one should be developed as the lasting legacy of the project.

[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf, at p5

KEEPING SCOTLAND RUNNING

Scottish Government and partners in Lombardy, Kennemerland and the Basque Region have developed this concept into a fully functioning, living and dynamic network of regions across the World, collaborating on critical infrastructure resilience, sharing good practice and learning from one another. The network is known as **CIRINT.NET**.

The network is designed to be somewhere you can go when you're looking for help or assistance, or just some advice in your specific subject of Critical Infrastructure Resilience. A trusted and accessible source, so that you don't have to re-invent the wheel or spend weeks researching. Somewhere you can access and share good practice, experience and expertise from an international network of practitioners, academics, responder organisations, industry or National and Regional government departments.

With a global reach, covering 17 Regions across Europe, the US, Australia and Canada, the International Critical Infrastructure Resilience Network (CIRINT.NET) hosts a website and secure discussion forum that brings practitioners together to share knowledge, experience and expertise through international collaboration.

CIRINT.NET is a voluntary association and no enforced commitment or participation is assumed.

It provides:

- Information sharing
- Collaboration
- Good practice
- Academic papers
- Learning
- Benchmarking
- Peer review
- Networking
- Free membership.

KEEPING SCOTLAND RUNNING

As a community concerned with critical infrastructure resilience issues, CIRINT seeks to provide a platform to connect practitioners who shape the future evolution of CIR strategy, policy and delivery.

Depending on individual access requirements, you can choose between Open and Secure discussion areas. Open discussion areas cover Resilience Education, Communities and General, whilst the secure discussion areas cover Energy, Health, Water, Food, Government, Emergency Responders, Transport, Civil Nuclear, Communications, Finance, Space, Chemical and Defence.

CIRINT.NET is your asset but will only be as useful and successful as the participants who use it.

A framework and Terms of Reference for the network has been developed and is available through the website at http://www.cirint.net/.

Membership and participation is now available. To register as 'Members' (Organisations) and 'Participants' (Individuals) please apply through the website at http://www.cirint.net/.

Resilience Direct

Resilience Direct is a government sponsored secure web-based platform for the resilience community to share information amongst all Category 1 and 2 emergency responders and organisations to assist with planning, response and recovery to major emergencies. It has been designed by the end user for the end-user.

Resilience Direct has been accredited to the Security classification 'Official'. This allows documentation to be shared securely amongst nominated individuals providing instant access to real-time information. The system also provides a content management system in conjunction with mapping capability.

With Resilience Direct you can:

- Gain access to resilience contacts who can be searched for, messaged instantly and create groups with, to give you immediate response in an emergency.
- Create, amend and share documents securely with colleagues in any location without worrying about file size or type, with instant notifications to keep you up to date.

- Create and query maps from the latest OS data so you know you have the latest information about any location and match these with live data feeds, including met office rainfall and Environment Agency flood data.

Resilience Direct is a robust platform that provides the tools and information to plan and respond to emergencies and may be accessed at:
https://collaborate.resilience.gov.uk/

Information Sharing Protocols and Non-Disclosure Agreements

The Civil Contingencies Act permits the use of information sharing protocols/agreements to formalise information sharing arrangements. The Strathclyde SECG multi-agency Critical Infrastructure Group has developed the following protocols to aid information sharing:

- Information Sharing Protocol (ISP) (see **Annex A**)
- Non-Disclosure Agreement (NDA) (see **Annex B**)

These tools aid the development of a multi-agency environment where information can be shared safely and appropriately, whilst ensuring that sensitive commercial information is not distributed or made available inappropriately to competitor organisations.

Annex A

INFORMATION SHARING PROTOCOL (ISP)

Established by

[Insert group/consortium name]

Version 1.0

KEEPING SCOTLAND RUNNING

Annex A

INDEX

SUMMARY SHEET

Annex A

INFORMATION SHARING PROTOCOL WITHIN THE [Insert name of group/consortium]

ISP Ref:	**[*To be completed by.....insert ISP record keeper e.g. Records Management, Company Headquarters*]**

PURPOSE	**To regulate the sharing of information among members of the [insert name of group/consortium]**

PARTNERS	**[Insert names of member organisations]**

Date Agreement Comes into Force	

Date of Agreement Review	**Annually or when amendment is identified**

Agreement Owner	**[Insert details Chief Officer or organisation chairing the Group]**

Agreement Drawn up by:	**[Insert details of ISP administrator]**

Location of Agreement	**[Insert details of location where principle signed document is stored]**

VERSION RECORD

Version No.	Amendments Made & By Whom
V1.0	First Version
V1.1	
V1.2	
V1.3	
V1.4	

KEEPING SCOTLAND RUNNING

Annex A

1. INTRODUCTION

The [Insert name of group/consortium] has responsibility for monitoring, developing, and addressing critical infrastructure related issues within the [Insert name of area] area. This may also include certain issues relating to sensitive information.

For the purposes of this document, “Sensitive Information” refers to [Describe the information] within a geographical area [Insert details of area (If applicable)]

The Group is chaired by [Insert details of chair and organisation] who also has responsibility for secretariat functions of the Group/Consortium, and administration of its various work-streams. Membership includes [Insert membership]. In addition, other organisations [List organisations if known] may also be invited onto the Group. Finally, the Group may – on an *ad hoc* basis – invite membership from other persons or bodies whose particular professional, technical or academic qualifications or experience may be thought of assistance to its work.

2. PURPOSE

The purpose of this Protocol is to regulate the procedure for and circumstances in which information may be shared among members of the Group/Consortium. It is intended that information is shared where appropriate, and disseminated in a manner that ensures its secure management.

This Protocol will assist in coordination among members and [Insert aim/purpose of the information sharing].

The benefits obtained in information to be shared has to be balanced against the harm that can be caused to national security, public safety, commercial confidentiality or the rights of individuals. Similarly, the use of information has to be with care to ensure that information shared is not misused.

3. PARTNERS

This Protocol is among the following partners who are members of the Group/Consortium:

- [Insert list of member organisations]

Point of Contact/members: - Names, contact details, organisation and roles are listed in Appendix 1.

Annex A

4. POWERS

The 2004 Act and delegated legislation under it, and the Scottish Government document 'Preparing Scotland' (2007), makes it clear that there is a need for Category 1 and 2 responders to share information for the purposes of civil contingency response and improving resilience. However, this is a general expectation of information sharing: sensitive information requires to be managed and stored securely.

Such information sharing will, as appropriate, also be in accordance with the provisions of

- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Freedom of Information (Scotland) Act 2002

5. PROCESS

5.1 GUIDANCE

It is incumbent on all Group/Consortium members to recognise that any information shared in terms of this Protocol must be shared appropriate to need, and be managed and secured appropriately. A record must be kept of the information being shared and the parties sharing it.

Adherence to this Protocol – and to the obligations to which it refers – shall be monitored through the Chair of the Group. It will be for the Chair of the Group, as required, to inform any Group member of their breach, or apparent breach, of their obligations; to recommend appropriate remedial action and to remind them of the relevant sanctions for repeated, or further, breaches. Those nominated to be Points of Contact and their substitute shall be satisfactorily vetted to a minimum of 'Baseline Security Standard'. Dependent on the sensitivity of work being undertaken, it may be necessary to obtain SC clearance. Decisions as to the appropriate vetting level requirements for members will rest with the Chair of the Group/Consortium.

5.2 TYPES OF INFORMATION TO BE SHARED

The Group will share information on:

- [Insert types of information]
- …….
- ……..
- ……..
- ……

- other pertinent information with relevance to the work of the Group/Consortium

5.3 CONSTRAINTS ON THE USE OF THE INFORMATION

The information which is shared among members only in consequence of the operation of this Protocol (and not otherwise) must not be disclosed to any third party without the written consent of the member that provided the information, and the approval of the Chair of the Group.

Notwithstanding that all members do not currently conform to the Government Protective Marking Scheme (GPMS) guidelines (See link - https://www.gov.uk/government/publications/government-security-classifications); all information shared in accordance with this Protocol must be handled in a manner which will comply with these guidelines.

Only some of the members of the Group are "public authorities" in terms of the Freedom of Information (Scotland) Act 2002 ('the 2002 Act'). All information which is shared in terms of this Protocol and which is in the hands of any Group member which is also a public authority in terms of the 2002 Act may, then, fall within the ambit of any relevant request for information received by that member (i.e. the public authority) under the 2002 Act. It will, in the first instance, be for the member in receipt of the request to determine what exemption – if any – may apply under the 2002 Act, however, that member will consult with the other member(s) in the Group from whom the information originated to seek their views on its disclosure (full or partial) or not. The Chair of the Group will also be consulted.

5.4 ROLES AND RESPONSIBILITIES UNDER THIS AGREEMENT

[Insert name of organisation] has responsibility for the chairing, management and administration of the Group/Consortium and its activities. It will ensure that all members receive briefings, discussion and other papers. In addition, it will co-ordinate and manage further work of sub groups which may be established.

Individual members of the Group/Consortium must nominate a Point of Contact/member, who will have responsibility for ensuring the management and use of information obtained via the group/consortium is stored and shared in a way that does not compromise any of the other partner organisations, or which fails to comply with the guidance provided in this document.

Should the Chair of the Group/Consortium determine that there has been a breach, or apparent breach, of this Protocol on the part of any member, then that shall be brought to the attention of the person who is the Point of Contact (as set out in Appendix 1) for that member – or some satisfactory alternative as determined by the Chair of the Group/Consortium. The member will be informed of the circumstances of the breach and remedial measures required to be put in place. If determined necessary by the

Chair of the Group/Consortium, the operation of this Protocol may be suspended for that member, until appropriate and satisfactory measures are in place to remedy the breach.

5.5 SPECIFIC PROCEDURES

All types of information shared with members will be recorded on a Log, which will be maintained by the Chair of the Group/Consortium. The Log will record a sufficient description of the details of information shared and the members who received it. Recipients will be advised of the appropriate GPMS marking level for the information, to allow appropriate storage/security measures to be employed, and that GPMS marking level will also be recorded in the Log.

5.6 SHARING OF INFORMATION UNDER THIS ISP WITH OTHERS

Information which is shared with Partners under this Protocol may also, and at the discretion of the Chair of the Group/Consortium, be shared with [Insert details of other groups/consortiums/organisations] established elsewhere in Scotland. Information shall only be shared for the Purpose articulated at Section 2 above.

Information which is shared with Partners under this Protocol may also, and at the discretion of the Chair of the Group/Consortium, be shared with appropriate representatives of Her Majesty's Government.

6. RETENTION, REVIEW & DELETION

Members of the Group/Consortium agree that information shared under this Protocol will only be used for the specific purpose for which it is intended. The recipient of the information is either required to keep it stored in accordance with the Cabinet Office Security Policy Framework (SPF) https://www.gov.uk/government/publications/security-policy-framework , or if this is not possible, in commensurate safe storage conditions as agreed with the Group/Consortium Chair.

Should any information have a GPMS marking level of OFFICIAL-SENSITIVE, or above, requiring safe storage in compliance with the Security Policy Framework, consideration should be given to storing the information in the most appropriate facility.

Any information exchanged in terms of this ISP should be reviewed at least on an annual basis to ensure that its continued retention is appropriate. It should also be deleted/destroyed when it is no longer required.

7. REVIEW OF THE INFORMATION SHARING AGREEMENT

This Protocol will be reviewed annually or when amendment is identified.

Annex A

8. INDEMNITY

Members of the Group/Consortium who cause loss, injury or damage to other members by reason of their negligent failure to adhere to this Protocol shall fully indemnify those other members.

9. GOVERNMENT AGENCIES

UK Government and Scottish Government are all fully compliant with the Security Policy Framework, and are subject to the Government Protective Marking Scheme (GPMS).

10. SIGNATURES

All signatories accept responsibility for the member on whose behalf they sign. Staff are to be trained so that there will be adherence to the Protocol and to relevant legislation in its operation.

Signed on Behalf of Member Organisation:

Organisation: .....

Signature: .....

Print Name: .....

Position: .....

Date: .....

[Repeat above information for all member organisations]

Annex A

List of Group Members

Name	Role	Organisation	Contact Details	Comments (e.g. Single point of Contact)

Annex B

Non-Disclosure Agreement Template

NON-DISCLOSURE AGREEMENT

Between

[Insert name of group/consortium] constituted under [Insert appropriate legislation (If applicable)]

and

[Insert name of organisations]

WHEREAS

The parties wish to disclose certain technical and/or financial and/or commercial information to each other, in connection with [Insert type of sensitive information] located within the [Insert name of area (if applicable)] for the purpose of [Insert purpose]

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS

"Affiliate"	Means in relation to [Insert name of organisation/company], any subsidiary, subsidiary undertaking or holding company of this body corporate, and any subsidiary or subsidiary undertaking of such holding company for the time being as deigned in Section 1159 of the Companies Act 2006;
'Commencement Date'	Means the last date of execution of this Agreement;
'Confidential Information'	Means any information, processes, strategies, data, know-how, trade secrets, designs, photographs, drawings, specifications, technical literature and other tangible and intangible information or material, whether in oral, written (including copies), graphic or electromagnetic form disclosed by the Disclosing Party either before or after the Commencement Date;
'Disclosing Party'	Means the party disclosing the Sensitive Information in terms of this Agreement;

'Receiving Party'	Means the party receiving the Sensitive Information in terms of this Agreement;
'Working Day'	Means a day (not being a Saturday or Sunday) on which the banks are open for normal banking business in Scotland.

2. Duty

2.1 For Sensitive Information that is disclosed by the Disclosing Party to the Receiving Party, the Receiving Party shall do the following for a period of 4 (four) years from the Commencement Date:-

a. Keep in strict confidence and in safe custody any Sensitive Information disclosed to the Receiving Party by the Disclosing Party by exercising the same duty of care used to maintain as confidential the Receiving Party's own Sensitive Information and at a minimum a reasonable duty of care;

b. Not use or exploit any Sensitive Information other than for the Purpose;

c. Not copy or reproduce any or all of the Sensitive Information except as is reasonably necessary for the Purpose; and

d. Not distribute, disclose or disseminate Sensitive Information to anyone, except, as defined in Clause 2.2 below, persons who have a need to know such Confidential Information for the Purpose.

2.2 Persons who have a need to know include persons who are employed by or are directors, officers, contractors or consultants of the Receiving Party and in respect of [Insert details as appropriate], shall also include an Affiliate. The Receiving Party shall notify all such persons of the existence of this Agreement at the time the Sensitive Information is disclosed to them.

3. Exceptions

The Receiving Party's duty to maintain Sensitive Information in accordance with the provisions of this Agreement shall not apply to Sensitive Information that:

(a) Was known to the Receiving Party (without obligation to keep the same sensitive) at the date of disclosure of the Sensitive Information by the Disclosing Party; or

(b) Is after the date of disclosure acquired by the Receiving Party in good faith from an independent third party who is not subject to any obligation of confidentiality in respect of such Sensitive Information; or

(c) In its entirety was at the time of its disclosure in the public knowledge or has become public knowledge during the term of the Agreement otherwise than by reason of the Receiving Party's neglect or breach of the restrictions set out in this or any other agreement; or

(d) Is requested or required to be disclosed by any court of competent jurisdiction, applicable law, or regulatory authority, or the regulations of any recognised stock exchange on which the Receiving Party's shares are listed of the Disclosing Party's Sensitive Information, provided that, prior to such disclosure or where that is impractical, as soon as reasonably possible thereafter, the Receiving Party shall notify the Disclosing Party (to the extent permitted by law) as to the proposed (or as the case may be, actual) form, nature and purpose of the disclosure and at the same time gives the Disclosing Party a copy of the disclosure so made; or

(e) Without prejudice to sub-paragraph (d) is disclosed in accordance with the Freedom of Information (Scotland) Act 2002. Before reaching a decision leading to the disclosure of information, where it is reasonably practicable to do so, the Receiving Party shall notify the Disclosing Party of the request for information and of the information to be disclosed and shall consider any representations that may be made by the Disclosing Party as to the possible application of exemptions and as to the balance of the public interest, where relevant, but nothing in this clause shall require the Receiving Party to delay disclosure in accordance with its statutory obligations. The decision of the Receiving Party in relation to disclosure shall be final; or

(f) Is independently developed by the Receiving Party without access to any or all of the Sensitive Information.

4. Termination and Renewal

This Agreement shall expire on a date that is [Insert duration] from the Commencement Date unless terminated earlier upon written agreement between the Parties. This Agreement shall not be renewed or extended unless agreed in writing between the Parties.

5. Return of Sensitive Information

On the earlier of either the expiration of the term of this Agreement, termination of this Agreement, or a written request of the Disclosing Party, the Receiving Party shall return or destroy (at the Receiving Party's option) within five (5) Working Days any part of the Sensitive Information that consists of original, and copies of, source material provided by it and still in the Receiving Party's possession and, if requested by the Disclosing Party, shall provide written confirmation to the Disclosing Party to that effect.

6. Exclusion of Warranties

Neither Party warrants the accuracy or completeness of any Sensitive Information and all implied warranties to that effect are hereby excluded.

7. Title

Nothing in this Agreement shall be construed as granting or conferring any rights in title to, or licence in respect of, any Sensitive Information. All Sensitive Information shall remain at all times the property of the Disclosing Party.

8. Transactions and Press Releases

8.1 The disclosure of Sensitive Information by the Disclosing Party will not create an obligation on either Party to enter into any further agreement or to proceed with any possible relationship or other transaction.

8.2 Without prejudice to the provisions of Clauses 3 (d) and (e) of this Agreement, neither Party shall disclose the existence of this Agreement or issue any press releases relating to the Purpose to any third party without the other Party's consent.

9. No Partnership

Nothing contained in this Agreement shall be construed as creating a joint venture, power of attorney, partnership or employment relationship between the Parties, it being understood that the Parties are independent entities in respect of one another. Except as specified herein, neither Party shall have the right, power or implied authority to create any obligation or duty, express or implied, on behalf of the other Party hereto.

10. Anti Bribery and Anti Corruption

Each party shall:
(a). comply with all applicable laws, regulations, codes and guidance relating to anti-bribery and anti-corruption, including but not limited to the Bribery Act 2010 ("Relevant Requirements"); and

(b). have and shall maintain in place throughout the term of this Agreement, and enforce where appropriate, its own policies and procedures to comply with the Relevant Requirements, including but not limited to adequate procedures under the Bribery Act 2010.

For the purpose of this Clause 10, the meaning of adequate procedures shall be determined in accordance with section 7(2) of the Bribery Act 2010 (and any guidance issued under section 9 of that Act)

11. Waiver

No delay or omission by either Party in exercising any right, power or remedy provided by law or under this Agreement shall affect that right, power or remedy or operate as a waiver of it.

12. Notice

Any notice will be either delivered in person, or sent to the other Party by (a) postal mail, (b) facsimile (electronically confirmed and followed up immediately by postal mail), or (c) electronic mail (followed up immediately by postal mail). A notice is considered given when it is delivered (which in the case of a facsimile or email shall be when the follow up copy of the facsimile or email sent by postal mail is delivered). For the purposes of this Agreement, the address of each Party shall be:

[Insert details as appropriate]	[Insert details as appropriate]
XXXXXXXXX	XXXXXXXXXXXXX

13. Entire Agreement

Save in respect of fraudulent misrepresentation by either Party, the Agreement constitutes the entire understanding between the Parties with regard to the disclosure of the Sensitive Information relating to the Purpose.

14. Non Assignation

Neither Party may assign or otherwise transfer this Agreement, or any of its rights and obligations hereunder, to any third party, except for the purposes of sharing Sensitive Information on a need to know basis as specified in this Agreement.

15. Remedy

Each Party agrees that damages may not be an adequate remedy for any breach of this Agreement and each Party shall be entitled to seek appropriate remedies for any reasonably threatened or actual breach of this Agreement.

16. Governing Law

This Agreement will be governed by the Law of Scotland and subject to the jurisdiction of the Scottish Courts.

IN WITNESS WHEREOF these presents consisting of this and the five preceding pages are executed as follows:

Subscribed for and on behalf of [Insert name of organisation] **on** [Insert date]

(Date)
Signed…..(Authorised Signatory)

Name…….

Date

Signed…..(Witness)

Name of Witness……

Occupation……

Address…….

Subscribed for and on behalf of [Insert name of organisation] **on** [Insert date]

(Date)
Signed…… (Authorised Signatory)

Name…….

Date

Signed…… (Authorised Signatory)

Name…….

Date

[Repeat above information for all participating organisations]

Annex C

Right issue, right time, right level

Table 1: "Right issue, right time, right level" Assessment [16]

Issue	Time	Level
Information on critical infrastructure (includes CNI)	Before emergency for CIR work, including civil emergency planning	Held by appropriate personnel in Stakeholder Organisations (Government, CI Industry and Responder Communities) who must be Security Cleared (SC) and have appropriate storage facilities.
Planning assumptions for critical infrastructure	Before emergency for CIR work, including civil emergency planning	SCG (RRP and LRP from 01.11.2013) members must satisfy the Baseline Personnel Security Standard (BPSS).
Information on critical infrastructure networks and systems	Before emergency, for assessment of interdependencies	Stakeholders must satisfy the Baseline Personnel Security Standard (BPSS).
Relevant information on critical infrastructure	During an emergency, for prioritisation and response	SCG (RRP and LRP from 01.11.2013) must satisfy the Baseline Personnel Security Standard (BPSS).

[16] HMG Personnel Security Controls: www.cabinetoffice.gov.uk/resource-library/hmg-personnel-security-controls

Annex C

Cabinet Office Guidance "Keeping the Country Running" – Critical Infrastructure Owner/Operator – Categories of Information for lead category 1 Responders

The provision of information (for emergency planning purposes only) to a lead Category 1 responder should include:

- Name of infrastructure asset / network / system
- Critical installations or sites in the network
- Location of critical installations / sites, and their function
- Network / site owners
- 24 / 7 Emergency contact name and numbers for emergencies
- Specific safety / hazards information for the network and sites (e.g. COMAH) and access / egress restrictions that the emergency services need to know
- Outline of the consequences of loss or disruption of the critical infrastructure in terms of loss of service to x number of people in the RRP/LRP area, and which other RRP/LRP areas could also be affected
- A general assessment of the service's vulnerability to natural hazards and accidents, and any mitigation measures taken to reduce the risks
- What action the network / site owner would take in case of an emergency
- Support the infrastructure owner anticipates receiving or may need from emergency services and other emergency responders during an incident.

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Guide 2
Identifying Significant Local Infrastructure

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 2

Identifying Significant Local Infrastructure

Overview

What	This guide seeks to: • Set out practical approaches that can be used to identify significant Local Infrastructure
Who	This guide is aimed at: • Government – CI Resilience Policy leads in Scottish Government • Critical Infrastructure (CI) Operators – Strategic Management, Resilience and Business Continuity Management (BCM) leads • Responder Communities – Regional Resilience Partnerships (RRPs), Local Resilience Partnerships (LRPs), Government department policy leads • Industry Groups
Why	The benefits of identifying significant local infrastructure include: • Achieving long term resilience of significant infrastructure • Ensuring understanding of Physical, Logical and People assets at a local level • Prioritisation of investment for asset protection • Providing context for the Resilience Preparedness Assessment process
How	• Compile a list of local infrastructure • Identify what is significant • Share with resilience partners through the RP CI groups • Map significant local infrastructure to assist in the identification of dependencies and interdependencies

KEEPING SCOTLAND RUNNING

Case Study

Significant Local Infrastructure Pilot Project

The North of Scotland Regional Resilience Partnership Critical Infrastructure Group carried out a pilot piece of work to identify significant local infrastructure in three Local Authority areas in the North capturing a variety of geographic types. These were:

- Angus Council – rural
- Aberdeen City Council – urban
- Orkney Islands Council – island

The aim was to establish a simple process for developing a database of Significant Local Infrastructure with relevant supporting data. This data included site addresses of sites, names of owners, GIS location data and 24/7 contact numbers.

Significant Local Infrastructure is defined as infrastructure which is regarded as important in a local geographic area and supports the delivery of essential services at a local level.

Each of the three pilot areas were approached via their Council emergency planning leads to provide a list of infrastructure sites. One to one discussions were held with each lead and a template provided to give some guidance as to the sectors to be considered. These were;

- Energy – including electricity, gas and fuel
- Civil Nuclear
- Communications - including telecoms, internet, broadcasting and postal services
- Transport - including aviation, ports and ferries, rail and roads and bridges
- Finance
- Government – including SG, local government, others
- Emergency Services – including Police, Fire, Ambulance and Coastguard
- Food
- Water
- Health
- Chemicals
- Defence
- Space

This required some consultation with other relevant areas within Council's including planning and roads etc. This initial piece of work captured not only significant local infrastructure but also some national and critical national infrastructure (CNI).

The methodology is described further in the following sections.

KEEPING SCOTLAND RUNNING

Background

This Guide has been developed to support infrastructure owners and operators, emergency responders, industry groups and government departments to work together to improve the resilience and security of critical infrastructure and essential services in Scotland.

This is best achieved through a **Team Scotland** approach that seeks to **Keep Scotland Running** and **Keep Scotland Informed** before, during and after infrastructure related emergencies.

Each of Scotland's three Resilience Partnerships have established Critical Infrastructure sub groups to support their understanding of infrastructure in their area and deliver an agreed work plan. These groups also provide context for their Risk Preparedness Assessments[17] and ultimately supports the production of Community Risk Registers.

All of this work forms part of Scotland's Strategic Framework, for dealing with Critical Infrastructure in Scotland. The other parts being delivered by:

- Scottish Governments Resilient Essential Services Team and their engagement with Infrastructure Sector Resilience Groups and individual infrastructure owners and operators.
- Police Scotland's Protect Profile work which identifies a broad range of infrastructure assets in each of their territorial Divisions.

This tripartite approach collates a rich picture of infrastructure and supports further work to identify dependencies and interdependencies (see Guide 3 for further information) through a GIS mapping product maintained by Police Scotland.

[17] See Preparing Scotland Guidance

A key part of this work will be collated by the 3 Resilience Partnerships CI groups to identify Significant Local Infrastructure. The term Significant Local Infrastructure refers to local sites known by responders and deemed to have local importance in the delivery of essential services. These include, bridges, tunnels, hospitals, police stations, fire stations, prisons, electricity sub stations etc. (see Annex B for more examples). It is used in this context to reduce sensitivities attached to the term critical. Significant Local Infrastructure work will provide a much more comprehensive list of infrastructure (a rich picture), some of which may be regarded as critical.

The identification of Critical National Infrastructure is well established and clearly described in the 2016 CPNI Guidance.[18]

Methodology

This sections describes the process used in the pilot to identify Significant Local Infrastructure. It is simplistic to encourage understanding and engagement with the process but nevertheless provides useful information in support of the overall strategy.

- Compile a list of local Infrastructure considered significant in each Local Authority area. Completion of the template at Annex A will assist to limit the scope of what is considered to be significant

- Identification of what is significant within the LA area will require local knowledge and expertise of various areas of the LA's key departments including planning, roads, business continuity and emergency planning

- Completing the list will in some cases include sites which may have a national criticality classification however this will be confirmed at a later stage in the process and should not prevent them being included at this point

- This list will be shared with the relevant Sector Resilience Groups within the Critical Infrastructure Resilience Partnerships governance structures for comparison and feedback

Ultimately this list will be combined with Police Scotland Protect Profiles and Scottish Government Critical Infrastructure lists to create the rich picture of sites across Scotland.

Future Work

Once significant local infrastructure is identified the Resilience Partnerships' Critical Infrastructure groups will support further work assessing

- Criticality
- Vulnerabilities
- Mitigation
- Identifying gaps in capability

[18] CPNI – CNI Protection in the UK – the role and functions of CPNI – September 2016

KEEPING SCOTLAND RUNNING

This work is already underway in respect to Telecoms Outages, Black Start planning and Fuel Disruption. The following bullets describe further work which will be required:

- Based on current Resilience Partnership knowledge and expertise, assess and complete the risk assessments associated with the loss of essential services and consider vulnerabilities and impact of the loss on the Resilience Partnership area

- Consider the Contingency Plans that are in place to mitigate the risks associated with the loss of essential services

- Include national plans, sector specific plans (e.g. COMAH, REPPIR), organisational plans and local plans and arrangements to mitigate the risk

- Assess the capability and capacity of the Resilience Partnership to respond to the worst case scenario caused by the loss of essential services

- Identify gaps in preparedness and response arrangements

- Gaps identified in relation to individual Operator and Sector responsibility, can be highlighted through the Critical Infrastructure Resilience Partnership arrangements or direct with the policy areas

- This assessment will feed directly into the Resilience Partnerships Measuring Preparedness Statements

Summary

As has been highlighted, this element of the Strategic Framework was designed to be simple and not require specialist knowledge or skills other than knowledge and appreciation of the significant infrastructure sites in individual Local Authority areas. It is envisaged that each Local Authority area should be able to collate the information required following one meeting of key personnel followed up by collation of the information required for each site as per the template in Annex A. The Resilience Partnership Critical Infrastructure groups will determine the pace at which the data is gathered but it has been proposed that small numbers of Local Authorities in each of the Resilience Partnership areas will work on collating their lists between meetings of the RP CI groups.

Police Scotland have a GIS secure mapping project underway which will be used to map the lists of infrastructure. Ultimately these lists will assist in further work to identify dependencies and interdependencies and in due course will support the identification of weaknesses and vulnerabilities in our portfolio of infrastructure.

Delivery

- CPNI – CNI Protection in the UK – the role and functions of CPNI
- CPNI – CNI Protection in the UK - Annexes
- RPA Process

Annex A

Significant Local Infrastructure Template

Local Authority Area –

Please complete the attached template with as much detail as required. If you have any questions, please contact the Resilient Essential Services Team mailto:ciru@gov.scot

Please add as many new lines under each sector as you need. You will have some sectors with no assets.

Sector	**Site name and address including post code**	**Owner and HQ address**	**Contact Details – if possible 24/7**	**GIS Coordinates**	**Rationale for significance.**
Energy includes • Gas • Electricity • Fuel					
Civil Nuclear					
Chemicals					
Communications includes • Telecoms • Internet • Broadcast • Postal					
Transport includes • Aviation • Maritime – Ports and Ferries					

KEEPING SCOTLAND RUNNING

Annex A

• Rail • Roads and Bridges					
Defence					
Government includes - • UK Gov • Scottish Government • Local Authorities • Others, Courts, Prisons, SEPA, HSE, etc					
Emergency Services includes • Police • Fire • Ambulance • Coastguard					
Health					
Water					
Food					
Finance					
Space					

KEEPING SCOTLAND RUNNING

Examples of Generic Critical Local Infrastructure List

Energy
- Hydro Generating Stations - Electricity
- Significant Power Stations - Electricity
- Gas Compression/Pumping Stations - National Grid Gas
- Significant Gas Distribution assets - Scotland Gas Networks (SGN)
- Oil Pumping Stations/Refinery/Distribution Centres - Oil/Fuel
- Significant Pipelines - Oil/Gas
- Nuclear Power Stations/assets - Nuclear
- Utilities Control Centres

Transport
- Significant road bridges/tunnels
- Arterial road routes/nodes
- Significant rail bridges/tunnels
- Hub railway stations
- Major bus stations
- Main/significant harbours/sea ports
- Airports
- Air Traffic Control Centres

Finance
- Significant Financial Institutions
- Significant cash handling areas

Communications
- BT Exchanges [particularly those supplying CNI sites]
- BT/Cable and Wireless – 999 Call Handling Centres
- Radio/Television Transmitters/masts
- Significant postal collection/distribution centre

Water
- Significant Reservoirs/dams
- Water treatment works
- Waste treatment/pumping sites

Food
- Significant Food Production assets
- Significant Food Processing assets
- Significant Food Distribution assets
- Significant Food Retail assets

Health
- Main Hospitals
- Specialist Health resources

- Other significant Health responsibilities

Emergency Services
- Police [e.g. HQ, Control Rooms, Major Incident Operations Centres, SCC]
- Fire [as above]
- Ambulance [as above]
- Maritime Coastguard [as above]

Government
- UK Government assets
- Scottish Government assets
- Local Government assets [e.g. Council Headquarters, Emergency Centre]
- Prisons

Crowded Places
- Main Shopping Centres
- Significant Football Grounds/Stadia
- Major events/festivals

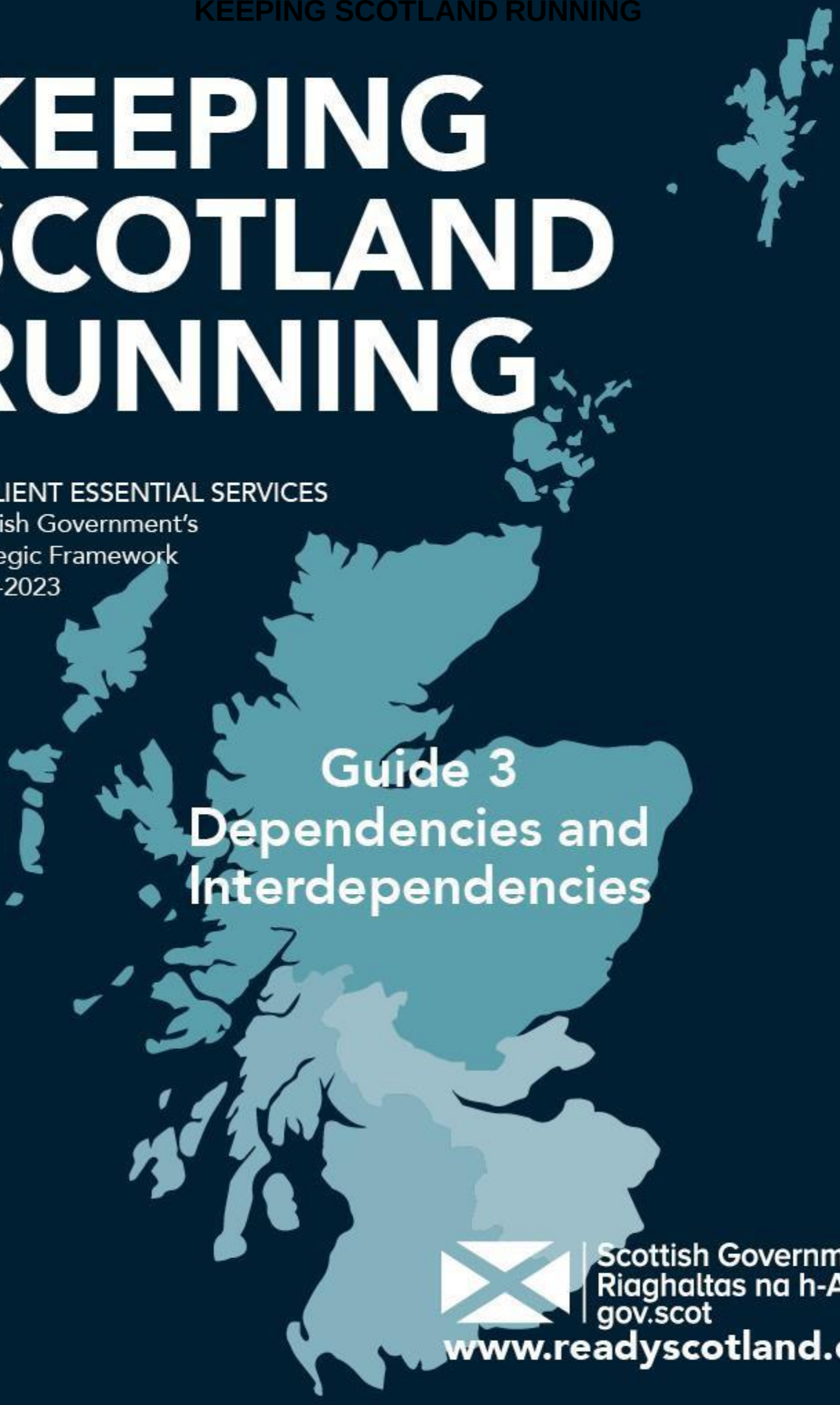
Military
- Significant Military Bases
- MACR sites

Other
- COMAH Sites
- Universities - particularly those with CBR assets
- Significant visitor attractions [e.g. significant hotels, golf courses, sporting attractions, Concert venues]
- Major Sector IT Data Centres

KEEPING SCOTLAND RUNNING

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023



Guide 3
Dependencies and Interdependencies

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 3

Dependencies and Interdependencies

Overview

What	The guide seeks to: • Outline practical approaches that can be used to assess dependencies and interdependencies at site specific, regional and sector level.
Who	This guide is aimed at: • Government - CI Resilience Policy leads in Scottish Government • Critical Infrastructure (CI) Operators - Strategic Management, Resilience and Business Continuity Management (BCM) leads • Responder Communities – Resilience Partnerships (RPs), Resilience and BCM leads
Why	The benefits of identifying dependencies and interdependencies include: • A better understanding of vulnerabilities, impacts on other infrastructure and consequences when things do go wrong • Enabling effective and proportionate mitigation action to be taken • Enabling a more effective multi-agency response to disruptive events
How	Examining Dependencies and Interdependencies should: • Be a fundamental aspect of good business continuity management • Inform specific local planning assumptions for RPs • Inform contingency planning and mitigation measures for CI owners and operators Available tools include: Resilience Direct Information Sharing Protocols (ISPs) – Guide 1 Annex A Data Sharing Agreements (DSAs) – Guide 1 Annex B

Case Study

Identifying Dependency/Interdependency Relationships

Asset

The Police in the west of Scotland conducted research into the identification of dependency/interdependency relationships at a key emergency services sector asset.

The process adopted the following stages:

- Examination of the asset to identify key dependency relationships within the sector and with other critical infrastructure sectors
- Identification of critical processes within the asset, and the services and providers which facilitated these processes
- Establishing the impact of disruption through loss of the dependencies
- Liaison with the service providers to ensure that delivery processes for the services were robust and resilient
- Develop information sharing protocols and non-disclosure agreements for the protection of commercially sensitive information and to facilitate partnership working and information sharing. (See Guide 1 – Collaborative Working for further detail)
- Use GIS mapping to plot supply routes for the critical services into the asset.
- Use the mapping to identify any critical points where service routes overlapped and presented an additional vulnerability or single points of failure for critical processes within the asset
- Conduct a table-top exercise involving a number of potential disruptive scenarios, in order to test the asset's resilience

The Asset owner was then able to use the findings of this work and resulting recommendations as the basis for improving the resilience of the site.

Sector

The Health Sector Resilience Group undertook work to "Assess and catalogue the strategic geographical and physical dependencies of critical infrastructure", in order to get a comprehensive understanding of the health sector dependencies and connections with the other critical infrastructure sectors.

Key staff within each NHS board in Scotland were tasked with completing a dependencies matrix to catalogue the strategic dependencies of the critical infrastructure relative to their board area (including critical services/systems common to more than one board). The dependencies matrix is reproduced at Annex A.

The outcome of this work was then taken to a sector workshop where the risks, vulnerabilities, mitigation measures and capability gaps of the dependencies were assessed. This work enabled the Health Sector Critical Infrastructure Resilience Group to identify a programme of measures to raise the resilience of the sector.

Community

The North's Resilience Partnership Critical Infrastructure Sub Group undertook to develop a methodology to understand significant infrastructure at a local level.

Using 3 diverse local authority areas as a pilot, work was carried out with Angus Council, (Rural) Aberdeen City Council (City) and Orkney Council (Island).

The group worked with the government to understand the types of assets/sites which could be considered significant at a local level.

Each organisation developed lists of infrastructure which they considered important at the local level. These lists were then combined along with information from Police and government to form a master list outlining a rich picture of infrastructure in these areas.

The group then worked with the local electricity distribution network operator and BT to map a selection of sector sites against their network infrastructure. This highlighted the main electricity substations and telephone exchange supporting these infrastructure clusters.

This work will enable the North's Resilience Partnership Critical Infrastructure Sub Group to ensure that significant local infrastructure (SLI) are fully considered in wider resilience programmes within the region.

Background

Scotland's critical infrastructure is a complex interconnected number of assets, systems and networks, providing essential services to the People of Scotland. This Guide has therefore been developed to support infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services.

We believe that this can be best achieved through a **Team Scotland** approach that seeks to **Keep Scotland Running** and **Keep Scotland Informed** before, during and after CIR related emergencies.

To achieve successful long term enhancement of CIR, it is crucial that dependencies and interdependencies are known and understood.

KEEPING SCOTLAND RUNNING

Events such as the Buncefield explosion in December 2005 or the January 2012 storms which affected Argyll and Bute vividly demonstrate how a single event can have far-reaching implications as a result of knock-on consequences passed through the **dependencies** chain of critical infrastructure, sometimes over a wide geographical area. Recent cyber-attacks have also highlighted the importance of understanding supply chains and ensuring that the vendors used by our critical infrastructure are also secure and resilient. These relationships between infrastructure networks need to be understood to establish reasonable local planning assumptions for civil emergency planning.

Physical dependencies are not always obvious and as such can represent a significant and hidden risk to networks and systems. Without a sufficient understanding of physical dependencies, the loss of a key element of the infrastructure network (such as a major installation) could lead to cascade failures where further disruption is caused beyond the point of failure.

Guidance

General – All Stakeholders

Dependencies can be categorised in numerous different ways, including physical (direct links – e.g. power supply line into asset) and geographical(due to location – e.g. local access road infrastructure) and may be *'Upstream'* or *'Downstream'*.

Geographical dependencies often highlight clusters of infrastructure and local single points of failure which more than one CI site may depend e.g. two adjacent chemical processing plants which both depend on a local electricity substation, telephone exchange or access road.

Upstream Dependencies: Where infrastructure assets are dependent upon other services to continue functioning, e.g. water treatment works may have an upstream dependence on the power network.

Downstream Dependencies: Where infrastructure assets are reliant on supplying services to other infrastructure in order to be able to continue to function (e.g. a refinery may have a downstream dependence on the airports and export jetties to offload aviation fuel produced, windfarm has a downstream dependence on consumer electricity demand, etc).

Interdependencies: Where dependencies between two assets exist in both directions (e.g. telecoms infrastructure dependent on the power network which is in turn dependent on the telecoms network to monitor and control the system.)

Examples of the various types of dependencies and interdependencies are included in the Guide 3 Annexes below.

- Annex B – wide spread dependencies from the 2012 Argyll and Bute Storms
- Annex C – physical dependencies
- Annex D – complex interdependencies

KEEPING SCOTLAND RUNNING

Three distinct approaches have been applied in Scotland: They are Sector, Asset and Community.

These approaches also include analysis of risk and mitigation – see Guide 2. The approaches are outlined in more detail in the guidance for Government, Industry and Responder Community sections below.

Government (Lead Government Departments)

The **Sector** based approach is generally best led by the Lead Government Departments (LGD) to identify the dependencies of the sector's critical infrastructure assets both within the sector and with other critical infrastructure sectors. The sector approach usually follows the process below:-

- Focus on one sector
- Identify direct dependencies and interdependencies of key assets/networks/systems with other sectors
- Extrapolate vulnerabilities and identify capability gaps
- Test sector resilience to disruptive events through exercising and identify risks, vulnerabilities, capability gaps and mitigation measures to improve resilience

Industry (Critical Infrastructure Operators/Owners)

The **Asset** based approach is generally led by the asset operator and includes identifying geographic and physical dependencies with other assets from within the same sector as well as assets from the other critical infrastructure sectors.

The assessment of dependencies is a fundamental aspect of good business continuity management. It is therefore good business practice for owners/operators of critical infrastructure to, as a minimum, identify their immediate dependencies.
It is often complex and prohibitively time consuming to map in depth dependencies associated with advanced supply networks where contingency measures can reroute supplies to minimise impacts of disruption. Complex network infrastructure such as power, communications and water networks are often able to be reconfigured to maintain supplies in the event of disruption to individual sites or infrastructure.

Understanding dependencies and interdependencies should enable operators to inform their strategic planning and capital investment decisions to improve the long-term resilience to threats and hazards.

The asset approach usually follows the process below:-

- Focus on one asset
- Identify dependencies and the services and providers required
- Establish the impact of disruption through loss of dependencies

- Develop information sharing protocols and non-disclosure agreements for protection of commercially sensitive information and to facilitate partnership working
- Work with service providers to ensure delivery processes are robust and resilient
- Map supply routes for critical services
- Use mapping to identify critical points where service routes overlap (single points of failure)
- Test asset resilience to disruptive events through exercising and identify risks, vulnerabilities, capability gaps and mitigation measures to improve resilience

Responder Communities (Resilience Partnerships (RPs) and Regional CI Groups)

The **Community** based approach is generally led by Responder Communities and involves looking at the major communities (centres of population) in a geographical area and determining the networks and critical infrastructure which provides essential services to those communities.

A key element of the Community based approach is that local emergency responders and infrastructure owners must work together to ensure a sufficient understanding of infrastructure networks and dependencies across sectors.

Information is available to the responder community[19] to identify infrastructure assets that are located in the same geographical area, which could potentially be affected by a single incident. For example – the area surrounding an industrial plant can be analysed for other critical infrastructure that could be affected by an explosion from the site, or a geographical area can be analysed for infrastructure that could be affected by a flood. The knowledge of critical infrastructure and potential risks to disruption of services should be used to develop specific local planning assumptions for the resilience partnerships.

The community approach usually follows the process below:

- Responder community group focuses on a specific community (Town/city/district/region/zone)
- Members individually identify potential significant local infrastructure (own organisations infrastructure as well as using local knowledge)
- Wider significant infrastructure identified with emergency services and government
- Significant local infrastructure lists combined into a master list for the community
- Work with key service providers and utilities to identify further infrastructure which supports the SLI and may also need to be considered
- Establish the consequences to the community of failure of the significant local infrastructure

[19] See Keeping Scotland Running – Guide 2 – Significant Local Infrastructure

- Test community resilience to disruptive events through exercising and identify risks, vulnerabilities, capability gaps and mitigation measures to improve resilience

Delivery

Critical Infrastructure resilience in Scotland is primarily delivered at three levels – organisational, resilience partnership and the Scotland wide Critical Infrastructure Resilience partnership, all working together to complement the wider UK guidance and work streams.

The **Critical Infrastructure Resilience Partnership** provides the overarching strategic direction for the advancement of Critical Infrastructure Resilience in Scotland. By working with the Lead Government Departments for reserved sectors at UK level and the Scottish Government for devolved sectors, the sector approach can be applied to enhance the understanding of the resilience of the critical infrastructure sectors as a whole.

The **Resilience Partnership Critical Infrastructure Resilience Groups** bring together the key CI owner/operators and resilience community to consider resilience at a regional and local level. These groups are ideally placed to use the Community approach to determine and map the networks and critical infrastructure which provides the essential services across the resilience partnership area. The groups may then advance the process and produce a dependency map for the area to be used as an information and challenge document during risk assessment, pre-event planning and exercising to ensure visibility of key dependencies during an emergency.

The **CI owners/operators** will have robust contingency planning processes in place, in some sectors this will be mandated through regulation and legislation, in others the driver will be reputational as a business prepared to cope with disruption is more likely to survive in the longer term. Examination of dependencies and interdependencies using an Asset based approach allows the business to identify capability gaps and potentially mitigate against disruption to operations.

KEEPING SCOTLAND RUNNING

Annex A

Matrix for Health Sector Dependencies with Water, Food, Communications and Finance Sectors
(Replicate matrix for dependencies with other Critical Infrastructure sectors)

Asset No.	**NHS BOARD**	**ASSETS**	**DEPENDENCIES**		**SECTORS** • **Insert details of geographical and/or physical dependencies** • **If there is no dependency with a specific sector then please enter 'NIL' in the box.**			
			Geographical Yes / No	Physical Yes / No	Water	Food	Communications	Finance
EXAMPLE **No 1: NHS Brae: Alton Hospital**			*Yes*	*Yes*	*Physical – Single source of water supply to asset from 'Alton Water Treatment Works'.*		*Geographical – NHS IT systems hosted by 'Alton IT systems Ltd' in building adjacent to asset.*	

Annex B

Example Of Cascading Dependencies Across A Wide Geographical Area

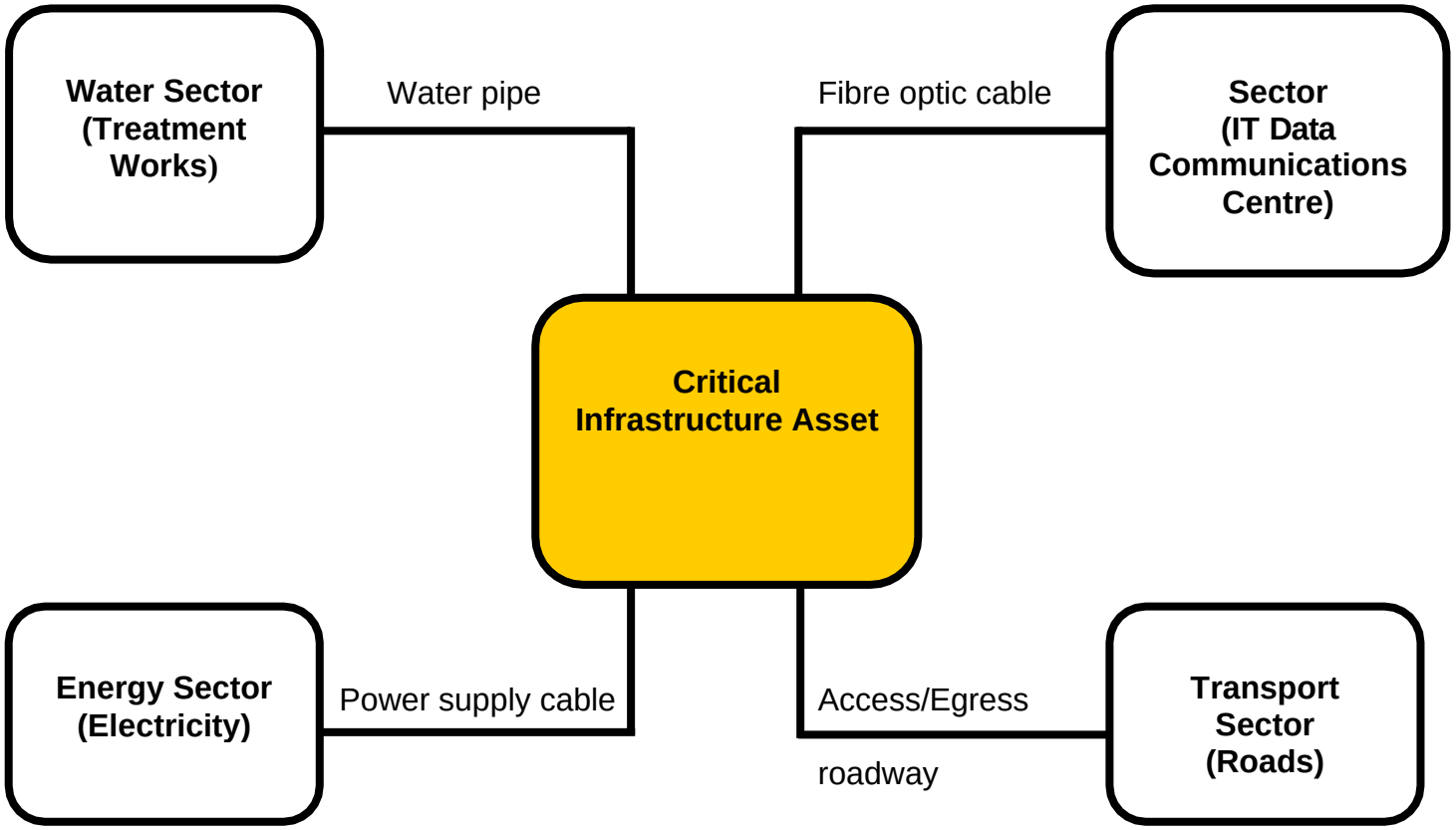
During January 2012, a severe storm affected large parts of Scotland. Storm force winds across the West of Scotland caused widespread loss of electrical power to approximately 190,000 premises.

In Argyll and Bute the power outage resulted in a cascade of consequences for critical infrastructure due to the significant dependencies and interdependencies. There included:-

- The loss of all mobile phones within approximately an hour as mast sites were dependent on power supplies, batteries or generators (which were dependent on fuel supplies)
- Loss of landline telephones and exchanges which were dependent on power when back-up generation failed or ran out of fuel
- Loss of water when water treatment works which were dependent on power and back-up generation failed or ran out of fuel
- Roads blocked by fallen trees, which delayed repair efforts for telecoms and power engineers who depended on them to access damaged infrastructure
- Severe difficulty in contacting local communities as responders were dependent on telephone lines, exchanges and mobile masts which were no longer functioning due to storm damage and/or power loss. This heightened concerns for vulnerable people
- Loss of electronic finance systems, including cash dispensers and electronic card readers due to their dependence on power and telecoms
- Filling stations unable to dispense fuel due to their dependence on power to pump fuels

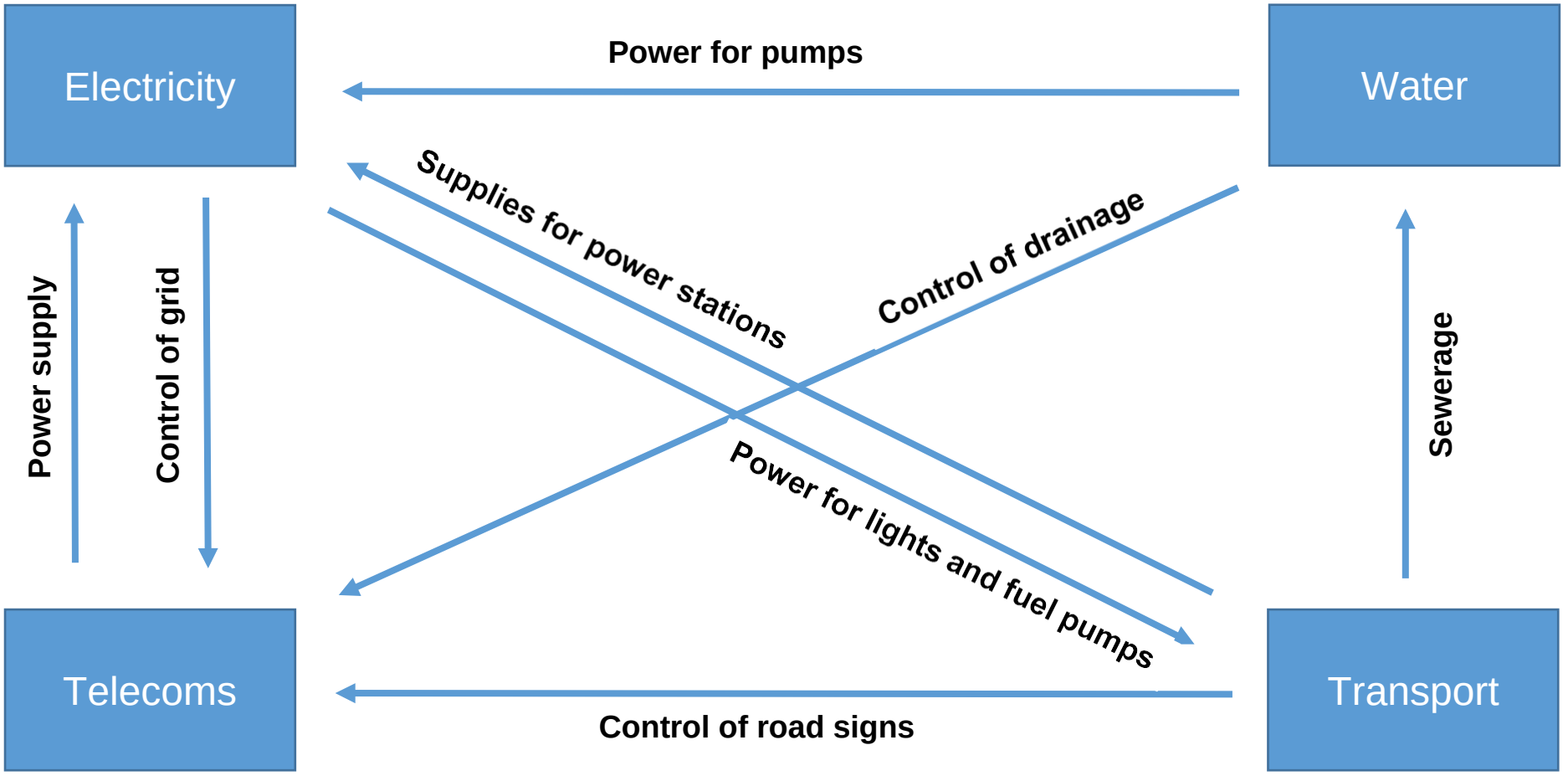
Annex C

Example of Physical Dependencies



Annex D

Example of Complex Interdependencies



KEEPING SCOTLAND RUNNING

Annex D

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Guide 4
Cyber Resilience and Critical Infrastructure

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 4

Cyber Resilience and Critical Infrastructure

Overview

What	This guide seeks to: • Establish a common cross-sector approach to Cyber Resilience and Critical Infrastructure. The guide includes information on the key risks for Scotland and the impact that these may have on infrastructure, and provides information on the resources and support available to organisations.
Who	This guide applies to: • **Government** - CI Resilience Policy leads in Scottish Government • **Critical Infrastructure (CI) Operators** at a tactical and strategic level • **Responder Communities** – Resilience Partnerships (RPs)
Why	Cyber represents a principle and growing disruptive threat to Critical Infrastructure and other essential services. It is necessary that the operators of Scotland's national and local infrastructure understand and protect their critical assets, understand the cyber threat to their organisation, the risk to their infrastructure, manage the risk from their supply chain and recognise staff as a potential access route. In addition, they should have adequately planned and prepared for the disruptions a cyber-attack on their organisation could have and should test these plans so that if the threat cannot be prevented, then the organisation responds and recovers as effectively as possible. A risk based approach to such planning, preparation, response and recovery will help organisations understand their vulnerabilities to cyber and take appropriate measures. Key to taking a risk-based approach is in actually understanding the nature of the cyber threat to the organisation.
How	Building organisational resilience to cyber threats an organisations cyber resilience measures should: • Be based on current good practice guidelines, standards and principals • Be based on a sound understanding of the cyber threat • Be owned as a board level risk • Be integrated into existing risk management and planning processes and decisions

	• Be informed by understanding the nature and likelihood of the threat and a cycle of review and action, monitoring the effectiveness of decisions and ensuring continuous improvement • Understand and take steps to manage the risk to the infrastructure, supply chain and staff • Take account of any expert advice from recognised organisations both in planning for and dealing with the impacts resulting from the cyber threat • Be developed in partnership with stakeholders/interested parties • Be integrated at an appropriate scale – some infrastructure may require national scale planning and collaboration; others may be specific to a particular area or site • Contribute to enabling other organisations to mitigate the cyber threat by sharing appropriately sanitised threat intelligence within the Cyber Security Information Sharing Partnership (CiSP) and other trusted networks

KEEPING SCOTLAND RUNNING

Case Study

2017 Wannacry Ransomware Attack

In May 2017 a global cyber-attack using hacking tools to deploy the Wannacry Ransomware spread at unprecedented speed across 150 countries and within the UK impacted significantly on the NHS within the UK.

WannaCry exploited a Microsoft vulnerability which was known and a patch to fix it was released in March.

Hospitals and GP surgeries in England and Scotland were among at least 16 health service organisations hit. Staff were forced to revert to pen and paper and use their own mobiles after the attack affected key systems, including telephones. Hospitals and doctors' surgeries in parts of England were forced to turn away patients and cancel appointments after they were infected with the ransomware, which scrambled data on computers and demanded payments of $300 to $600 to restore access. People in affected areas were being advised to seek medical care only in emergencies.

The incident was declared to be a national cyber incident and the National Cyber Security Centre undertook a central co-ordination role. At a Ministerial level both the Cabinet Office Briefing Room and the and Scottish Government Resilience Room were stepped up to manage the escalating incident. The incident received significant media attention and was a wake-up-call questioning the resilience of critical infrastructure such as the NHS ability to respond appropriately. The National Cyber Crime Unit of the National Crime Agency and Police Scotland Cyber Teams played a vital role in supporting the NCSC.

In Scotland the CEO's of all public sector organisations were contacted over the weekend to alert them to the risk and ensure that assurance could be given to Ministers that steps had been taken to mitigate against the threat.

Key insights:

- The speed at which this virus spread through the NHS nationally highlights the interconnectedness of organisations
- Incident Response plans need to recognise this interconnectedness and reach beyond the individual organisation
- Service delivery was impacted
- Effective media handling is essential
- National Co-ordination of significant emergencies (SGOR and COBR) were tested in the first managed major cyber incident
- There needs to be a clearer understanding of engagement with and roles of Central co-ordination organisations particularly the NCSC, Police Scotland and the Scottish Government
- The value of membership of the NCSC Cybersecurity Information Sharing Partnership (Cip) to gain essential threat intelligence was tested and proven

- The attack identified the need for organisations to take proper cognisance of having the basic cyber hygiene in place to combat the most common internet borne threats
- Cyber as a risk was elevated to Board/ Executive level as a result of Wannacry incident
- As a result of the incident the Scottish Government accelerated plans to introduce a Public Sector Action Plan on Cyber Resilience[20] to provide assurances that this sector was resilient to the growing cyber threat

Background

Cyber has been identified as one of the top risks to UK security. A serious attack on a critical infrastructure or essential service organisation may result in the disruption or denial of service output, with the compromise and harm to a critical network asset causing significant financial and reputational damage. This is exacerbated if organisations are not prepared to respond and recover from cyber-attacks.

Critical Infrastructure sectors are at constant risk from state actors, cyber criminals, hacktivists and staff (deliberate or accidental), while terrorist groups aspire to acquire cyber capability.

The Scottish Government's policy in respect of Critical Infrastructure stakeholders is as follows:

Primary Driver:

Enhancing cyber resilience arrangements to mitigate and respond to cyber threats

Outcomes:

- Active management of cyber threats and vulnerabilities is embedded in corporate risk management processes and policies, with oversight at Board level
- Effective processes exist to:
  - Identify and assign ownership of critical assets that may be vulnerable to cyber threats
  - Assess and understand cyber threats and vulnerabilities in respect of corporate assets, and refresh this understanding on a continuous basis
  - Manage and respond to cyber threats and vulnerabilities on a continuous basis
- Staff at all levels are supported and incentivised to adopt appropriate behaviours to mitigate cyber risks/threats, including through staff education/training
- Appropriate technical controls and policies are in place (including in respect of secure configuration, network security, user privileges, malware protection and

[20] https://beta.gov.scot/policies/cyber-resilience/

monitoring), with specialist advice and support made available where required via internal or external sources

- Robust Incident Response, Business Continuity Management (BCM) and contingency arrangements in place to manage and minimise disruption from a cyber-attack, including a test/exercise programme
- Enhancing cyber security arrangements to mitigate cyber threat

Scottish Cyber Resilience Strategy

Safe, secure and prosperous: a cyber-resilience strategy for Scotland[21], was published in 2015. It set out the Scottish Government's vision for Cyber Resilience in Scotland and sets out the aspirations and outcomes required for Scotland to become a world leader in cyber resilience.

"Safe, secure and prosperous" is closely aligned with the UK National Cyber Security Strategy[22], which sets out the UK Government's strategic approach to making the UK secure and resilient in cyberspace. Cyber security is a reserved matter, but it has strong implications for the delivery and resilience of devolved services – as such, the Scottish Government works closely with key partners such as the UK National Cyber Security Centre to ensure alignment between work on cyber resilience at the UK and Scottish levels.

The National Cyber Resilience Leaders Board (NCRLB) is an advisory board to Scottish Ministers and comprises of leaders from the Public, Private and Third Sector and Academia and was formed to help drive forward the Scottish Government's Cyber Resilience Strategy.

Following the Wannacry attack in May 2017, which had a high profile impact on the NHS in England and Scotland, the Programme for Government committed the SG to working with the NCRLB to develop and implement a suite of 5 action plans, which will drive Scotland towards our strategic ambitions.

As of 2018, the action plans[23] have been published. The action plans are as follows:

- The **Learning and Skills action plan**, which sets out the actions we and our partners will take from 2018 to 2020 to support the development of cyber resilient behaviours amongst our population (helping them to avoid become victims of cybercrime), and to build a skilled and growing cyber security profession for Scotland. (Published March 2018)

- The **Public Sector Action Plan**, which aims to ensure that Scotland's public bodies have in place a common baseline of good cyber resilience practice, and are working towards becoming exemplars of cyber resilience. This is vital to ensuring our digital public services are safe and secure and protected from

[21] http://www.gov.scot/Publications/2015/11/2023
[22] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[23] https://beta.gov.scot/policies/cyber-resilience/

cybercrime. If successful, Scotland will be the first nation in the UK to have achieved this common baseline across its public sector. (Published November 2017)

- The **Private and Third Sector Action Plans**, which set out a detailed programme of work in partnership with Scotland's private and third sectors to help raise fundamental levels of cyber resilience. They have a particular focus on supporting our small and medium sized businesses and charities to understand the cyber threat and how to address it. (Published June 2018)

- The **Economic Opportunity Action Plan**, which will set out actions to help create the conditions for a world class cyber security goods and services cluster to flourish in Scotland.

Guidance

Good cyber security and resilience practices are wide ranging, from policy level to implementation, and have to be applied at every level of the business, from boardroom to control systems. Important guidance is available from the National Cyber Security Centre website (https://www.ncsc.gov.uk/guidance) where additional information on Threat Intelligence, Incident Management, Insight, Skills and Certified Security Services are listed.

It is also important to remember that cyber resilience is not something that can be considered in isolation. It goes hand in hand with physical and personnel security (e.g. building management systems and insider threat) to create a holistic approach to protective security. In a digital age good cyber resilience should be regarded as an essential digital enabler. The cyber threat is a business risk and requires managed at board level.

A number of critical infrastructure organisations will be impacted by the EU Directive on Security of Network Information Systems (NIS Directive) which was introduced in May 2018. As a result of this directive the UK Government will be producing clarity on the regulation of those that are directly impacted by the Directive. A set of security principals will be developed and will form a high level standard to which those impacted by the directive will be required to comply. These principals will follow recognise international good practice in security as such form good practice which organisations should strive to achieve taking into regard their size, sector and appetite for managing risk.

The following are common key areas for consideration in achieving good cyber resilience. They are presented to follow the **4 key domains** and 14 sub categories that are likely to make up the NIS Framework.

Identify: ***Appropriate organisational structures, policies, and processes should be in place to understand, assess and systematically manage security risks to organisations***

Governance:

- There are appropriate management policies and processes in place to govern the organisations approach to the security of network and information systems.

Risk Management:

- The organisation takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.

Asset Management:

- All systems and/or services that are required to maintain or support essential services are determined and understood. This includes data, people and systems as well as any supporting infrastructure

Supply Chain Risk Management:

- The organisation understands and manages security risks to the network and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

Protect: ***Proportionate security measures should be in place to protect essential services and systems from cyber-attack, system failures, or unauthorised access. Specific requirements will be set out in respect of:***

Service Protection Policies and Processes:

- The organisation defines and communicates appropriate policies and processes that direct the overall organisational approach to securing systems and data that support delivery of essential services.

Identity & Access Control:

- The organisation understands, documents and controls access to systems and functions supporting the delivery of essential services. Rights or access granted to specific users or functions should be understood and well managed.
- Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

Data Security:

- The organisation prevents unauthorised access to data whether through unauthorised access to user devices, interception of data in transit or accessing data that remaining in memory when technology is sent for repair or disposal.

System Security:

- Critical Systems are protected from cyber-attack. This includes minimising the opportunity for attack by configuring technology well, actively managing software vulnerabilities, minimising services available, and controlling connectivity and physical access.

Resilient Networks & Systems:

- The organisation builds resilience against cyber-attack, implementation, operation and management of systems.

Staff Awareness & Training:

- Staff are given appropriate support to ensure they can support the security of network and information systems of essential services.

Detect: ***Appropriate capabilities should be in place to ensure network and information system security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services/public services. Specific requirements will be set out in respect of:***

Security Monitoring:

- The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the on-going effectiveness of protective security measures.

Anomaly Detection:

- The organisation detects anomalous events in the network and information systems affecting, or with the potential to affect, the delivery of services.

Respond and Recover: ***Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services/public services, including the restoration of those services where necessary.***

Response and Recovery Planning:

- There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure

- Mitigation activities are in place that are designed to contain or limit the impact of compromise

Improvements:

- When an incident occurs, steps must be taken to understand the root cause of that incident and take appropriate remediating action.

Additional clarity on the impact and extent to which the NIS Directive will apply will be forthcoming from the UK Government in 2018. In developing cyber resilience action plans for the public, private and third sectors the Scottish Government will, where possible, be seeking to achieve a commonality of approach with regards to the application of cyber resilience standards.

Delivery

Operators are again referred to the many resources offered by the National Cyber Security Centre (NCSC) as well as being encouraged to join the Cyber Security Information Sharing Partnership (CiSP) where additional real time threat intelligence is offered, including:

NCSC website
https://www.ncsc.gov.uk
There is a significant body of advice and guidance contained within the NCSC website. NCSC is developing the Network Information Systems (NIS) Cyber Assessment Framework (CAF). The NIS CAF is the tool that NCSC will be recommending for assessing cyber security for CNI.

Cyber Security Information Sharing Partnership: https://www.ncsc.gov.uk/cisp
The Cyber Security Information Sharing Partnership (CiSP) is a confidential forum for sharing intelligence about cyber threats and vulnerabilities, in real time. Run by the NCSC, CiSP is a joint industry and government initiative that helps to increase overall situational awareness and reduce impact on UK business. Scotland has established its own non sector based community within the Cisp known as the Scottish Cyber Information Network (SCiNET)

NCSC Cyber Incident Management
https://www.ncsc.gov.uk/section/about-ncsc/incident-management
The National Cyber Security Centre has a role in managing significant cyber incidents and indeed is the competent authority to declare significant Cyber Incidents that have an impact on the UK. The NCSC can provide critical support to organisations and as such operators should make themselves aware of the NCSC Incident reporting process

NCSC Ten Steps to Cyber Security
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
Guidance on how organisations can protect themselves in cyberspace, including:

- An introduction to cyber security for executive/board-level staff.
- A white paper that explains what a common cyber-attack looks like, and how attackers execute them.
- The 10 technical advice sheets an organisation should consider putting in place.

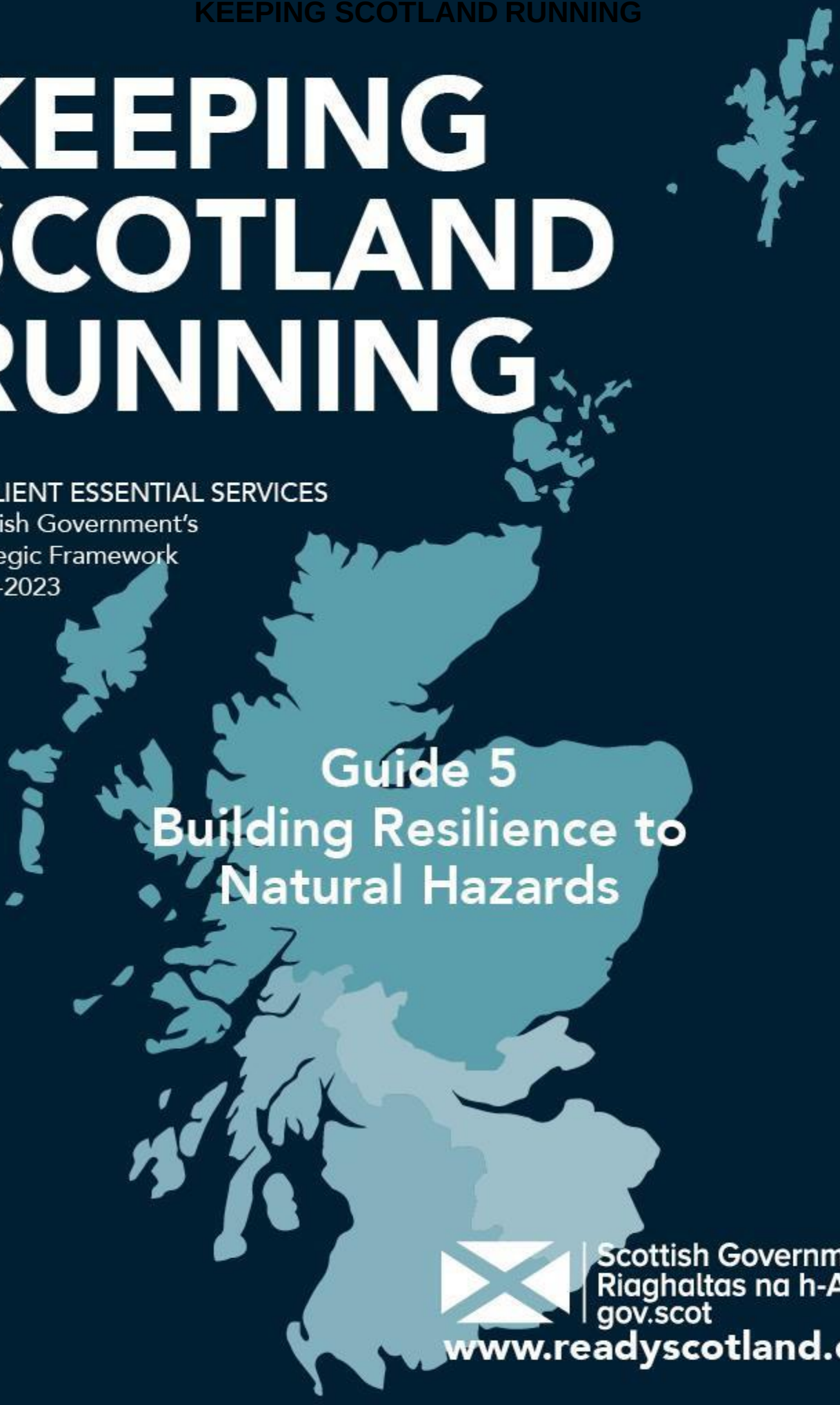
KEEPING SCOTLAND RUNNING

Cyber Essentials
https://www.cyberaware.gov.uk/cyberessentials/
Cyber Essentials is a government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors. The scheme addresses five key controls that, when implemented correctly, can prevent around 80% of cyber-attacks.

Water UK Cyber Security Principles for the Water Industry
https://www.water.org.uk/news-water-uk/latest-news/cyber-security-principles-water-industry
The Water UK Cyber Security Good Practice Group has produced a set of principles and recommendations to help its members address the risks posed to water and waste water services by cyber related threats. In drawing this work together, the industry engaged with stakeholders, government and regulators.

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023



Guide 5
Building Resilience to Natural Hazards

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 5

Building Resilience to Natural Hazards

Overview

What	This guide seeks to: • Establish a common cross-sector approach to building resilience to Natural Hazards. The guide includes information on the key risks for Scotland and the impact that these may have on infrastructure, and provides information on the resources and support available to organisations.
Who	This guide is aimed at: • **Government** - CI Resilience Policy leads in Scottish Government • **Critical Infrastructure (CI) Operators** - Strategic Management, Resilience and Business Continuity Management (BCM) leads • **Responder Communities** – Resilience Partnerships (RPs)
Why	Infrastructure can be damaged or disrupted by a variety of natural hazards e.g. severe weather, flooding etc. and it is necessary that the operators of Scotland's national and local infrastructure have adequately planned and prepared for such disruptions. A risk-based approach to such planning and preparation will help organisations understand their vulnerabilities to natural hazards and take appropriate measures.
How	Building the resilience of infrastructure to natural hazards should: • Be integrated into existing risk management and planning processes and decisions. • Be informed by a cycle of review and action, monitoring the effectiveness of decisions and ensuring continuous improvement. • Take account of any expert advice from recognised organisations both in planning for and dealing with the impacts resulting from the natural hazard. • Be developed in partnership with stakeholders/interested parties. • Be integrated at an appropriate scale – some infrastructure may require national scale planning and collaboration; others may be specific to a particular area or site.

KEEPING SCOTLAND RUNNING

Case Study

Severe Winter Weather

December 2015 through January 2016 saw spells of severe weather which resulted in challenging conditions for communities and emergency responders. December was exceptionally wet with frequent spells of heavy rain across much of Scotland. Many places in the west and north recorded 2 to 3 times the average rainfall, with a few places as much as 4 times. Inevitably there was extensive and major flooding in some parts of Scotland.

Storm “Desmond” brought strong winds on 4th/5th but it was the heavy rain which caused more problems in Scotland during Saturday 5th with flooding on many major road and rail routes in central and southern Scotland. Hundreds of properties were evacuated in Hawick due to concerns over the River Teviot.

The unsettled weather through to Christmas before Storm “Frank” brought more heavy rain and strong winds to many parts of the UK on 29th December. Scotland bore the brunt of the impacts of “Frank”, with hundreds of homes evacuated due to flooding in the Borders towns of Dumfries, Hawick and Peebles. The villages of Newton Stewart and Carsphairn were cut off, with fire crews rescuing people from properties by boat. In South Ayrshire 12 passengers had to be airlifted from a bus stuck in flood water. More than 100 people were evacuated from their homes in Ballater in Aberdeenshire. Elsewhere, thousands of homes experienced power cuts and fallen trees caused problems on the roads.

While there was only one named storm during January – Storm Gertrude on the 29th – the legacy of Storms Desmond and Frank meant there were ongoing sensitivities to rain in many parts, particularly in northeast Scotland, the Borders and Dumfries & Galloway as the unsettled weather continued. Impacts throughout the month included:

Many communities in northeast Scotland continued to be affected by flooding

The evacuation of a sheltered housing complex in Aboyne with flooding also threatening an electricity substation in the town.

numerous road closures reported due to flooding particularly in the north east and in the south (D&G, Borders),

Rail lines blocked due to flood damage, including between Perth and Inverness and between Aberdeen and Dundee

Large scale power outages

A brief cold interlude brought snow and some disruption to Lothian and Borders on the 13th/14th with the A68 closed in Midlothian, the Borders and Northumberland due to three separate snow related incidents. Problems were also reported on the A7 and A1.

When storm “Gertrude” arrived on the 29th the winds associated with it closed the Tay and Forth Road Bridges during the morning, caused localised landslides, fallen trees, some structural damage, overturned HGVs on the M9, A96 and M74

and closed schools. It left around 8,500 properties without power across Scotland. In Shetland, gusts of wind over 100mph resulted in the closure of schools, some power outages, a van was blown off a road and a couple of caravans were overturned.
These severe weather events highlighted the interconnectivity between the critical infrastructure that underpins the essential services upon which daily life in modern Scotland relies. The major consequences faced by critical infrastructure Operators and Responders as a result of severe weather, demonstrates the importance of building resilience to mitigate future impact.

Background

There have been many examples in recent years of natural hazards affecting the infrastructure of Scotland.

The prolonged snow and ice of the winter of 2010/2011 resulted in stranded motorists on blocked roads and issues with salt supplies and domestic fuel deliveries. Snow and ice also caused massive disruption to power supplies and mobile communications across southwest Scotland and Argyll and Bute in March 2013.

Severe gales have caused widespread damage, power outages and transport disruption (e.g. bridge closures) on a number of occasions in recent years, notably December 2012, January 2013 and December 2013.

There have been numerous flooding incidents impacting on transport links and property while, in December 2013, a coastal surge event put the oil refinery at Grangemouth at risk of flooding.

In December 2014, extensive lightning strikes caused major power and telecommunications outages in northwest Scotland.

Two volcanic eruptions in Iceland in April 2010 and May 2011 resulted in massive disruption to aviation services including key lifeline services to the Scottish islands and landslides have caused several periods of disruption to key road links such as the A83.

In recent years there have been great improvements in the partnership working between the various expert agencies and responders.

For example, the Met Office and SEPA, as the expert agencies in weather and flooding respectively, work together in the Scottish Flood Forecasting Service bringing together world class weather forecasting science and expert knowledge of Scotland's rivers and coastline to provide accurate flood forecasts. Through a variety of products and a network of advisors, advice is disseminated up to five days in advance to key responders giving them time to prepare an appropriate response to help protect lives and property in Scotland.

Guidance

This section highlights the natural hazard risks which are included in the UK National Risk Register and provides guidance on information available to infrastructure operators which aims to help militate against these risks. The risks are:

Hazard	Scottish Context
Severe Weather	Storms and Gales
	Low temperatures and heavy snow
Flooding	Inland Flooding
	Coastal Flooding
Drought	Drought
Volcanoes	Explosive volcanic eruptions (Ash)
	Effusive volcanic eruptions (Gases)
Severe Space Weather	Severe space weather
Geological Hazards	Landslides
Severe Wildfires	Severe wildfires

Further information can be found in Cabinet Office documents:

National Risk Register of Civil Emergencies

Keeping the Country Running: Natural Hazards and Infrastructure

Severe Weather

Severe weather can cause significant disruption to infrastructure. Infrastructure operators should plan and prepare for the consequences of severe weather and ensure that they are aware of forecasts of severe weather.

The Met Office is the official source of meteorological information in the UK. Legislation supporting the Civil Contingencies Act 2004 states that Category 1 responders must have regard to the Met Office's duty to warn the public and provide information and advice, if an emergency is likely to occur or has taken place.

There are three severe weather risks in the UK National Risk Register – H17 (Severe storms and gales), H18 (Low Temperatures and Heavy Snow) and H48 (Heatwave). The table below gives the risks and the description of the risk in the UK National Risk Register along with examples of the potential impacts on infrastructure (not exhaustive):

Risk	Reasonable Worst Case	Potential Impacts
Severe storms and gales	Storm force winds affecting most of a region for at least 6 hours. Mean speeds in excess of 70mph with gusts in excess of 85mph.	• Loss of power • Loss of telecoms • Blocked road and train routes and flight disruption
Low temperatures and heavy snow	Snow falling and lying over most of the area for at least one week and after an initial fall of snow there is further snow fall on and off for at least 7 days. Most lowland areas experience some falls in excess of 10cm, a depth of snow in excess of 30cm and a period of at least 7 consecutive days with daily mean temperature below -3ºC.	• Loss of primary transport routes • Lack of staff availability • Impaired site access • Loss of power supplies • Loss of water supplies • Closure of local businesses • Increased demand for emergency power and water supplies • Increased demand for health and emergency services
Heatwave	Daily Maximum temperatures in excess of 28°C and minimum temperatures in excess of 15°C over most of the region for around 2 weeks at least, with 5 consecutive days where maximum temperatures exceed 32°C.	• Increased demand for health and emergency services • Impacts on electricity generation and cooling systems • Possible poor air quality • Possible impact on transport infrastructure • Increased risk of wildfires

Of these, the “Severe Storms and Gales” and “Low Temperatures and Heavy Snow” are most applicable to Scotland. The “Heatwave” risk in Scotland is very low although unusually high temperatures can result in some minor impacts.

More detail on **Wind** and its impacts can be found at:

- The Natural Hazards Partnership’s (NHP) Science Note available at http://www.naturalhazardspartnership.org.

More detail in the impacts of **Snow** and **Ice** can be found at:

- The Natural Hazards Partnership’s (NHP) Science Note available at http://www.naturalhazardspartnership.org.uk.

Heavy rainfall can also cause significant disruption but since the main impact from this is flooding, this is dealt with separately.

KEEPING SCOTLAND RUNNING

Stakeholders

Critical Infrastructure Operators / **Responder Communities** (Regional Resilience Partnerships (RRPs), Local Resilience Partnerships (LRPs) and Regional CIR Groups)

Infrastructure operators and responders should plan and prepare for the consequences of severe weather and ensure that they are aware of forecasts of severe weather.

National Centre for Resilience

The National Centre for Resilience (NCR) is Scotland's first resilience "centre of excellence", focusing on natural hazards. It is a multi-agency collaboration, involving many partners across the resilience, scientific and academic communities, and supported by a core team based at Maxwell House, Crichton Campus, Dumfries, part of the University of Glasgow estate.

The purpose of the NCR is to help build Scotland's resilience capabilities, particularly in relation to natural hazards, community resilience and critical infrastructure resilience, and to further enhance Scotland's leading resilience reputation. The Centre also performs a resilience research function to create new knowledge, identify gaps in resilience research and exploit existing knowledge to support best practice.

The NCR has six strategic priorities:

- To improve Scotland's resilience to natural hazards such as severe weather, flooding and landslides
- To build Community Resilience across Scotland
- To contribute to the development of Scotland's resilience research capability on natural hazards and community resilience
- To improve the protection and resilience of Scotland's water assets and critical infrastructure
- To scope the development of innovative approaches to natural hazards training
- To exploit world class multi-agency resilience arrangements at the local level to build national resilience.

Contact: Direct Line: +44 (0)1387 702034

Delivery

The Met Office provides a number of services to Category 1 and 2 responders to help them plan and prepare for severe weather – these include:

KEEPING SCOTLAND RUNNING

National Severe Weather Warning Service (NSWWS)

The Met Office warns the public and emergency responders of severe or hazardous weather which has the potential to cause danger to life or widespread disruption through our National Severe Weather Warning Service (NSWWS). Warnings are issued for rain, snow, wind, fog and ice. “Dual” warnings may warn for any two of these five elements. Warnings will be given a colour (Yellow, Amber or Red) depending on a combination of both the likelihood of the event happening and the impact the conditions may have.

Warnings are available via a variety of media but Category 1 and Category 2 responders can register to receive AMBER and RED warnings directly. Since September 2014 Yellow warnings highlighting the very low or low likelihood of medium or high impacts have also been pushed to registered responders. More details of the NSWWS and how they should be interpreted can be found on the Met Office’s website: www.metoffice.gov.uk/guide/weather/warnings

www.metoffice.gov.uk/weather/uk/advice/

Note: Infrastructure operators may take bespoke weather forecast services from the Met Office or other forecast providers to help them plan their operations and on which to base operational decisions. Warnings issued under the NSWWS should never be used in place of such bespoke services.

Civil Contingencies Advisors

In addition to the above information services there are three Civil Contingencies Advisors in Scotland. The Advisors’ primary function is to serve as a regional/national point of contact for the Met Office within the resilience community. This involves engaging with, and integrating into, national and local emergency planning groups so that emergency planners are fully aware of Met Office capabilities and can derive maximum benefit from these when dealing with any incident where the weather may play a role.

Amongst the principal tasks of the role are i) real-time response to weather-related emergencies; ii) input to those emergency plans which are, in any way, weather sensitive; and iii) involvement in exercises designed to test those plans.

During incidents the Advisors are able to support responders by telephone and in person, subject to availability. They are also able to respond to requests from Command and Control Centres or Science and Technical Advice Cells (STACs) and attend in person if required and if resources permit.

The Hazard Manager website for Emergency Responders

Hazard Manager is a Met Office interactive web portal which provides a range of services to help authorities prepare for and respond to emergency incidents that are caused or influenced by the weather. All weather warnings are interactively presented in Hazard Manager, along with weather forecasts and observations. Daily guidance from partners such as the Scottish Flood Forecasting Service and the Natural Hazards Partnership is also available.

Hazard Manager is designed to supplement the role of the Civil Contingencies Advisors in providing consistent weather-related information for the UK Emergency Response community. Due to the specialised nature of the information available, the website is not designed to function as a self-briefing tool but should be used in conjunction with advice from your regional Civil Contingencies Advisor.

Any Category 1 or 2 responder can request access, please see: https://www.metoffice.gov.uk/services/government/environmental-hazard-resilience/access

Flooding

Flooding can have a significant effect on infrastructure, often resulting in road closures, impacts on the rail network and potential inundation issues for utilities, especially drainage and sewerage systems.

The Scottish Environment Protection Agency (SEPA) has a strategic role in flood risk management including publishing Scotland's Flood Risk Management Strategies. Working with local authorities, Scottish Water and others, it is developing and using the best available information and data to ensure Scotland's efforts to tackle flooding are targeted at the most vulnerable areas. Their service delivery role includes providing flood forecasting and warning services, advice on flood risk to planning authorities and providing the public and communities with appropriate information and advice to be better prepared for floods.

SEPA is the official source of river and coastal flood warning information in Scotland and:

- Operates **flood warning schemes** in many parts of Scotland http://floodline.sepa.org.uk/floodupdates/quickdialcodes
- Provides **live flood warnings** through Floodline 0345 988 1188 and online at http://floodline.sepa.org.uk/floodupdates/
- Offers **free flood warning messages** direct to registered customers, by text or voice message http://www.sepa.org.uk/environment/water/flooding/floodline/

More general detail in the impacts of inland flooding can be found in the Natural Hazards Partnership's (NHP) Science Note available at http://www.naturalhazardspartnership.org.uk.

In addition to Floodline, SEPA also provides other services designed to help Category 1 and 2 responders plan and prepare for flooding, namely:

Flood Advisory Service

SEPA's four regionally-based Flood Advisors are at the heart of this service, delivering to partners and the public. Their purpose is to work with the public, strategic and professional partners to improve the understanding of flood risk, with the aim of improving their preparedness and response to flooding. Their key activities include:

- Facilitating communication and advice to our partners;
- Helping Category 1 & 2 responders to sign up for flood risk & warning information;
- Providing earlier information and sharing opinion on potential flood impact;
- Increasing confidence in forecast information;
- Providing benefit to organisations that do not have a strong relationship with SEPA.

During incidents they are able to support responders, through teleconferences and in tandem with Resilience Officers participating in formal RRP arrangements, subject to availability.

Scottish Flood Forecasting Service (SFFS)

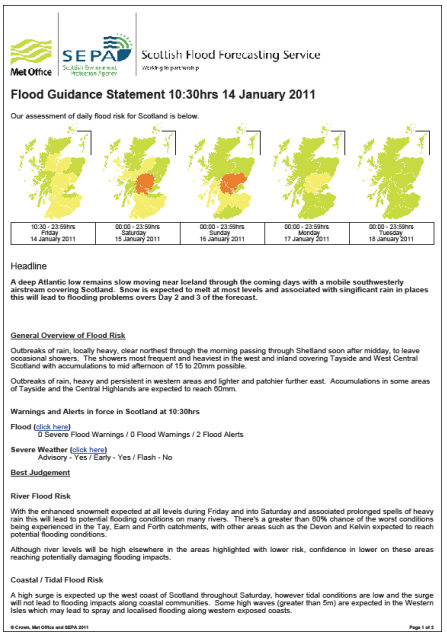
A joint initiative between SEPA and the Met Office, the Scottish Flood Forecasting Service combines hydrological and meteorological information so that both organisations can share their expertise to improve the accuracy of flood forecasts for the whole of Scotland.

The service offers a five day outlook on the likelihood and impact of flooding, targeted for emergency services, local authorities and other organisations with flooding management duties.

The joint service allows flexibility during flooding incidents where staff have the ability to co-locate during major flooding events to share facilities and services between SEPA and Met Office teams.

A Flood Guidance Statement is sent each day to registered Category 1 and 2 responders. This provides them with an assessment of the risk of flooding for the next five days from rivers, coastal and tidal areas.

The Flood Guidance Statement is uploaded each day to the Met Office's Hazard Manager website in the Flood Guidance (Scotland) section. Category 1 or 2 responders can register to receive the daily Flood Guidance Statement by emailing flooding@sepa.org.uk.



Met Office | SEPA | Scottish Flood Forecasting Service

Flood Guidance Statement 10:30hrs 14 January 2011

Our assessment of daily flood risk for Scotland is below.

10:30 - 23:59hrs Friday 14 January 2011	00:00 - 23:59hrs Saturday 15 January 2011	00:00 - 23:59hrs Sunday 16 January 2011	00:00 - 23:59hrs Monday 17 January 2011	00:00 - 23:59hrs Tuesday 18 January 2011

Headline

A deep Atlantic low remains slow moving near Iceland through the coming days with a mobile southwesterly airstream covering Scotland. Snow is expected to melt at most levels and associated with significant rain in places this will lead to flooding problems overs Day 2 and 3 of the foreast.

General Overview of Flood Risk

Outbreaks of rain, locally heavy, clear northest through the morning passing through Shetland soon after midday, to leave occasional showers. The showers most frequent and heaviest in the west and inland covering Tayside and West Central Scotland with accumulations to mid afternoon of 15 to 20mm possible.

Outbreaks of rain, heavy and persistent in western areas and lighter and patchier further east. Accumulations in some areas of Tayside and the Central Highlands are expected to reach 60mm.

Warnings and Alerts in force in Scotland at 10:30hrs

Flood (click here)
0 Severe Flood Warnings / 0 Flood Warnings / 2 Flood Alerts

Severe Weather (click here)
Advisory - Yes / Early - Yes / Flash - No

Best Judgement

River Flood Risk

With the enhanced snowmelt expected at all levels during Friday and into Saturday and associated prolonged spells of heavy rain this will lead to potential flooding conditions on many rivers. There's a greater than 60% chance of the worst conditions being experienced in the Tay, Earn and Forth catchments, with other areas such as the Devon and Kelvin expected to reach potential flooding conditions.

Although river levels will be high elsewhere in the areas highlighted with lower risk, confidence in lower on these areas reaching potentially damaging flooding impacts.

Coastal / Tidal Flood Risk

A high surge is expected up the west coast of Scotland throughout Saturday, however tidal conditions are low and the surge will not lead to flooding impacts along coastal communities. Some high waves (greater than 5m) are expected in the Western Isles which may lead to spray and localised flooding along western exposed coasts.

SEPA also publishes an **online flood risk map** to help you check whether an area is at risk from river or coastal flooding:
https://www.sepa.org.uk/environment/water/flooding/flood-maps/

Our Flood Risk hydrology staff also provide expert **flood risk advice** to external partners, organisations, companies and members of the public, and act as statutory consultees to local authority planning departments. More information on our Flood Risk duties and what we can provide is available at:
https://www.sepa.org.uk/environment/water/flooding/

Drought

A drought is a period of water shortage for people, the environment, agriculture or industry. A hot, dry summer is an example of a short, intense drought; and dry winters can have a big impact on water resources. Droughts are different to other hazards in that they tend to develop slowly, over a large area, with the exact beginning and end often difficult to identify. Several factors play a part including:

- lack of rainfall
- an environment, soil or bedrock, which is poor at retaining water or lacks underground storage
- hot weather, which increases evaporation of water

Drought impacts on a very wide range of sectors including agriculture, industry, water supply, fisheries, health, environment, wildfire, buildings. The impact of droughts is poorly documented in the scientific literature and it is often associated with potential risks, in particular on sectors such as health and water supply.

The Natural Hazards Partnership's (NHP) Science Note on Drought, available at http://www.naturalhazardspartnership.org.uk gives more information on drought and its potential impacts on the UK.

As part of its service to government the Natural Hazards Partnership (NHP) produces a daily strategic assessment of risks to the UK from natural hazards including drought. The NHP Daily Hazard Assessment is available to Category 1 and Category 2 responders via the "Hazard Advice" section of the Hazard Manager web portal.

The Natural Hydrological Monitoring Programme publishes every month a hydrological summary reporting current status of rivers, aquifers and reservoirs compared to the historical average. See http://www.ceh.ac.uk/data/nrfa/nhmp/nhmp.html.

Volcanoes

Volcanic eruptions abroad can have significant consequences in the UK, including disruptions to aviation and, depending on the volume of gases emitted, significant public health and environmental impacts. This subsequently leads to a number of secondary impacts, including disruption to critical supply chains and economic impacts. There are a number of volcanoes across Europe (such as Santorini in the Aegean Sea and Vesuvius in Italy) which could have consequences for the UK; but volcanoes in Iceland are of most concern because of the active volcanic nature of this region (it has 30 separate volcanic systems).

If periods of intense volcanic activity of this type coincide with unfavourable weather conditions they can result in significant ash incursions over the UK which can result in disruption to aviation as the fine ash in the plume can, in sufficient concentrations, damage aircraft engines. High-pressure weather systems, which tend to result in more stable weather conditions, can result in prolonged periods of unfavourable weather conditions and therefore prolonged ash incursions over the UK.

Once in the atmosphere, ash, gases and aerosols are rapidly dispersed by wind, potentially resulting in higher than usual concentrations of various gases and particles at flight altitude. The ash, gases and aerosols are gradually brought down to ground

level by atmospheric pressure and precipitation (for instance, rain or snow) and this may result in higher than usual concentrations of these gases at ground level and deposits of chemicals on the ground.

The volcanic risks in the UK National Risk Register are given below along with examples of the potential impacts on infrastructure (not exhaustive).

Risk	Reasonable Worst Case	Potential Impacts
Explosive volcanic eruption (ash)	Volcanic ash incursions for up to 25 days. The entire UK mainland and potentially other parts of Europe could be affected for up to 10 of these days. A single period of closure within the 3 month eruptive episode may last up to 12 consecutive days, depending on meteorological conditions.	• Sporadic and temporary closures of significant parts of UK airspace
Severe effusive volcanic eruption (gases)	Severe volcanic eruption, generating large amounts of gas and ash over a five month period affecting UK and northern Europe.	• Increased demand for healthcare systems • Closure of UK airspace • Reduced yield from harvests

As part of its service to government the Natural Hazards Partnership (NHP) produces a daily strategic assessment of risks to the UK from natural hazards including volcanic activity. This risk assessment is produced by the Met Office using information from Icelandic Meteorological Service which monitors volcanic activity in Iceland, the most likely source of any volcanic related impacts to the UK. The NHP Daily Hazard Assessment is available to Category 1 and Category 2 responders via the “Hazard Advice” section of the Hazard Manager web portal.

However, under the auspices of the World Meteorological Organization, the Met Office has responsibilities, as one of the nine Volcanic Ash Advisory Centres (VAAC) around the world, to provide forecast guidance up to 24 hours ahead to support decision-making. This guidance is provided to the Civil Aviation Authority as the lead agency, NATS, airports and airline operators in order to support their decisions on whether aircraft can fly safely.

The Met Office London VAAC uses a range of technologies and expertise to predict the movement of volcanic ash. The Met Office dispersion model forecasts are routinely validated, verified against all available observations, such as from satellite, Radar, Lidar and aircraft, and advice is then adjusted accordingly.

Guidance charts showing the predictions are available, during volcanic eruptions, on the Met Office website at http://www.metoffice.gov.uk/aviation/vaac/.

Space Weather

Weather on Earth, such as wind, snow and rain, has different terrestrial impacts and different meteorological causes. Similarly, space weather, including geomagnetic storms, radiation storms and solar radio noise, has different terrestrial impacts and is the result of different types of solar phenomenon, including coronal mass ejections (CMEs), solar energetic particle events, solar flares and solar radio bursts affecting the Earth. Current understanding is that a severe space weather event could have impacts on a range of technologies and infrastructure, including power networks, satellite services, transport and digital control components.

The space weather risk in the UK National Risk Register is given below along with examples of the potential impacts on infrastructure (not exhaustive).

Risk	Reasonable Worst Case	Potential Impacts
Severe Space Weather	Resulting from solar eruptions causing rapidly varying geomagnetic fields on earth.	• Disruption to satellite services for several days • Loss of power supplies • Loss of satellite communications and computer based control systems • Disruption to monetary systems • Interruptions to Global Positioning System (GPS) • Disruption to broadcast services • Disruption to aviation sector

The Carrington Event in 1859 is described as the perfect storm because the largest CMEs, radiation storms and solar flares ever recorded happened during this period. Government has worked together with space weather scientists and engineers as well as industry and asset owners from the communications, transport and energy sectors to assess the risk of a severe space weather event of a similar scale to the Carrington Event.

However, space weather science is a relatively young field and its impacts on modern society are only recently coming to the fore as our dependence on technologies vulnerable to solar phenomena increases. Therefore significant work is continuing to better understand and plan – in a proportionate way – for the expected impacts of a severe space weather event. In particular, the government and partners in the energy sector are working closely together to clarify the potential impacts of a severe event on electricity assets and networks.

More information on space weather and its potential impacts on the UK can be found at https://www.metoffice.gov.uk/weather/specialist-forecasts/space-weather

The Met Office has developed a space weather prediction capability which became operational in April 2014. The Met Office Space Weather Operations Centre delivers warnings and alerts to key infrastructure operators. . The Met Office has daily operational coordination teleconferences with the US NOAA Space Weather Prediction Centre, the global centre for space weather forecasts.

During periods of increased concern, the Met Office will produce specific daily briefings which will be made available to the response community

The British Geological Survey (BGS) examine solar activity daily and forecast if this is likely to have any geomagnetic effect on Earth. If this 'space weather' indicates that a large magnetic storm is possible in the next few days BGS may send out a space weather alert.

You can sign-up to receive a Geomagnetic Disturbance Alert email from BGS – see http://geomag.bgs.ac.uk/data_service/space_weather/alerts.html.

Geological Hazards

In general, the UK is a geologically stable region. Large scale incidents, such as earthquakes, no longer significantly affect our country and therefore very few geological hazards feature within the National Risk Register. However, at the local level, risk is determined by the geological characteristics of the specific location under consideration. As a consequence, the impact of geological hazards still carries a significant cost for UK society. For example, the British Geological Survey has estimated that cost of damage to property caused by the swelling and shrinking of clay was in excess of £3 billion for the last decade.

It is therefore important that geological risks are considered as part of a site specific risk assessment. Landslide is one of the most common geological hazards to affect Scotland.

More information on the **Landslides** can be found at:

- The National Centre for Resilience (NCR), Natural Hazard Overview (see Guide 6 Annex B)
- A British Geological Survey (BGS) Geohazard Note, “Landslides” which can be found at:
    - http://eprints.gla.ac.uk/166428/1/166428.pdf
    - http://www.bgs.ac.uk/downloads/start.cfm?id=2497.

For more information on geological hazards see: https://www.bgs.ac.uk/products/geohazards/home.html

Wildfires

Wildfires are any unintentional, self-sustaining outdoor fire which consumes significant quantities of natural vegetation as its primary fuel source. Several factors affect wildfire behaviour. Many of these, such as the vegetation type and topography, remain relatively static over time. It is the seasonal cycle of the vegetation and changes in the weather conditions and the subsequent changes in the state of the vegetation which lead to changes in wildfire behaviour.

For more detailed information see the Natural Hazards Partnership’s (NHP) Science Note available at

http://www.naturalhazardspartnership.org.uk/products/science-notes/

KEEPING SCOTLAND RUNNING

There is work ongoing to provide organisations such as Fire & Rescue Services with assessments of risk of wildfire but at this time this is not an operational or publicly available service.

In Scotland, the Muirburn Code provides statutory restrictions that must be followed when fire is used as a land management tool. It has been recently updated to reflect legislative changes introduced by the Wildlife and Natural Environment (Scotland) Act 2011. Adherence to the code, which sets out best practice for land managers carrying out muirburn, is a requirement of cross compliance. The Code can be found online at: https://www2.gov.scot/Resource/Doc/355582/0120117.pdf.

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Guide 6
Building Resilience to a Changing Climate (Adaption)

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 6

Building Resilience to a Changing Climate (Adaptation)

Overview

What	This guide seeks to: • Provide relevant information to those responsible for critical infrastructure in Scotland to help build resilience to the impacts of the changing climate.
Who	This guide is aimed at: • **Government** - CI Resilience Policy leads in Scottish Government • **Critical Infrastructure (CI) Operators** – Strategic Management, Resilience and Business Continuity Management (BCM) leads • **Responder Communities** – Resilience Partnerships (RPs), Resilience and BCM leads
Why	We are already seeing evidence of Scotland's climate changing. Over the last few decades our climate has warmed, sea-levels have risen, rainfall patterns have changed and we have been impacted by extreme weather events. Climate projections for the next century indicate that the climate trends observed over the last century will continue and intensify over the coming decades. We can expect future changes in climate to be far greater than anything we have seen in the past. These changes pose serious risks for infrastructure. Legislative duties are now also in force requiring major public bodies, including many infrastructure operators, to exercise their functions in a way best calculated to deliver the Statutory Scottish Climate Change Adaptation Programme and, report progress annually as part of Public Bodies Duties Mandatory Reporting. Critical infrastructure operators in the private sector are equally at risk and should build climate change adaptation into their resilience planning and risk management strategies.
How	To avoid longer-term impacts on people and the economy, it is essential that investments in new infrastructure, as well as the adaptation of existing infrastructure, are considered in the context of climate change risks and impacts. There is still considerable uncertainty about the nature and extent of future climate change. Adaptation of infrastructure will therefore need to be flexible in order to cope with a wide range of possible changes. This will involve a combination of measures that include[24]:

[24] The Adaptation Principles set out above are taken from Dawson RJ (ed.) (2015) A Climate Change Report Card for Infrastructure. LWEC Report Card. Living With Environmental Change. ISBN 978-0-9928679-4-2 copyright © Living With Environmental Change.

	• Retrofitting existing infrastructure to be more resilient to changed weather conditions • Adding redundancy into infrastructure networks in order to provide viable alternatives when some parts of the network fail • Building in flexibility so that infrastructure assets can be modified in future without incurring excessive cost • Designing systems that consider how changes in climate will alter supply, demand and risks • Identifying alternative and creative ways of delivering services, e.g. the use of green spaces to aid flood management • Incentivising reduced demand for services through behaviour change and the use of more efficient technologies • Ensuring infrastructure organisations and professionals have the necessary skills and capacity to implement adaptation measures

Case Study

Scottish Water River Spey Flooding Programme

This case study demonstrates how Scottish Water has addressed the impacts of flooding on the River Spey through incorporating adaptation projects in their five year capital maintenance programme.

How flooding affects infrastructure and water quality
River flows in the River Spey can be relatively low during dry weather. During periods of snowmelt and heavy rain there is a significant rise in the river level onto the flood plain. Scottish Water's aim was to improve the level of treatment to protect and improve water quality, and at the same time make the infrastructure resilient to an increased risk of flooding. With climate change likely to alter rainfall patterns and bring more heavy downpours, flood risk is expected to increase in the future.

What we did
We worked with Local Authority planners and the Scottish Environment Protection Agency (SEPA), and consulted with various stakeholder groups and the Cairngorm National Park Authority. This identified development growth pressures and flood risk areas as an issue throughout the River Spey catchment. This was the basis for planning a series of upgrades to the treatment plants at Newtonmore, Kingussie, Aviemore, Boat of Garten, Grantown and Nethybridge, as well as modifications to two pumping stations.

Climate change was a focus in this planning:
• Detailed flood risk assessments were carried out to identify the areas prone to flooding.
• Treatment plants were sited to avoid the impact of increased flood events
• Resilience to flood risk was built into the upgraded facilities.
• A variety of methods were used to adapt the sites to future flood risk. This included
- using bunds to prevent flood water reaching the treatment plant,
- building up the land surrounding the plant, and
- creating compensatory storage for flood waters at other points upstream.

Noting the key findings from the climate projections, the improvements also took into account the possibility of longer periods of dry weather. This presented challenges for the level of treatment required.

KEEPING SCOTLAND RUNNING

What has changed as result of this process?
The upgraded treatment plants and pumping stations can continue to operate and treat wastewater even when the River Spey bursts its banks. The work has both increased the flood resilience of the assets and improved their capability to protect the Special Area of Conservation of which the River Spey comprises a large part.

Recommendations
• Engage and collaborate with a wide range of organisations to explore options and opportunities
• Consider key findings from the climate projections to assess future business risk
• Review existing strategic plans and policies for exposure to climate-related risks and identify opportunities for adaptive strategies to be incorporated into them and their associated processes.

Next steps
• Complete work with Local Authorities on catchments at risk of flooding and agree a prioritised strategy for flood mitigation measures.
• Incorporate climate change scenarios when designing all new treatment plants and upgrading existing ones.
• Use the outcomes from the climate risk assessment to inform future investment decisions.

For full case study information see:
http://www.adaptationscotland.org.uk/how-adapt/case-studies/including-adaptation-capital-maintenance-programmes-Scottish

Background

Critical infrastructure is a broad term used to describe Critical National Infrastructure (CNI) and other infrastructure of 'national significance', the loss or compromise of which would have severe, widespread effects impacting on the UK, as well as infrastructure and assets of local significance.

Disruption to critical infrastructure would lead to the loss or disruption of essential services, or present a hazard to the community, or reduce the effectiveness of an emergency response, and/or could lead to loss of life. Disruption of essential services is also expected to have a significant impact on commercial and business activity. As such, critical infrastructure needs to be robust in the face of many risks and pressures that it faces. Infrastructure typically has a long operational life, so needs to not only consider current risks, but future risks.

Scotland's climate is changing with increases in severe weather events, changes in rainfall, sea level rise and increased temperatures already affecting infrastructure. These changes are set to increase in the decades ahead and should be factored in to decisions about infrastructure design, planning and operation.

This document provides guidance about the changes in climate observed and projected for Scotland; sets out key risks for infrastructure; signposts to sources of

information and support; provides a summary of legislative and policy drivers and identifies adaptation principles.

Weather is what we experience on a day-to-day and year-to-year basis. It can be very variable.

Climate is the average of weather conditions over a long period of time (usually a 30 year period), while **climate change** is a long-term trend in climate

"Climate is what you expect – weather is what you get" R. A.Heinlen, 1973

Resilience: 'the capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity"[25]

Adaptation – the adjustment in economic, social or natural systems in response to actual or expected climate change, to limit harmful consequences and exploit beneficial opportunities.

Guidance

Scotland's changing climate

We are already seeing evidence of Scotland's climate changing. Over the last few decades our climate has warmed, sea-levels have risen, rainfall patterns have changed and we have been impacted by extreme weather events. Temperatures have been increasing, with the last decade the warmest since records began. Rainfall has been increasing in Scotland over the last thirty years, with more heavy downpours.

Climate projections for the next century indicate that the climate trends observed over the last century will continue and intensify over the coming decades. We can expect future changes in climate to be far greater than anything we have seen in the past.

Key long-term climate change trends for Scotland are:

- Weather will remain variable, it may become more variable
- Typical summer is hotter and drier
- Typical winter / autumn is milder and wetter
- Sea level rise

We can also expect to see:

- Increase in summer heat waves, extreme temperatures and drought
- Increased frequency and intensity of extreme precipitation events

[25] Charles Edwards; Resilient Nation; Demos; 2009

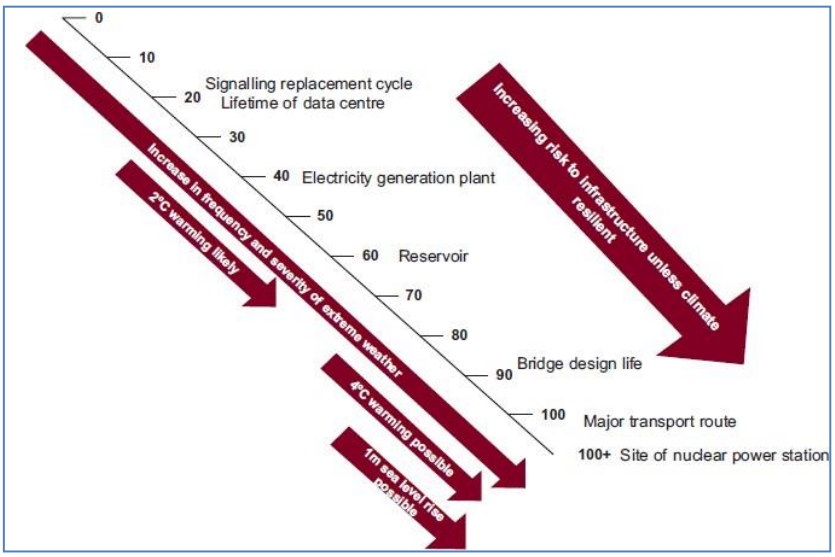
- Reduced occurrence of frost and snowfall

For further information about climate trends and projections visit the Adaptation Scotland website: www.adaptationscotland.org.uk

Risks to infrastructure

The long operational lifetime of infrastructure systems means that they are vulnerable to both existing and future climate risks. It is therefore essential that these risks are considered during the construction of new assets and also in the upgrade of existing assets.

Figure 1: General lifetime of infrastructure assets shown alongside projected temperature increase[26]



Infrastructure in Scotland is exposed to a wide range of climate change impacts. Impacts on some assets have the potential to cascade on to others as part of interdependent networks.

Flooding poses the greatest long-term risk to infrastructure performance from climate change but, growing risks from heat, water scarcity and slope instability could be significant. Storms will also continue to pose a serious challenge.

[26] Image extracted from Defra, 2011. *Climate Resilient Infrastructure: Preparing for a Changing Climate*. [online] Available at: http://www.defra.gov.uk/publications/2011/05/09/climate-resilient-infrastructure

Figure 2: Summary of Climate Change risks to UK infrastructure

The UK Climate Change Risk Assessment 2017: Evidence report identifies risks and opportunities for infrastructure including:

Risks to infrastructure services from river, surface water and groundwater flooding

Infrastructure across all sectors is exposed to coastal, river, surface water and groundwater flooding. Flooding already accounts for significant losses in infrastructure services, with outages caused by flooding tending to last longer than other weather-related hazards.

The risk of flooding is expected to rise, as patterns of rainfall become more intense. Western areas of Scotland in particular could be subject to significant increases in heavy winter rainfall.

Risks to infrastructure services from coastal flooding and erosion

Scotland has significant infrastructure assets located in coastal areas and so potentially exposed to flooding from the sea. Key infrastructure assets located in the coastal zone include power stations, ports, roads and rail networks. Some stretches of the Scottish coastline are actively eroding, exposing some road and rail networks.

Risks of sewer flooding due to heavy rainfall

Combined sewer systems have a limited capacity and cannot easily be adapted to deal with increased intensity and duration of rainfall, particularly in densely populated urban areas. An additional challenge is the issue of ‘urban creep’, when the paving over of front gardens or large patio areas can impact on drainage, sewer and surface water flooding.

Without additional action being taken, it is estimated that a combination of climate change, population growth and continued urban creep will lead to an increase in the amount of surface water entering the sewer system. This is likely to lead to increased frequency of the sewer system exceeding its capacity and increased risk of surface water flooding when this occurs.

Risks to bridges and pipelines from high river flows and bank erosion

Peak river flows in Scotland are expected to increase. High and fast river flows can cause localised riverbank erosion, undermining structures such as bridges and exposing buried cabling and pipework.

Risks to transport networks from slope and embankment failure

Older, less well compacted earthworks such as those supporting the rail network are deteriorating at a faster rate than newer earthworks built to more modern construction standards. Increased incidences of natural and engineering slope failure effecting the road and rail network in the winters of 2012/2013 and 2013/2014 demonstrate their vulnerability to the type of more frequent, intense rainfall events that are expected.

Risks to public water supplies from drought and low river flows

At a national level, Scotland currently has a comfortable 22% supply/demand surplus in the public water supply. However, not all individual Water Resource Zones are in a surplus position. Climate change is expected to restrict the supply of water whilst population growth will add to demand.

Risks to energy, transport and digital infrastructure from high winds and lightning

High winds are a significant cause of damage and disruption to electricity and rail networks. Most of this damage and disruption is caused by trees and branches falling onto power lines and railway tracks.

The observed increase in the length of the growing season, which has gained ten days in Northern Europe since the 1960s, is likely to continue and will, in the absence of additional management, increase the amount of tree-related damage and disruption.

Risks to offshore infrastructure from storms and high waves

Increases in severe weather could increase the challenge of managing and maintaining offshore infrastructure. For example, extreme weather conditions are likely to increase scour and erosion of sediment around windfarm foundations leading to the potential for engineering failure in the foundations.

These challenges can be managed through the use of Third Party Verification for renewable demonstrator projects and Third Party Certification for commercial projects. These independent assessments include assessment of risks posed by 1 in 100 year

events. Third Party Verifications are normal process for developers and are needed to gain insurance cover. They should include an assessment of changing frequency of severe weather events.

Risks to transport, digital and energy infrastructure from extreme heat

Rail and electricity transmission and distribution networks are the sectors most vulnerable to impacts during periods of high temperatures. Hot weather has the potential to cause train service cancellations and speed restrictions, and require de-rating of overhead power lines. High temperatures can also affect what maintenance can be performed, for example making tensioning rail track difficult due to thermal expansion or by new road tarmac drying too quickly.

Potential benefits to water, transport, digital and energy infrastructure from reduced extreme cold events

Cold weather, including snow and ice, is a major cause of disruption to transport services, and electricity transmission and distribution. For example, snow and ice account for 13% of weather-related impacts to the UK high voltage electricity distribution network.
The average number of extreme cold days is likely to reduce over the course of the century. Cold winters will still be possible, but are expected to become increasingly unlikely. There may be opportunities arising from fewer snow and ice days reducing winter disruption and maintenance costs.

Risks of cascading failures from interdependent infrastructure networks

Infrastructure networks do not operate in isolation and climate change impacts affecting one infrastructure system have the potential to cascade and impact other interdependent networks.

Information and support

A wide range of peer to peer support, guidance and tools are available to infrastructure operators. Key sources are outlined below:

Infrastructure Operators Adaptation Forum

The Infrastructure Operators Adaptation Forum (IOAF) is a UK wide forum that brings together infrastructure operators, regulators, government, trade associations, professional bodies and academics to learn from each other and work together to address adaptation challenges.

The IOAF online community is open to all infrastructure operators and interested parties and includes a resource catalogue.

The IOAF also have working groups where members address shared challenges including: Climate risk assessment approaches; Interdependencies and cascade failure risks; Embedding adaptation in organisations and; Implications for standards. All infrastructure operators are invited to consider joining an IOAF working group.

To join the online community:

1. Register with the Institution of Engineering Technology for a free online account http://www.theiet.org/index.cfm
2. Visit the communities page https://communities.theiet.org/communities and request to join the IOAF community

To find out about working groups or for more information about the IOAF contact: climatechange@environment-agency.gov.uk

Adaptation Scotland Programme

The Adaptation Scotland programme provides advice and support to help organisations and communities in Scotland prepare for, and build resilience to the impacts of climate change. The programme includes a range of tools and projects that are relevant for infrastructure operators including:

- Climate information – Information about past trends, climate projections and links to detailed SEPA, Met office and UKCP18 climate projections.
- Tools and resources - including a toolkit to support consideration of climate risks in built environment and infrastructure projects
- Training and events – A wide range of training and events to develop adaptation skills and networks.

Visit www.adaptationscotland.org.uk or contact adaptationscotland@sniffer.org.uk to find out more about the support listed above.

Climate Ready Clyde

The Climate Ready Clyde initiative is creating a shared vision, strategy and action plan for an adapting Glasgow City Region.

- In 2018 Climate Ready Clyde published a risk and opportunity assessment for the Glasgow City Region which includes assessment of infrastructure risks – view the risk assessment here: https://www.crc-assessment.org.uk/
- Contact Climate Ready Clyde to find out more about their work: visit www.climatereadyclyde.org.uk email climatereadyclyde@sniffer.org.uk

Scottish Environment Protection Agency (SEPA)

SEPA works closely with other organisations responsible for managing flood risk including Local Authorities, Scottish Water, the National Park Authorities and Forestry Commission Scotland through a network of partnerships and stakeholder groups to ensure that a nationally consistent approach to flood risk management is adopted.

Visit http://www.sepa.org.uk/environment/water/flooding/ for more information about Flood risk in Scotland

Further reading

A wide range of research is available to inform adaptation planning and action for infrastructure.

Key sources are outlined below:

Committee on Climate Change (CCC)

The CCC is an independent, statutory body established under the UK Climate Change Act 2008. The committee provides advice on progress made in preparing for climate change.
Relevant publications include the UK Climate Change Risk Assessment evidence reports (July 2016).These include a report on risks to infrastructure and a summary report of risks for Scotland.
View the publications at https://www.theccc.org.uk/publications/

Adaptation and Resilience in the Context of Change (ARCC) Network

The ARCC was funded by the Engineering and Physical Sciences Research Council and focused on adaptation and resilience in buildings, urban environments, transport networks, water resources and energy systems. The ARCC website has a wide range of research and publications relevant to infrastructure operators.
Visit the ARCC website: http://www.arcc-network.org.uk/

LWEC climate Change Impacts report cards

LWEC's climate change impacts report cards present the latest evidence on how climate change is affecting different aspects of our environment, economy and society. They are designed for decision-makers at any level, but in particular for use by policy advisors, ministers and local authorities.
Download the infrastructure report card here:
http://www.nerc.ac.uk/research/partnerships/lwec/products/report-cards/infrastructure/

Delivery

Legislative and policy drivers for action

- Climate Change (Scotland) Act 2009

The Climate Change (Scotland) Act 2009 requires a climate change adaptation programme to be developed every five years to address the risks identified in successive UK Climate Change Risk Assessments (CCRAs). The first UK CCRA was published in January 2012 and the first Scottish Climate Change Adaptation Programme was published in 2014.

The Public Bodies Climate Change Duties, established by the Climate Change (Scotland) Act 2009 require that Public Bodies exercise their functions in a way best

calculated to deliver any statutory adaptation programme. In 2015 the Scottish Government introduced an Order requiring all 151 Public Bodies who appear on the Major Player list to submit an annual report, detailing their compliance with the climate change duties.

- Civil Contingencies Act (2004)

The Civil Contingencies Act (2004) requires Public Bodies to assess the risk of emergencies occurring and maintain plans to ensure if an emergency occurs that services are able to continue.

Two of the three meanings of the term "emergency" can be interpreted as relating to severe weather or climate change. The first is *"an event or situation which threatens serious damage to human welfare".* This includes where the emergency involves, causes or may cause loss of human life; human illness or injury; damage to property; disruption of supplies of money, food, water, energy or fuel; disruption of a system of communication' disruption of facilities for transport; or disruption of services relating to health.

The second relevant meaning is *"an event or situation which threatens serious damage to the environment".* This includes where the emergency involves, causes or may cause (a) contamination of land, water or air with biological, chemical or radioactive matter, or (b) disruption or destruction of plant life or animal life."

National Planning Framework 3, Scottish Planning Policy, Land Use Strategy and Flood Risk Management Strategies are all examples of policy and strategy drivers.

KEEPING SCOTLAND RUNNING

RESILIENT ESSENTIAL SERVICES
Scottish Government's
Strategic Framework
2020-2023

Guide 7
Critical Infrastructure Resilience (CIR) Continuous Improvement Model

Scottish Government
Riaghaltas na h-Alba
gov.scot
www.readyscotland.org

KEEPING SCOTLAND RUNNING

Guide 7

Critical Infrastructure Resilience (CIR) Continuous Improvement Model

Overview

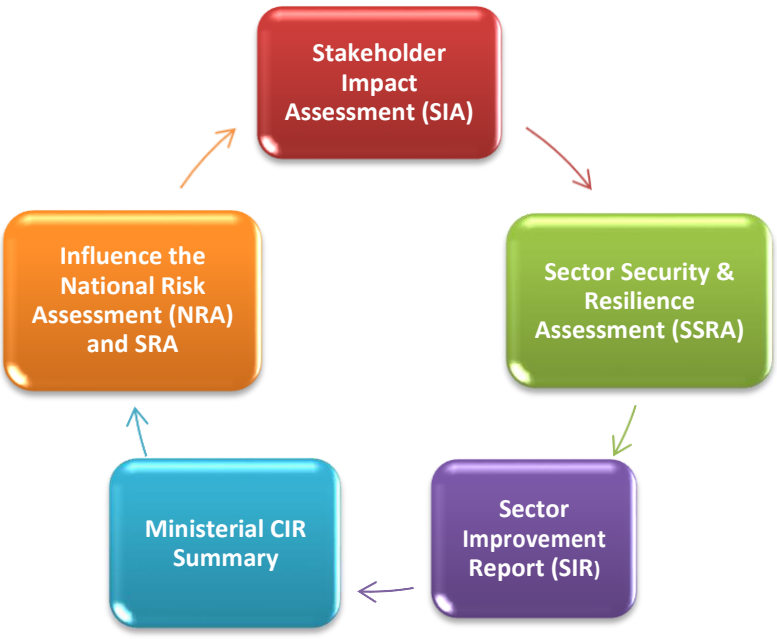
What	This guide seeks to: • Demonstrate a common cross-sector approach to continuous Critical Infrastructure Resilience (CIR) improvement in Scotland. It explains the process by which continuous improvement will be assessed and monitored by the Scottish Government.
Who	This guide is aimed at: • **Government** – Critical Infrastructure (CI) Resilience Policy leads in Scottish Government • **Critical Infrastructure (CI) Operators** - Strategic Management, Security and Resilience leads • **Responder Communities** – Resilience Partnerships (RPs), Security and Resilience leads
Why	The benefits of engagement in the continuous CIR improvement process include: • A consistent and standard approach across all sectors in Scotland • Enhanced organisational resilience • Economic and reputational advantage • Reassurance that the wider Scottish Government vision of a 'resilient critical infrastructure in Scotland' is being realised
How	This will involve engagement in and completion of four key CIR performance documents - Stakeholder Impact Assessments (SIA), Sector Security and Resilience Assessments (SSRA), Sector Improvement Reports (SIR) and a biennial Ministerial Summary.

KEEPING SCOTLAND RUNNING

Background

To support sectors in developing a culture of continuous improvement and to facilitate the capturing of relevant performance data, the Scottish Government has worked in collaboration with CIR stakeholders to develop the following model of CIR continuous improvement.

- As can be seen in the diagram below, the process begins with a robust assessment of their infrastructure at company/organisation or asset level (Stakeholder Impact Assessment)
- These separate SIA responses are then collated into an overarching sector security and resilience overview (Sector Security & Resilience Assessment)
- This information is then summarised for reporting purposes (Sector Improvement Report), which will be submitted by each of the Sector Resilience Groups or policy leads for the attention of the Critical Infrastructure Resilience Partnership meetings which will be held on a six monthly basis
- The SIR and the SSRA will also be used to prepare a biennial report for Ministers on critical infrastructure resilience in Scotland (Ministerial CIR Summary)
- The model also allows the Scottish CIR perspective to influence the on-going development of the National Risk Assessment (NRA) at UK Government level and the Scottish Risk Assessment as it develops
- Collating and identifying investment gaps to improve infrastructure resilience is a new element being developed and will feature more prominently in future iterations of this guide



Guidance

Stakeholder Impact Assessment (SIA)

The Stakeholder Impact Assessment (SIA) provides answers to the 4 key questions used to assist in the risk assessment process on which the Sector Security & Resilience Assessment (SSRA) and the Sector Improvement Report (SIR) are based. The SIA provides an overview of individual key companies and organisations that make up each sector, their rationale for criticality, their identified vulnerabilities and describes mitigation, protection and contingencies in place to tackle vulnerabilities.

The SIA will be completed with each of the sectors key stakeholders using a standardised template and guidance. The template includes information on the following:

- Sector
- Sub-Sector (if relevant)
- Scottish Government Policy Lead
- Rationale for Criticality including the identification of critical sites and systems
- Planning Assumptions and Mitigation/Contingencies
- Reasonable Worst Case Scenario(s)
- Testing and Exercising
- Significant Disruptive Events experienced by stakeholder in recent years
- Impacts on other Sectors
- Climate Change
- Expectations of SG and Resilience Partnerships.
- Contributions to the Resilience landscape in Scotland

Given the sensitivities associated with a detailed analysis of the criticality and vulnerabilities associated with assets/systems, the SIA will be jointly owned by the operator/owner and Scottish Government and protectively marked as Official – Sensitive - Commercial. The SIA will be shared (subject to appropriate information security arrangements) with relevant Scottish Government and UK Government departments and the Centre for the Protection of National Infrastructure (CPNI). In addition, the SIAs will be made available to the relevant Scottish Government Minister if requested.

Sector Security & Resilience Assessment (SSRA)

While the Stakeholder Impact Assessment (SIA) provides an overview of individual asset owners and operators, the Sector Security & Resilience Assessment (SRRA) provides an overview of the relevant sector/sub sector as a whole. For example, in the Communications Sector in Scotland, the individual operators within each of the four sub sectors – Telecoms, Postal, Broadcasting and Internet will each complete a SIA. In turn, these responses will be collated into Telecoms, Postal, Broadcasting and Internet Sector Security & Resilience Assessment's (SSRA) for Scotland.

SSRAs will be developed through a collaborative approach between lead officials in Scottish Government, Sector Sponsor Departments in UK Government, sector regulators and asset operators.

UK Government Departments with policy responsibility for the security and resilience of sectors each produce Sector Security and Resilience Plans on an annual basis. These documents are shared with the Scottish Government and increasingly SG is being invited to submit information as to what is happening in Scotland.

The SSRAs will be completed using a standardised dashboard style template and guidance. The template includes:

- An Executive Summary of the Sector
- An overview of criticality
- An overview of the identified vulnerabilities (using information provided in the SIAs)
- An overview of Sector resilience (against each of the identified vulnerabilities included in the sub sector SIAs)
- An overview of Sector resilience to the current National Risks,
- A programme of measures/steps for achieving the appropriate level of ambition for resilience (mitigating the risks and vulnerabilities identified)

Given the sensitivities associated with a detailed analysis of the vulnerabilities of each sector's critical assets, the SSRA will be owned by the Scottish Government's Resilient Essential Services Team and protectively marked Official – Sensitive and stored securely. The SSRA will be shared (subject to appropriate information security arrangements) with relevant Scottish Government and UK Government departments and the Centre for the Protection of National Infrastructure (CPNI). In addition, the SSRAs will be made available to the relevant Scottish Government Minister if requested.

Sector Improvement Report (SIR)

The Sector Improvement Report (SIR) is a common reporting and performance management framework in a dashboard format. This enables each of the Critical Infrastructure Sector Resilience Groups in Scotland or policy leads to report on progress to the Critical Infrastructure Resilience Partnerships (CIRP) group against an agreed set of improvement criteria. An annual timeline for the reporting process ensures that the SIR complements the UK process co-ordinated by the Cabinet Office – see the diagram in the 'Delivery' section below.

The SIR will be completed by each of the Critical Infrastructure Sector Resilience Groups or policy leads in order to provide the Critical Infrastructure Resilience Partnership with assurance on continuous CIR improvement. The SIR template includes:

- Targets
- Progress against agreed work plans.
- Future Milestones/Next Steps

The SIR has been designed to 'ensure that delivery and progress of the CIR Strategy is monitored and reviewed on an ongoing basis and to determine that effective outcomes are achieved'.

Delivery

Continuous CIR Improvement Model Timeline

The governance arrangements for CIR in Scotland and also at a UK Government level are supported by the following timeline. In particular, the annual review of SSRAs and the submission of a biennial CIR Summary for Ministers, requires a degree of synergy with Sector Resilience Groups, policy leads and Critical Infrastructure Resilience Partnership meeting dates. In view of this, the timeline has been established in order to provide a common standard reporting cycle for stakeholders.