Rail Delivery Group

National Rail

RDG Approved Code of Practice:
Rail Emergency Management - Response

RDG-OPS-ACOP-011
Issue 1.1 – 13 June 2024

About this document

Explanatory note

The Rail Delivery Group (RDG) is not a regulatory body and compliance with Guidance Notes or Approved Codes of Practice is not mandatory; they reflect good practice and are advisory only. Users are recommended to evaluate the guidance against their own arrangements in a structured and systematic way, noting that parts of the guidance may not be appropriate to their operations. It is recommended that this process of evaluation and any subsequent decision to adopt (or not adopt) elements of the guidance should be documented. Compliance with any or all of the contents herein, is entirely at an organisation's own discretion.

Other Guidance Notes or Approved Codes of Practice are available on the Rail Delivery Group (RDG) website.

Executive summary

The UK railway faces a range of threats, hazards and operational challenges that have the potential to jeopardise its ability to run services safely, securely, and reliably and to uphold customer confidence. Increased, 'integrated emergency management' (hereafter IEM) capability has never been more critical. In the past few years, transport organisations have had to show unprecedented levels of resilience.

This Approved Code of Practice (ACOP) with Guidance Notes (GN) is the third document issued in response to the nine recommendations arising from the industry Rail Resilience Project (RRP) Emergency Management Review: Findings & Recommendations Report (completed June 2021); it is the second ACOP in a series across the prepare-respond-recover model for IEM:

- RDG-OPS-ACOP-010 with Guidance: IEM, Preparation
- **RDG-OPS-ACOP-011 with Guidance: IEM, Response**
- RDG-OPS-ACOP-012 with Guidance: IEM, Recovery

This ACOP sets out the requirements for the rail industry to respond to emergencies within the remits of IEM activities. The Code addresses the legal and regulatory provisions required when responding to emergencies and reflects industry guidance and other best practice for response. The Code outlines these requirements across key topics of emergency response, command and control, responder requirements and data handling.

The Code aims to be user friendly across the rail industry and is aimed at those with responsibility for local implementation and management of IEM activities within railway undertakings and infrastructure managers. During the preparation of this ACOP, all key stakeholders have had the opportunity to provide feedback and inputs to the development of this work.

Issue Record

Issue	Date	Comments
1.0	23/02/2024	First Draft
1.1	13/06/2024	Final Document Issue

This document is reviewed on a regular 3-year cycle or whenever a material change in provisions is required.

Written by / Prepared by:
Claire Hunt, Heather Griffin, Robert Sunley & Emma Leafe of AtkinsRéalis.

RDG RRP Delivery Team
Contact: Andrew Wade

Authorised by:
Rail Resilience Steering Group (RRPSG)

Steve Enright, Independent Chair Rail Resilience Steering Group (RRPSG)

The following RRPWG and RRPSG representatives contributed to the development of this Code of Practice: Train Operators (passenger & freight), infrastructure manager (Network Rail), TfL, TfW, Transport Scotland, BTP, DfT, ORR & GBRTT.

Contents

Abbreviations

Key acronyms applicable to this Approved Code of Practice and Guidance Note are as follows:

Acronym	Full Form
AAP	Anticipate, Assess, Prevent
ACOP(s)	Approved Code(s) of Practice
BAU	Business-as-Usual
BC	Business Continuity
BCI	The Business Continuity Institute
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BT	British Telecom
BTP	British Transport Police
CBRN	Chemical, biological, radiological, or nuclear
CCA	Civil Contingencies Act 2004
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
COBR	Cabinet Office Briefing Room
CoP(s)	Code(s) of Practice
COP	Common Operating Picture
CRIP	Common Recognised Information Picture
DfT	Department for Transport
EA	Environment Agency
ECHR	European Convention of Human Rights
EM	Emergency Management
EPC	Emergency Planning College
ESICTRL	Emergency Services Inter Control
FCO	Foreign & Commonwealth Office
FOC	Freight Operating Company
GBRTT	Great British Railways Transition Team
GDPR	General Data Protection Regulation
GN(s)	Guidance Note(s)
HADDR	Holding and Audit Area for Deceased People and Human Remains
HAT	Health Advisory Team
HVAC	Heating, Ventilation, Air Conditioning
IDS	Intruder Detection System
IEM	Integrated Emergency Management
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardisation
JDM	Joint Decision Model
JESIP	Joint Emergency Services Interoperability Principles
LGD	Lead Government Department
LoA	Lines of Assurance
LRAG	Local Risk Assessment Guidance

LRF	Local Resilience Forum
LRP	Local Resilience Partnership
MCA	Maritime and Coastguard Agency
MHSWR	Management of Health and Safety at Work Regulations 1999
NHS	National Health Service
NPSA	National Protective Security Authority
NRSP	National Rail Security Programme
NSC	National Security Council
ORR	Office of Rail and Road
PSTN	Public Switched Telephone Network
RAIB	Rail Accident Investigation Branch
RAIRR	Rail (Accident Investigation and Reporting) Regulations 2005
RCG	Recovery Co-ordinating Group
RDG	Rail Delivery Group
ResCG	Response Co-ordinating Group
RM^3	Risk Management Maturity Model
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RRP	Rail Resilience Project
RRPSG	Rail Resilience Project Steering Group
RRPWG	Rail Resilience Project Working Group
RVP	Rendezvous Point
SAGE	Scientific Advisory Group for Emergencies
SCC	Strategic Co-ordination Centre
SCCM	Supply Chain Continuity Management
SCG	Strategic Co-ordinating Group
SCR	Security Control Room
SIDOS	Security In the Design of Stations
SITREP	Situation Report
STAC	Science and Technical Advice Cell
TfW	Transport for Wales
THRC	Threats, Hazards, Resilience and Contingencies
TOC	Train Operating Company
TOLO	Train Operator Liaison Officers
TSG	Telecommunications Sub Group
VSS	Video Surveillance System
WAN	Wide Area Network
WRCCA	Weather resilience and climate change adaptation

Definitions

Key definitions used in the text are described in the table below (listed in alphabetical order). Readers are also directed to the list of definitions contained in the RDG Legal and Regulatory Register and accompanying Guidance Note (GN). Readers are referred to the UK Civil Protection Lexicon [LEXICON_v2_1_1-Feb-2013.xls (live.com)] for a full glossary of definitions used in the context of UK Emergency Management and Resilience.

For consistency, definitions remain the same across the ACOPs for IEM. Definitions have been removed where not referenced in this ACOP and new definitions have been added where referenced in this ACOP.

Term	Definition in the context of this document
Aide-Mémoire	Any tool intended as a prompt or checklist of key principles, objectives, and priorities. *(RDG-OPS-GN-014 Major Incidents – Preparation of Aide-Mémoires for Senior Managers)*
Assurance	Assurance provides certainty through evidence and brings confidence that systems are working. With assurance, triangulated evidence is provided to demonstrate that what needs to happen is happening. Evidence is seen in practice or reliable sources of information are received and reviewed. Organisations often have evidence of historic progress in the area in question and outcomes that confirm this. *Source: Governance 101: assurance and reassurance* Assurance and compliance activity related to IEM are addressed by the Three Line of Assurance (3LoA) model. The definition of this model can be found in RDG ACOP: Part A – Governance.
Business Continuity	Capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. *(ISO22301:2019 Security and resilience – Business continuity management systems – requirements).*
Business Continuity Management System	A Business Continuity Management System (BCMS) identifies organisational continuity requirements and implements recovery strategies. It also supports the design and implementation of plans and procedures used by professionals to protect and continue the value-creating operations of an organisation during a disruption. *(BCI Good Practice Guidelines 2023).*
Category 1 and 2 Responders	The Civil Contingencies Act divides those with duties for emergency preparation and response at the local level into two groups (Category 1 and Category 2 responders), each with different duties. Category 1 responders are those at the core of most emergencies and include: the emergency services, local authorities, some NHS bodies. Category 2 responders are organisations less likely to be at the heart of emergency planning but who are required to co-operate and share information with other responders to ensure that they are well integrated within wider emergency planning frameworks. They will also be heavily involved in incidents affecting their sector. Category 2 organisations include: the Health and Safety Executive, Highways Agency, transport, utility companies and the EA. *Part 3 of the Civil Contingencies Act 2004 comprises a list of the Category 2 Responders: General and includes the following within the sub-section on transport:* *A person who holds a licence under section 8 of the Railways Act 1993 (c.*

	43) (operation of railway assets) in so far as the licence relates to activity in Great Britain. *A person who provides services in connection with railways in Great Britain and who holds—* *(a) a railway undertaking licence granted pursuant to the Railway (Licensing of Railway Undertakings) Regulations 2005; or* *(b) a relevant European licence, within the meaning of section 6(2) of the Railways Act 1993.* *(Civil Contingencies Act 2004, RDG Rail Emergency Management: Legal and Regulatory Register).*
Civil Contingencies Act (CCA) 2004	The Civil Contingencies Act 2004 is an Act of the Parliament of the United Kingdom that makes provision about civil contingencies. The Civil Contingencies Act, and accompanying non-legislative measures, delivers a single framework for civil protection in the UK. The Act is separated into 2 substantive parts: local arrangements for civil protection (Part 1); and emergency powers (Part 2).
Crisis	An event or series of events that represents a critical threat to the health, safety, security, or well-being of a community or other large group of people usually over a wider area. *(UK Resilience Framework: December 2022).* An abnormal or extraordinary event or situation that threatens an organisation or community and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity. *(ISO 22361:2022 Crisis Management)*
Crisis Communications	Communications both internal and external to provide information, updates, and instructions to internal and external interested parties. *(ISO 22361:2022 Crisis Management)*
Crisis Management	Coordinated activities to lead, direct and control an organisation with regard to crisis. *(ISO 22361:2022 Crisis Management)*
Critical Incident	A Critical Incident is defined for the purpose of this ACOP as “any incident that has the capability to cause sustained, widespread disruption to the national network, requiring a response beyond the scope of business-as-usual operations, and is likely to involve serious harm, damage, disruption or risk to essential services, the environment, reputational risk to the railway”. It could include, but is not limited to: • An event that completely blocks a line of route in both directions and requires a response from railway partners such as a person struck by train. • The overturning or collapse of any crane, collapse of a high scaffold, collapse of a bridge or tunnel, major failure of a structure which occurs on, or blocks, the railway. • Any incident of a runaway train, vehicle, engineers' trolley, or on-track machinery. • Any other event as determined by industry partners Command Structure. When an incident is considered critical, the same protocols will be applied as with a Major Incident, following the same communication guidelines and command structure. A critical incident is less likely to involve wider agencies such as emergency services and LRFs, however, should it require this response, then the incident should be reviewed, and consideration given to the stepping-up to a Major Incident. *(RDG-OPS-GN-063 RDG Guidance Note: Critical Incident Management, Issue 1 – January 2023, updated following lessons learnt from incidents during 2023 and*

	the development of a new major incident protocol)
Data controller	A 'data controller' is a person who determines the purposes for which, and manner in which, personal data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons. *(Data Protection Act 2018)*
Emergency	An event or situation which threatens serious damage to human welfare, or to the environment; or war, or terrorism, which threatens serious damage to security. *(UK Resilience Framework: December 2022).* **For the purposes of this document the term Emergency has been used in relation to an emergency, business continuity event or similar event that triggers the activation of emergency, business continuity or contingency arrangements.**
Exercise	A simulation designed to validate organisations' capability to manage incidents and emergencies. Specifically, exercises will seek to validate training undertaken and the procedures and systems within emergency or business continuity plans.
Governance	Human-based system by which an organisation is directed, overseen, and held accountable for achieving its defined purpose. *(ISO 37000:2021 Governance of Organisations – Guidance).*
Hazard	Hazards are non-malicious risks such as extreme weather events, accidents, or the natural outbreak of disease. *(UK Resilience Framework, December 2022).*
Incident	An event or situation that can be, or could lead to, a disruption, loss, emergency, or crisis. *(ISO 22361:2022 Crisis Management)*
Integrated Emergency Management	Integrated Emergency Management (IEM) is the framework adopted by UK government and Devolved Administrations for anticipating, preparing for, responding to, and recovering from emergencies or disruptive events. 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. It involves Category 1 and Category 2 responders (as defined in the Civil Contingencies Act 2004) and also the voluntary sector, commerce, and a wide range of communities. *(Preparing Scotland – Scottish Guidance on Resilience Chapter 3).*
Interoperability	Interoperability in integrated emergency management is the extent to which organisations can work together coherently as a matter of routine. Interoperability allows emergency responders to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real-time, when needed, and when authorised. *(JESIP Joint Doctrine: jesip.org.uk).*
Issue	A change in environment, product, system, process, or control which presents new/change in exposures and requires action to forestall the cause or potential causes of one or more incidents.
Joint Decision Model (JDM)	The Joint Decision Model (JDM) is a common model used nationally to enable commanders to make effective decisions together in a multi-agency working environment. It is part of the Joint Emergency Services Interoperability Principles (JESIP), which aim to ensure the emergency responders are trained

	and exercised to work together as effectively as possible. The JDM centres around three primary considerations: Working together, saving lives, and reducing harm. The JDM guides commanders through the steps of an emergency situation and helps bring together available information, reconcile objectives, and make effective collaborative decisions. *(JESIP The Joint Decision Model (JDM)).*
Joint Emergency Services Interoperability Principles (JESIP)	JESIP (Joint Emergency Services Interoperability Principles) aims to improve and standardise the way the police, fire and rescue and ambulance services work together when responding to major multi-agency incidents. To achieve the overarching aim of 'working together, saving lives, reducing harm', JESIP models and principles have become the standard for interoperability across the responder agencies in the UK. JESIP is the thread that should run through all plans and subsequent incidents, and recovery from these. All incident phases need to consider multi-agency working, best served by following the JESIP principles. The JESIP *Joint Doctrine: the interoperability framework* sets out a standard approach to multi-agency working, along with training and awareness products for responding organisations to train their staff. Whilst the initial focus was on improving the response to major incidents, JESIP is scalable, so much so, the principles for joint working and models can be applied to any type of multi-agency incident.
Major Disruption **(BLACK)**	**BLACK – "We are experiencing major disruption to our service, which is severely affecting our ability to provide a rail service".** A major route disruption might include: • A complete route closure. • Weather related disruption. • A prolonged incident which will significantly affect the route for 12 to 24 hours, causing multiple cancellations and alterations to the service.
Major Incident	"An event or situation with a range of serious consequences which requires special arrangements to be implemented by one or more emergency responder agencies." Note: "Emergency responder agency" describes all Category 1 and 2 responders as defined in the Civil Contingencies Act (2004) and associated guidance. *(JESIP Website, Joint Doctrine, Definitions)* A Major Incident on the rail network could include, but is not limited to: • An incident with multiple stranded trains requiring multiple responding agencies to support evacuation plans, • Any accident (derailment, collision, fire etc.) to a passenger train where fatalities or serious injuries occur. • Any serious accident to a train (e.g., high-speed derailment or head-on collision) even if there are no casualties. • Any accident involving the release or combustion of dangerous goods from a train which necessitates the evacuation of railway personnel or the public from the area affected. • Any dangerous occurrence involving a freight train carrying radioactive materials. • Any fatal accident or serious injury (life threatening) to a rail employee on duty.

	• An environmental event as defined in the Network Rail National Emergency Plan. • Any other event as determined by industry partners Command Structure. *(RDG-OPS-GN-063 RDG Guidance Note: Critical Incident Management, Issue 1 – January 2023)*
Major Passenger Rail Incident	A serious rail accident or incident, whatever the cause (including terrorism), which is beyond the capacity of normal customer service arrangements to provide adequate response to, and which therefore requires mobilisation of additional support and organisational resources. It should be recognised that this definition applies within the rail industry and therefore the detail of the incident should be communicated fully to outside parties. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident)*
Organisation	Person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives. The concept of organisation includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part of combination thereof, whether incorporated or not, public, or private. *(ISO 22361:2022 Crisis Management)*
ORR RM^3 Model	The ORR's RM^3 (Risk Management Maturity Model), is a tool for assessing an organisation's ability to successfully manage risks, to help identify areas for improvement and provide a benchmark for year-on-year comparison. The RM^3 model is well understood and used across the rail industry.
Primary Support Operator	The railway undertaking which has been agreed as the best placed (geographically) to provide initial assistance to the Owning Operator in meeting the latter's responsibilities for providing the humanitarian assistance response following a major passenger rail incident. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident)*
Provision	A specific statement or condition within an agreement or a law that a particular thing must happen or be done.
Rail Entity	A passenger train or freight operating company running passenger or freight trains on mainline GB rail infrastructure, or an infrastructure owner or manager of that infrastructure. *(RDG Guidance Note: Emergency Management Legal & Regulatory Register RDG-OPS-GN-064).*
Rail Incident Commander (RIC)	A Rail Incident Commander (RIC) may additionally be appointed by Network Rail when either a major incident is declared or it is considered that the scale of the incident warrants a strategic level of command. If appointed, the RIC has overall responsibility for management of the incident. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Response Following A Major Passenger Rail Incident)*
Rail Incident Officer (RIO)	The Rail Incident Officer - the nominated and certificated person charged with the role of on-site command and control of all rail-related organisations and their support for an emergency involving train operations, lines, or sidings. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident)*
Resilience	There are several definitions of resilience; the following are commonly used within the industry: The UK's ability to anticipate, assess, prevent, mitigate, respond to, and recover from natural hazards, deliberate attacks, geopolitical instability, disease outbreaks, and other disruptive events, civil emergencies, or threats to our way of

	life. *(UK Resilience Framework: December 2022).* Ability to absorb and adapt in a changing environment. *(ISO 22371:2022 Security and Resilience – Community and Resilience – Principles and framework for urban resilience).* **The following definition is to be taken as best practice for the context of this ACOP:** **The Railway Industry's ability to anticipate, assess, prevent, mitigate, respond to, recover from, and learn from natural hazards, deliberate attacks, geopolitical instability, disease outbreaks, and other disruptive events, civil emergencies, or threats to the Rail Network and its associated assets.**
Response	Response encompasses the decisions and actions taken to deal with the immediate effects of an emergency. It is the decisions and actions taken in accordance with the strategic, tactical, and operational objectives defined by emergency responders. At a high level these will be to protect life, contain and mitigate the impacts of the emergency and create the conditions for a return to normality. In many scenarios it is likely to be relatively short and to last for a matter of hours or days – rapid implementation of arrangements for collaboration, co-ordination and communication are, therefore, vital. Response encompasses the effort to deal not only with the direct effects of the emergency itself (e.g., fighting fires, rescuing individuals) but also the indirect effects (e.g., disruption, media interest). *(Emergency Response and Recovery non-statutory guidance accompanying the Civil Contingencies Act 2004)*
Risk	An event, person or object which could cause loss of life or injury, damage to infrastructure, social and economic disruption, or environment degradation. The severity of a risk is assessed as a combination of its potential impact and its likelihood. The Government subdivides risks into: hazards and threats. *(UK Resilience Framework: December 2022).* The effect of uncertainty on objectives. *(ISO 31000:2018 Risk management - Guidelines).* **DfT have identified six priority risk areas to the transport network (see Section 3.3.4.1)**
Risk Appetite	The amount of risk an individual, business, organisation or government is willing to tolerate. *(UK Resilience Framework: December 2022).*
Severe Space Weather	Space weather is a collective term used to describe variations in the Sun, solar wind, magnetosphere, ionosphere, and upper atmosphere that can influence the performance of a variety of technologies, and that can also endanger human health and safety. Day-to-day space weather, much like terrestrial weather, most often occurs with no tangible disruptive impacts. The UK Severe Space Weather Preparedness Strategy is focused on the rare events that could have a significant impact on infrastructure or vital services. The strategy directly supports the aims of the 2021 Integrated Review of Security, Defence, Development and Foreign Policy by seeking to build resilience to the risk of severe space weather, whilst also making science and technology integral to addressing this risk. *(Department for Business, Energy & Industrial Strategy: UK Severe Space Weather Preparedness Strategy, September 2021)*

Significant Disruption **(RED)**	RED – "We are experiencing significant disruption to our service" for example, "damage to overhead electric wires" or "a person hit by a train". Significant disruption might include: • A partial route closure. • An incident causing or likely to cause multiple delays of at least 60 minutes. • Disruption is estimated to last for 2 hours or more. • There are 4 or more consecutive services cancellations and/or terminations. • Service diversions are implemented.
Stakeholder	Person or organisation that can affect, or be affected by, or perceive itself to be affected by a decision or activity. *(ISO 37000:2021 Governance of Organisations – Guidance).*
Station Incident Officer	The nominated and certified person charged with the role of on-site command and control of all rail related organisations and their support for an emergency involving a station. Appointed by the Station Facility Owner – which may be either Network Rail or a railway undertaking – to take responsibility for managing the operation of a station in the event of an incident at that station. The Station Incident Officer will call together representatives of all rail related organisations at the station and provide accommodation, facilities and staff as agreed to operate this Code. In some circumstances the RIO may assume this role. For an incident that affects both the route and a station, the RIO assumes command of the incident and the SIO reports to that RIO. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident)*
Survivor	All those directly involved in a Major Passenger Rail Incident along with their friends / family and those bereaved. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Response Following A Major Passenger Rail Incident)*
Threat	Malicious risks such as acts of terrorism, hostile state activity and cybercrime. *(UK Resilience Framework: December 2022).*
Train Operator Liaison Officer (TOLO)	Person appointed by a railway undertaking as the lead representative of all those railway undertakings affected by the incident. The TOLO will report to and liaise with the RIO on-site (and could act as RIO until such time as a Network Rail appointed RIO is available), or to the Station Incident Officer for station related incidents. *(RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident)*

1 Introduction

1.1 Purpose

This RDG ACOP and supporting GNs contribute to a growing body of Rail Emergency Management Codes of Practice (CoPs) that seek to address the full IEM cycle.

Building on previous documents, this ACOP sets out requirements and provisions that focus on response in the context of IEM within the rail industry.

To support the provisions, accompanying guidance is provided to give users a reference for best practice and/or examples for the associated response elements for IEM. It is hoped that the GNs will provide practitioners, organisations, and Rail Entities the support needed to implement those requirements set out within the provisions in a manner that is representative of, and commensurate to, the operations of their Rail Entity.

This ACOP aims to facilitate a resilience culture, raising awareness of the IEM response elements, encouraging buy-in, and ensuring both the required competencies and appropriate training / learning opportunities are provided.

1.2 Audience

This document is intended to be used by those who are responsible for their Rail Entity's response to emergencies within the rail industry.

This ACOP applies to individual Rail Entities operating in the rail industry and at the pan-industry level (see RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance and RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP)).

This ACOP and accompanying GNs are applicable to all members of RDG who manage infrastructure or operate services over the mainland mainline GB rail network. This includes infrastructure managers, train operating companies and freight operators.

Where a future infrastructure manager or train / freight operator is developing their business, they should consider adopting, or planning to adopt, the IEM ACOP in Rail as part of their process to satisfy licence conditions and to follow industry best practice.

This document will be made publicly available by RDG.

1.3 Background

This ACOP has been formulated in response to the RRP Emergency Management Review: Findings & Recommendations Report (2021). The Review was carried out following several high-profile, weather-related failures in rail industry emergency management. These included:

1. The Carmont derailment, August 2020.
2. The mass self-evacuation outside Lewisham during darkness and poor weather conditions, March 2018.
3. The "Beast from the East" severe winter weather, 2018.

These events took place within periods covered by amber weather warnings and resulted in fatalities, extensive disruption to passengers and significant negative publicity. As a result, the UK Cabinet Office asked the rail industry to carry out a review of its emergency management capabilities.

In early 2021 the RRP Emergency Management Review was set up and carried out by the rail industry under the sponsorship of the RDG. The report was submitted to industry and the Cabinet Office in May 2021 and was formally published in September 2021, following approval by the RDG Board. In November 2021 the RDG Board formally mandated the establishment of a programme of work to deliver against the Review's recommendations.

Rail incidents and emergencies continue to happen, and the lessons learned from these events must contribute to improved rail resilience and incident management across the rail industry.

1.4 Document Orientation: An Integrated Emergency Management (IEM) ACOP

This document**:**

1. Is the **response** section of the Prepare, Respond & Recover ACOPs.
2. Is one in a series of ACOPs for RDG that outline the IEM model for the rail industry (see Figure 1 Document Orientation).
3. Should be read as a part of the collective IEM ACOPs, aligned to the following structure:

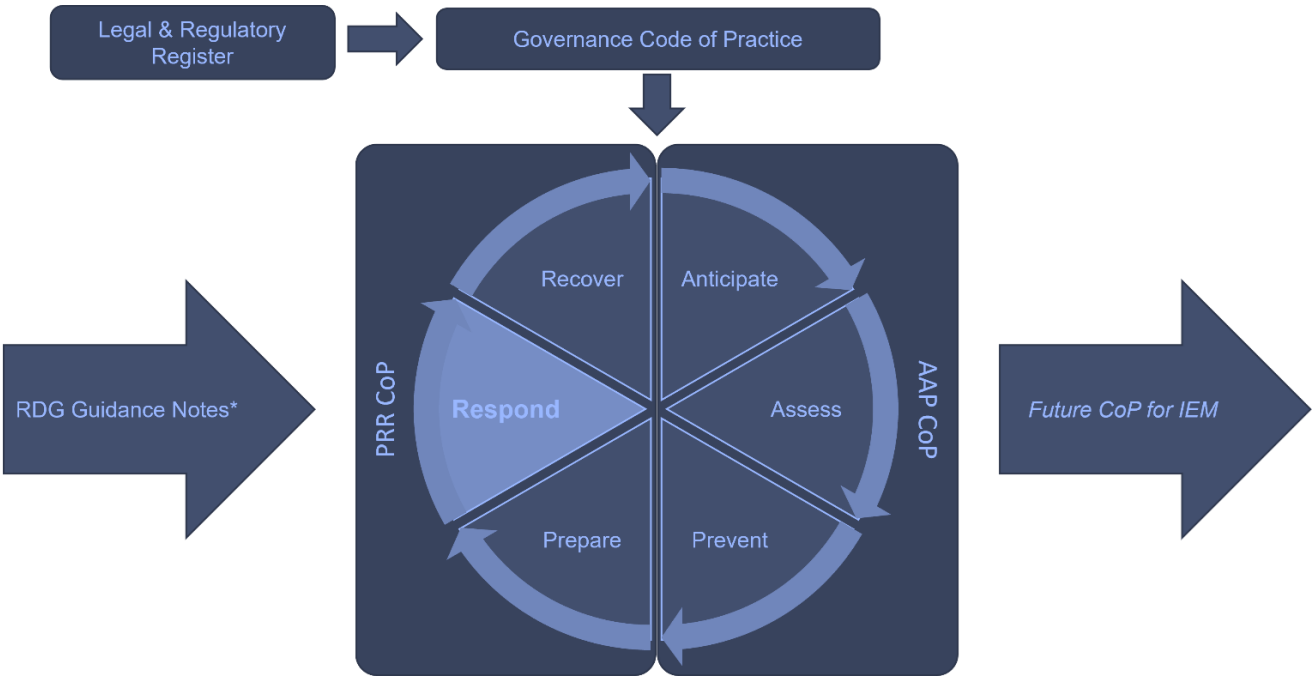

Figure 1 Document orientation

*** Other RDG Guidance Notes used to support IEM CoPs are referenced in Chapter 7 of this document.**

For the purposes of document continuity and best practice referencing, elements of this ACOP are sourced from RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance and RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP).

1.5 Document Structure

This ACOP is broken down into the following chapters. Chapters 3-6 provide the body of the ACOP:

Chapter 1 – Introduction
Chapter 2 – The Rail Industry Resilience Landscape & IEM
Chapter 3 – Emergency Response
Chapter 4 – Command & Control
Chapter 5 – Responder Requirements
Chapter 6 – Data Handling
Chapter 7 – References
Chapter 8 – Appendices

The structure of the document has been provided to ensure the content is accessible, implementable, and relevant to members of the RDG. Each chapter hereafter will also include a quick reference acronym section to help navigate the reader through some of the terminology used throughout the document.
Chapters 3-6 are structured as follows:

1. **Overview** – Providing an overview of the chapter content for the reader.
2. **Provisions** – Outlining the 'must', 'should' & 'could' statements related to that chapter (refer to Section 1.6 Reading the 'provision' statements for more detail).
3. **Guidance Notes** – outlining best practice methods for the implementation of the must and should provisions. The GNs impart a set of good practice guidance, developed such that the relevant practitioner(s) can implement the provisions.

The document also includes a section for definitions, references, plus appendices containing relevant case studies to support the reader to achieve their IEM requirements.

1.6 Reading the 'provision' statements

Within each section of the ACOP, there are provisions made. Provision statements are conditions, requirements or recommendations imposed by law, regulation, codes of practice, guidance or other documents as set out in Table 1 below. They provide a clear structure for Rail Entities to follow to implement both legal requirements, industry best practice, and to support improvements in cross-organisational resilience capability.

The provisions have been included across the following categories as a '**must'**, '**should**' or '**could**'. In the context of this ACOP, this means the following:

Term	Definition
Must	A **legal or regulatory requirement**, and what is typically meant by a provision statement. For example, response 'musts' include statements from the Civil Contingencies Act (CCA) 2004 and the Rail (Accident Investigation Reporting) Regulations 2005 (RAIRR). Where a ***MUST*** provision is provided, the legislative reference will be stated. There are must provision statements within the following chapters: Chapter 4 – Command & Control Chapter 5 – Responder Requirements Chapter 6 – Data Handling
Should	This is **good practice** based on various ISO/BS standards, existing industry good practice, examples of good practice from other industries and academic/professional literature. The literature is supplemented by the expertise of experienced IEM practitioners. There are ***SHOULD*** provision statements within the following chapters: Chapter 3 – Emergency Response Chapter 4 – Command & Control Chapter 5 – Responder Requirements Chapter 6 – Data Handling
Could	This is **leading practice** drawing on the same sources as above**.** It is aspirational depending on a Rail Entity's current and desired maturity and it defines what could be done to achieve excellence. The Capability Maturity Model referenced from RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance is also referenced within this ACOP (see Appendix 8.1). There are ***COULD*** provision statements within the following chapters: Chapter 3 – Emergency Response Chapter 4 – Command & Control

Table 1 Definition of provision statements.

All references consulted for this ACOP are listed in Chapter 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document.

The ORR Enforcement Management Model is included below to demonstrate how the provision statements used in these ACOPs can be mapped against enforcement models used by regulators, noting that not all

legislative elements are enforceable in this manner (for example, the CCA is not enforceable by the ORR). The ORR statements can be cross referenced with the provisions table as follows:

Provision Term	ORR Descriptor	ORR Definition
Must	**Defined**	The minimum standard specified by Acts, Regulations, Orders and ACOPs. For example, the defined standards for welfare; the defined standards for edge protection/scaffold; the defined standard for a train protection system.
Should / Could	**Established**	Codes of Practice and other published standards endorsed by ORR, HSE, industry or other credible organisations that are well known and link to legislation. For example, the HSE's CIS series, including CIS69 for construction dust controls and Network Rail and RSSB standards.
Should / Could	**Interpretive**	Standards that are not published or widely known/available but are those required to meet a general duty. These may be interpreted by inspectors from first principles. For example, how industry dealt with the pandemic and the standards that were quickly formed, but not widely known, around that.

Table 2 Descriptors from ORR Enforcement Management Model, cross referenced with Provisions.

2 The Rail Industry Resilience Landscape

2.1 Resilience in the Transport Sector

The transport sector comprises the road, aviation, rail, and maritime sub-sectors. Most transport operates on a commercial basis, with responsibility for resilience devolved to a mixture of owners and operators.

The Department for Transport (DfT) works closely with stakeholders, including industry, to develop a common assessment of risks and ensures that proportionate and cost-effective mitigations are in place to reduce the likelihood. The department works closely with the British Transport Police (BTP) and the Maritime and Coastguard Agency (MCA) to deliver effective emergency response to, and mitigation against, security and resilience hazards.

However, resilience has not been incorporated across all transport system designs. Resilience within transport system design has historically evolved over time and fails to capture a holistic or whole system approach; IEM will provide better cross mode/sector resilience and give an industry-wide common framework.

2.2 Integrated Emergency Management and Resilience in the Rail Industry

This section is referenced from RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance and is applicable for this RDG ACOP for Response.

IEM is the framework adopted by UK government and Devolved Administrations for anticipating, assessing, preparing for, responding to, and recovering from emergencies:

"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. It involves Category 1 and Category 2 responders (as defined in the Act) and also the voluntary sector, commerce, and a wide range of communities".

Source: Preparing Scotland – Philosophy, Principles, Structures & Regulatory Duties. Chapter 3.

IEM comprises six key activities, namely:

1. **Anticipation**: outward scanning to identify threats, hazards, and opportunities
2. **Assessment**: assessing the likelihood and impacts of those threats, hazards, and opportunities
3. **Prevention**: taking steps to prevent/reduce risks occurring and/or reducing their impact
4. **Preparedness**: preparing Rail Entities to respond to disruptive events through planning, training, and testing and exercising
5. **Response**: being able to deal with disruptive events when they occur
6. **Recovery**: getting back to the new normal and bouncing forward

IEM's key activities operate in a linked framework (see Figure 2 below) with Preparedness at its centre feeding into the **Respond** activity, which makes up the implementation phase, where learning and adaptation also occur, then feeding into the Recover activity and back into Preparedness.

Broadly Anticipation, Assessment and Prevention contribute to enabling Preparedness. Preparedness in turn enables Rail Entities to **respond** effectively and recover quickly. Lessons learned are then fed back into further Preparedness activity.

Given the complexity and levels of resourcing, it may mean that recovery has to be phased but with the guiding principle for a resumption of train services as soon as practically possible, even if that's not back to a full service in just one phase.

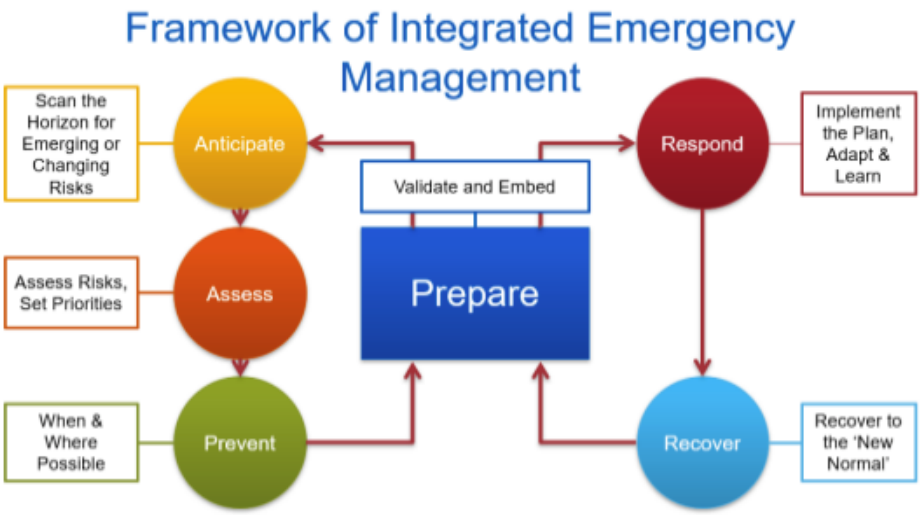

Figure 2 Framework of IEM, sourced from the Emergency Planning College.

As its name suggests, IEM activities need to be integrated throughout individual organisations (Rail Entities), across the wider rail industry and with other civil responders. This requirement for integration applies equally to the other disciplines that collectively contribute to overall resilience.

IEM delivery should not be seen as a separate function within Rail Entities but should be woven through the Business-as-Usual (BAU) activities of the organisation/industry including through the design stages of infrastructure changes/upgrade projects and new systems introduction etc so that resilience continues to be enhanced by design.

RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance adopted six disciplines that comprise the 'Resilience Landscape':

- Enterprise risk management
- Security
- Weather resilience and climate change adaptation (WRCCA)
- Operational resilience
- Business continuity
- IT service continuity

Each discipline that makes up overall resilience has a distinct focus. However, integration and engagement across disciplines is essential to deliver coherent resilience activities.

RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance stresses the importance of inclusive engagement across the resilience disciplines. It is essential to embedding IEM / resilience objectives into overall business strategy and delivery, across all functions and departments.

2.3 Principles

This section is referenced from RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance and is applicable for this RDG ACOP for Response.

Underpinning effective IEM in the rail industry are five principles. These principles guide activity through all five phases of the IEM framework. The principles are key, overarching concepts that are crucial to successful delivery of IEM. More information on the principles can be found in the RDG ACOP: Part A - Governance. The below table identifies each principle with a descriptor:

Principle	Description
Leadership, Competency & Accountability	Leadership at all levels of an organisation is critical to successful IEM. Senior Leaders uphold methods for effective governance that promote clear responsibilities, accountability, unity of vision and transparency. There should be a clear strategy and commitment to IEM and wider resilience activities, ensuring that there are long-term, sustainable financing mechanisms in place to provide ongoing support and direction to resilience activities. This framework should be aligned to the wider business goals and vision of the organisation.
Awareness	Horizon scanning, real-time monitoring and data gathering are core activities to improve awareness, anticipate change and promote risk-informed evidence-based decision making as part of Business-as-Usual (BAU). This horizon scanning needs to be wider than immediate railway issues and consider broader potential risks.
Maturity & Culture	Maturity will vary across each principle and between entities. Using a recognised and understood methodology based on ORR's RM^3, entities should assess their current maturity. They should then identify the steps and timeframes required to achieve their desired maturity level. Measuring the Rail Entity's maturity in resilience is important to help quantifying the benefit in resilience investments. Creating and embedding a culture of resilience will support Rail Entities in empowering ownership for resilience throughout the organisation and developing their maturity. A good resilience culture makes everyone comfortable that it is part of their job description. (See Appendix 8.1 for more details on the Maturity Model).
Inclusive Engagement	Inclusive engagement helps to build consensus, trust, and an integrated approach to resilience across disciplines and organisational boundaries.
Adaptation & Improvement	IEM should be flexible to enable Rail Entities to quickly adapt to an evolving situation and find alternative solutions outside of traditional response structures. Learning together to continually improve and delivering better future outcomes for customers. Bouncing forward following disasters so that organisations can thrive, not just survive.

Table 3 IEM Principles and Definitions

Responding to an emergency encapsulates the resilience principles above. This is further detailed below in Chapter 3.

2.4 Risk Management in relation to Emergency Management

This section is referenced from RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance and RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP) and is applicable for this RDG ACOP for Response.

Rail systems are complex; they have multiple interconnected processes and assets, each with varying lifespans, maintenance, and renewal schedules, and more critically, the systems are exposed uniquely to threats and hazards. Each Rail Entity will have existing risk management capabilities, processes, and structures in place to manage risks affecting their organisation.

The *RDG ACOP for AAP (RDG-OPS-ACOP-009)* relates to risk management and does not seek to establish any kind of separate EM risk management process. Instead, the intention is that EM risks are appropriately considered and addressed within existing structures and that the EM practice (e.g., the work of preparing for, responding to and recovering from emergencies) is driven first and foremost by a good understanding of what types of risk might lead to an emergency, the impacts of those risks manifesting, what is done to limit the likelihood of that risk manifesting and the measures that can be taken (including the relevant plans) to mitigate the consequences should the risk materialise.

The consideration of risks and threats undertaken by rail entities should also include wider resilience risks that have identified by the UK government and included in the National Security and Risk Assessment (NSRA) and the National Risk Assessment (NRR).

3 Emergency Response

3.1 Overview

It is essential for Rail Entities to respond to emergencies, not only to protect their ability to continue to service rail operations across the country, but also from a moral, ethical, and reputational standpoint. Emergency response involves foremost the protection of life, containing and mitigating the impacts of an emergency and the ability to create the conditions for a return to normality, or business as usual (BAU) for the responding entity(ies).

Response encompasses the effort to deal with the direct effects of an emergency itself (e.g., humanitarian aid, rescue work, fighting fires, etc), but also the indirect effects (e.g., media interest, disruption to communications, displaced persons etc.). In many scenarios the response phase is likely to be relatively short, meaning rapid implementation of arrangements for mobilisation, collaboration, coordination, and communication are vital.

The Civil Contingencies Act (CCA) 2004 assigns a duty to warn and inform the public in the event of an emergency, but otherwise response activities do *not* fall as legal duties under the CCA. Nevertheless, effective response, and recovery, are its intended outcomes, with specific requirements outlined for rail in the guidance for a Category 2 Responder (Rail). The CCA should be viewed in the wider context of IEM (see section 2.2), the concept upon which civil protection in the UK is based.

RDG-ACOP-016: Incident Response Duties of Primary Support Operators states that Rail Entities should initiate a response to any incident affecting the railway infrastructure to meet the requirements set out in Railway Group Standards GE/RT8000 and the Rail Industry Standard RIS-3118-TOM, company emergency plans and in support to the infrastructure manager.

In most cases this is likely to be by means of a cascaded management notification process implemented by the relevant operations control using telephone communication (landline and/or mobile) and email.

Rail Entity responses to an incident affecting the railway infrastructure should normally be implemented by the Primary Support Operator for the line of route concerned in agreement with the Owning Operator(s) of any train(s) involved. (*Source: RDG-ACOP-016: Incident Response Duties of Primary Support Operators*).

3.1.1 Emergency Response Principles

Emergency response arrangements should be flexible and tailored to reflect circumstances. Across the UK, a multi-agency response seeks to follow a common set of underpinning principles, as identified in *Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004, October 2013.* These are:

Anticipation
Ongoing risk identification and analysis is essential to the anticipation and management of the direct, indirect, and interdependent consequences of emergencies.

Preparedness
All organisations and individuals that might have a role to play in emergency response and recovery should be properly prepared and clear about their roles and responsibilities, specific and generic plans, and rehearsing response arrangements periodically.

Subsidiarity
Decisions should be taken at the lowest appropriate level, with co-ordination at the highest necessary level. Local agencies are the building blocks of the response to and recovery from an emergency of any scale.

Direction
Clarity of purpose comes from a strategic aim and supporting objectives that are agreed, understood, and sustained by all involved. This will enable the prioritisation and focus of the response and recovery effort.

Information
Information is critical to emergency response and recovery and the collation, assessment, verification, and dissemination of information must be underpinned by appropriate information management systems. These systems need to support single and multi-agency decision making and the external provision of information

that will allow members of the public to make informed decisions to ensure their safety.

Integration
Effective co-ordination should be exercised between and within organisations and levels (i.e., local, and national) to produce a coherent, integrated effort.

Cooperation
Flexibility and effectiveness depend on positive engagement and information sharing between all agencies and at all levels.

Continuity
Emergency response and recovery should be grounded in the existing functions of organisations and familiar ways of working, albeit on a larger scale, to a faster tempo and in more testing circumstances.

Section 3.3.1 provides more detail on these guiding principles for response to emergencies.

3.1.2 Levels of Emergencies

Local responders are the building blocks of the response to any emergency in the UK. Emergencies (or major incidents) are routinely handled by the emergency services and other local responders without the need for any significant central government involvement. Such emergencies may include major incidents on the railway network, localised flooding, and industrial accidents.

To provide guidance to responders on when they might expect central government involvement in responding to an incident, three broad types (or levels) of emergency have been identified by central government which are likely to require direct engagement, in addition to those emergencies described above which are managed locally. These are:

Significant emergency (Level 1) has a wider focus and requires central government involvement or support, primarily from a Lead Government Department (LGD).

Serious emergency (Level 2) is one which has, or threatens, a wide and/or prolonged impact requiring sustained central government co-ordination and support from a number of departments and agencies. This usually includes the regional tier in England and where appropriate, devolved administrations.

Catastrophic emergency (Level 3) is one which has an exceptionally high and potentially widespread impact. It requires immediate central government direction and support, such as a major natural disaster, or a significantly scaled industrial accident.

See Figure 3 in Section 3.3.2, which provides further guidance on levels of emergencies.

3.1.3 Emergency Powers

Part 2 of the Civil Contingencies Act 2004 contains the government's emergency powers legislation. Emergency powers are a last-resort option for responding to the most serious of emergencies where existing legislative provision is insufficient for the situation; they are a mechanism for making temporary legislation to prevent, control or mitigate an aspect or effect of the emergency.

Emergency regulations must be necessary to resolve the emergency and proportionate to the effect or aspect of the emergency they are aimed at. What emergency regulations will contain will depend on the specific requirement arising out of the potential or actual circumstances of the emergency. There must be no expectation from rail entities that government will agree to use emergency powers. All planning and responding arrangements must assume that they will not be used.

See Section 3.3.3 for further guidance relating to Emergency Powers.

3.1.4 A Resilience Framework

His Majesty's (HM) Government Emergency Response and Recovery Non-Statutory Guidance accompanying the Civil Contingencies Act 2004 is an agreed national framework for managing the local multi-agency response to emergencies. The Emergency Response guidance establishes a common framework for England and Wales that is flexible enough to be adapted to local circumstances and specific problems. It is not intended to be prescriptive or an operational manual, as there is no single approach that will meet the needs of every area, nor is there one single set of organisational arrangements that will be appropriate to each and every type

of emergency and its responding requirements. Section 3.3.4 provides further guidance on the framework.

The guidance describes the single-agency and multi-agency management tiers that comprise the local framework; their roles and responsibilities; the interaction between the tiers; and the interaction between individual agencies within the tiers.

There is further detail and specific information on utilising and adapting the guidance in specific circumstances such as terrorist, animal health and maritime incidents, as different arrangements apply, and additional agencies are involved. The response framework within the UK is designed to be both flexible and scalable and is based on the principle of subsidiarity and agencies acting within their own functions.

3.1.5 Response and Business Continuity

Business continuity is the collective term to include response, recovery and resumption of an organisation's activities impacted by an emergency. RDG-OPS-ACOP-010 IEM, Preparation, discusses embedding Business Continuity as a key operational requirement in ensuring Rail Entities are prepared for emergencies and can more rapidly recover in the event of an incident affecting their operations, systems, and locations.

A Business Continuity Management System (BCMS) supports the organisation's strategic objectives and proactively builds the capability to continue business operations during an emergency, including creating Response Structures to be used in the event of an incident. These BC response structures should be aligned to the normal and recognised incident management frameworks within the organisation.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Chapter 7, References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document.

3.2 Provisions

3.2.1 Emergency response and recovery arrangements ***SHOULD*** be flexible, adaptable, and tailored to reflect the circumstances. [1]

3.2.2 Emergency response and recovery arrangements ***SHOULD*** follow a common set of underpinning principles, and these ***SHOULD*** be applied at the local, subnational, and national levels [1]:

- Anticipation
- Preparedness
- Subsidiarity
- Direction
- Information
- Integration
- Co-operation
- Continuity

3.2.3 Rail Entities ***SHOULD*** follow the nationally agreed framework for managing emergency response and recovery to integrate plans and procedures within and between agencies and across geographical boundaries. [1]

3.2.4 Rail Entities' strategic aims ***COULD*** look beyond the immediate demands of the response and ***COULD*** embrace the longer-term priorities of restoring essential services and helping to facilitate the recovery of the affected communities. [1]

3.2.5 Strategic Commanders within responder organisations ***SHOULD*** establish clear aims and objectives for their organisations, to bring direction and coherence to the activities of multiple agencies under circumstances of sustained pressure, complexity and potential hazard and volatility. [1]

3.2.6 Rail Entities ***SHOULD*** establish systematic information management systems and embed them within multi-agency emergency management arrangements. [1]

3.2.7 Rail Entity Emergency Responders ***SHOULD*** include voluntary and private sector organisations in the

multi-agency response and, as such, they ***SHOULD*** be integrated into the information management structures and processes that are established, trained, exercised, and tested. [1]

3.2.8 Rail Entities ***SHOULD*** put in place clearly defined structures to ensure support for key agencies to [1]:

- Combine and act as a coherent multi-agency group.
- Consult, agree, and decide on key issues.
- Issue instructions, policies and guidance to which emergency response partners will conform.

3.2.9 Rail Entities ***SHOULD*** have in place mechanisms to manage emergencies which straddle Local Resilience Areas and regions or affect more than one part of the UK. [1]

3.2.10 Rail Entities ***SHOULD*** understand each other's functions, ways of working, priorities, and constraints. [1]

3.2.11 Rail Entities ***SHOULD*** support and assure openness between agencies by a commitment to the confidentiality of shared information when dealing with third parties and / or the public. [1]

3.2.12 Response and recovery arrangements ***SHOULD*** be reflective of trained and exercised ways of working within the rail industry and across the wider responder community. [1]

3.2.13 Rail Entities' procedures and capabilities ***SHOULD*** be well integrated between agencies and across the rail industry to ensure response and recovery work is effective. [1]

3.2.14 Rail Entities ***SHOULD*** work in a directed and co-ordinated fashion where multi-agency strategic coordinating groups are established. [1]

3.2.15 Rail Entities ***SHOULD*** consider response requirements to concurrent events and the requirements for risk-based prioritisation of emergencies in response arrangements. [2, 3]

3.2.16 Rail Entities ***SHOULD*** use Rail Safety and Standards Board (RSSB) Rule Book Module M1 GERT8000-M1 Issue 7 as a checklist when dealing with a train accident or incident. [12]

3.2.17 Rail entities ***SHOULD*** ensure terminology used during response and recovery is consistent with that used by multi-agency partners, ensuring interoperability, and reducing the risk of miscommunication.

3.2.18 Rail Entities ***SHOULD*** implement and maintain a response structure that will enable timely warning and communication to relevant interested parties. It ***SHOULD*** provide plans and procedures to manage the organisation during an incident. The plans and procedures ***SHOULD*** be used when required to activate business continuity solutions.

3.2.19 Rail Entities ***SHOULD*** implement and maintain a structure, identifying one or more teams responsible for responding to incidents.

3.2.20 The roles and responsibilities of each team and the relationships between the teams ***SHOULD*** be clearly stated.

3.2.21 Collectively, the teams ***SHOULD*** be competent to:

- Assess the nature and extent of an incident and its potential impact.
- Assess the impact against pre-defined thresholds that justify initiation of a formal response.
- Activate an appropriate business continuity response.
- Plan actions that need to be undertaken.
- Establish priorities (using life safety as the first priority).
- Monitor the effects of the incident and the organisation's response.
- Activate the business continuity solutions.
- Communicate with relevant interested parties, authorities, and the media.

3.2.22 For each team there ***SHOULD*** be:

- Identified personnel and their alternates with the necessary responsibility, authority, and competence to perform their designated role.
- Documented procedures to guide their actions, including those for the activation, operation, coordination, and communication of the response.

3.2.23 Rail Entities ***SHOULD*** document and maintain procedures for:

- Communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate.
- Receiving, documenting, and responding to communications from interested parties, including any national or regional risk advisory system or equivalent.
- Ensuring the availability of the means of communication during an incident.
- Facilitating structured communication with emergency responders.
- Providing details of the organisation's media response following an incident, including a communications strategy.
- Recording the details of the incident, the actions taken, and the decisions made.

3.2.24 Rail Entities ***SHOULD*** alert interested parties potentially impacted by an actual or impending incident and ***SHOULD*** ensure appropriate coordination and communication between multiple responding organisations.

3.2.25 Rail Entities ***SHOULD*** exercise their warning and communication procedures as part of their exercise programme.

3.2.26 Rail Entities ***SHOULD*** document and maintain business continuity plans and procedures. The business continuity plans ***SHOULD*** provide guidance and information to assist teams to respond to an incident and to assist the organisation with response and recovery.

3.2.27 Business continuity plans ***SHOULD*** contain:

- Details of the actions that the teams will take in order to continue or recover prioritised activities within the predetermined time frames and, monitor the impact of the disruption and the organisation's response to it.
- Reference to the pre-defined threshold(s) and process for activating the response.
- Procedures to enable the delivery of products and services at agreed capacity.
- Details to manage the immediate consequences of a disruption giving due regard to the welfare if individuals, the prevention of further loss or unavailability of prioritised activities and the impact on the environment.

3.3 Guidance Notes

3.3.1 Emergency Response Principles

What constitutes an appropriate response to and recovery from an incident or emergency will be determined by a range of factors, including but not limited to:

- The nature and demands of the emergency, specifically context, geographical extent, duration, complexity, and potential impacts.
- Local experience.
- The designated lead agency; local circumstances, priorities, and experience.
- Whether or not there is sub-national, national, or international involvement in the response and recovery effort.

There are eight guiding principles that underpin the response to and recovery from every emergency. These principles apply equally to each tier (local, sub-national and national) and are consistent with Central Government Arrangements for Responding to an Emergency: Concept of Operations. In the interests of achieving coherent arrangements for emergency response and recovery, these principles should be applied at the local, sub-national and national levels.

A check-list of considerations for responders for each of these principles can be found in **Part 3 of the Cabinet Office Expectations and Indicators for Good Practice Set for Category 1 and 2 Responders,** Expectation and Indicators of Good Practice Set for Category 1& 2 Responders.pdf (publishing.service.gov.uk).

3.3.1.1 Anticipation

Anticipation is crucial in both the pre-emergency and post-emergency phases. Anticipation is commonly used to describe the first phase of the IEM process, which sees organisations actively horizon-scanning for risks and potential emergencies. Anticipation is also a principle of effective response and recovery, and, at the strategic level, the risk focus must be forwards, upwards and outwards, with more operational risks being appropriately addressed at lower levels. This process should consider a wide spectrum of potential risks.

All emergencies have disparate direct and indirect impacts that may not be immediately apparent amidst the pressure, uncertainties, and demanding circumstances of an emergency. Two factors merit particular consideration in planning: training and exercising.

In emergencies, risk becomes dynamic. New risks emerge, previously recognised risks recede and the balance between risks changes continuously. Active risk assessment and management should be an ongoing process. But this should enable, rather than obstruct, effective operations by providing analysis of, and solutions to, anticipated problems before they arise. Emergencies create business continuity challenges. Demands on staff time, resources and management attention will be significant and maintaining the response and recovery effort alongside an organisation's day-to-day functions will pose a major challenge. The risk of senior management discontinuity during prolonged periods of pressure may not be immediately apparent but can be significant. This can be managed through good organisation; planning and thorough training; and preparation of deputies and second teams at every level.

An important aspect of anticipation is addressing recovery issues at the earliest possible opportunity, ensuring that the response and recovery effort is fully integrated and working to a common understanding. This will ensure that recovery priorities are factored into the initial response and are aligned which will ensure coherence between the two streams of activity. Ideally, the two activities should be taken forward in tandem from the outset, although in some cases constraints on capacity may necessitate a degree of separation, with the recovery effort gathering momentum once the initial risk to life has been addressed.

See RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance and RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP) for further detail on anticipating and risk management guidance in the rail industry.

3.3.1.2 Preparedness

All individuals and organisations that might play a part in the response and recovery effort should be appropriately prepared. This requires a clear understanding of their roles and responsibilities and how they fit into the wider, multi-agency picture. The Civil Contingencies Act 2004 requires those organisations likely to be at the core of an emergency response to work together to ensure that they are prepared for emergencies, as identified through the national to local processes of risk assessment. Emergency Preparedness explains the requirements of the legislation and offers good practice advice to local responders.

See RDG-OPS-ACOP-010 IEM, Preparation for further detail on Preparation for Emergencies in the rail industry.

3.3.1.3 Subsidiarity

The UK's approach to emergency response and recovery is founded on a bottom-up approach in which operations are managed and decisions are made at the lowest appropriate level. In all cases, local agencies are the building blocks of response and recovery operations. The local level deals with most emergencies with little or no input from the sub-national or national levels.

The role of central government and devolved administrations is to support and supplement the efforts of local responders through the provision of resources and co-ordination. The central and sub-national tiers will only become involved in emergency response and recovery efforts where it is necessary or helpful to do so.

That said, given the potential implications to UK Plc, central government may request regular updates through the lead government department (DfT), which is normally facilitated at the national or sub-national level.

3.3.1.4 Direction

When an emergency occurs, those responsible for managing the response and recovery effort will face an array of competing demands and pressures. These will vary according to the event or situation that caused the emergency, the speed of its onset, the geographical area affected, any concurrent or interdependent events, and many other factors. The information available will often be incomplete, inaccurate, or ambiguous, and perceptions of the situation may differ within and / or between organisations. The response and recovery effort may involve many organisations, potentially from across the rail industry, the public, private and voluntary sectors, and each will have its own responsibilities and capabilities requiring co-ordination. Additionally, there may be competing priorities to contend with as the situation evolves and multiple or escalating incidents have subsequent consequences to manage and respond to.

To negotiate these pressures, it is essential to establish and communicate clear and unambiguous strategic aims and objectives. This is often done by the respective Strategic lead Strategic Co-ordinating Group for

multi-agency events and a Strategic Rail Group for rail specific emergencies (single agency). See Section 4.1.2 for more on Strategic Co-ordinating Groups.

Clear strategic aims and objectives between responders helps establish a shared set of priorities and thereby efficiently focus effort and resources where they are most required. The determination of the aims and objectives and their communication and observance are fundamental to the success of the multi-agency effort.

In sudden impact emergencies (e.g., explosions or transport accidents) local responders will immediately strive to save life, alleviate suffering, and contain and mitigate the impacts of the emergency. In most cases, the response phase is relatively short, perhaps only a matter of hours. The strategic aims and objectives should look beyond the immediate demands of the response and embrace the longer-term priorities of restoring essential services and helping to facilitate the recovery of the affected communities.

Common objectives for responders are:

- Saving and protecting human life.
- Relieving suffering.
- Containing the emergency – limiting its escalation, spread and / or mitigating its immediate and subsequent impacts.
- Providing the public and businesses with warnings, advice, and information.
- Protecting the health and safety of responding personnel.
- Safeguarding the environment; as far as reasonably practicable, protecting property.
- Maintaining or restoring critical activities.
- Maintaining normal services at a pre-agreed and appropriate level.
- Promoting and facilitating self-help in affected communities.
- Facilitating investigations and inquiries (e.g., by preserving the scene and effective records management.
- Facilitating the recovery of the community, including the humanitarian, economic, infrastructure and environmental impacts.
- Evaluating the response and recovery effort.
- Identifying and taking action to implement lessons learned / identified.

In slow-onset emergencies (e.g., disruption to the fuel supply or the spread of an infectious disease) where the emergency services may not necessarily lead the response, the strategic aim may be more difficult to identify and formulate. It is equally important to establish clear aims and objectives to bring direction and coherence to the activities of multiple agencies under circumstances of sustained pressure, complexity and potential hazard and volatility.

During the course of a protracted incident or emergency it is useful to undertake reviews of the stated Strategic aims and objectives to confirm they are still valid and identify if additional ones are required etc.

Government may, in certain limited circumstances, assume the role of setting the strategic direction where only it is able to deliver the necessary co-ordination; such was the case during the COVID-19 pandemic where the Department of Health and Social Care took the leading response role, with the Government's chief scientific adviser and chief medical officer leading the Scientific Advisory Group for Emergencies (SAGE) or where wider UK Plc interests may conflict with normal operational priorities e.g. prioritising critical freight movements.

Source: Emergency Response and Recovery Non statutory guidance accompanying the CCA 2004 (October 2013).

3.3.1.5 Information

Information is critical to emergency response and recovery, yet maintaining the flow of information, within agencies, with external partners, and to the wider public, is extremely challenging under emergency conditions. The importance of information to emergency responders and those affected by events must not be underestimated.

Effective information management is dependent upon appropriate preparation measures being in place to build situational awareness and the development of a Common Recognised Information Picture (CRIP) (otherwise known as Common Operating Picture (COP)) at the local, sub-national and national levels (if appropriate). Such measures will need to support:

- The transmission and collation of potentially high volumes of information from multiple sources.

- The assessment of collated information to ensure its relevance, accuracy, timeliness, accessibility, interpretability, and transparency.
- The translation of available information into appropriate information products, for example, briefing the Strategic Co-ordinating Group / strategic groups or national groups, or release to the media for public information.

Challenges that may need to be addressed to realise the collation, assessment, validation, and dissemination of information under emergency conditions include but are not limited to:

- Information management procedures may vary between agencies.
- Perspectives on the event or situation may differ, and the management of risk may vary in response requirements.
- Key information may not be shared in a manner that is easily understood, or that could be open to interpretation.
- Mistakes and misunderstandings may occur under pressure.
- Communications can become overloaded.

Balance is required to ensure decisions are well informed, appropriately acted upon and implemented swiftly and decisively. Establishing systematic information management systems and embedding them within multi-agency emergency management arrangements will enable the right balance to be struck.

It is important to note that voluntary and private sector organisations will typically need to be included in the multi-agency response and, as such, they must be integrated into the information management structures and processes that are established, trained, exercised, and tested and interdependencies are better understood.

In particular, the sharing of information in a way that is responsive to the needs of emergency responders, and is compliant with data protection and other legislation, needs to be thoroughly understood and tested.

In establishing information management systems and processes responders should bear in mind the following guidance: **Data Protection and Sharing – Guidance for Emergency Planners and Responders** Data protection and sharing guidance for emergency planners and responders - GOV.UK (www.gov.uk) and the RDG Data Sharing guidance. Further detail on handling data and information as part of an emergency response is also contained within Chapter 6 - Data handling.

Information Language
Parochial usage of terms may interfere with interoperability and co-operation with local partners and neighbouring areas and hinder co-ordination at the sub-national and national levels.

The same applies to concepts of operation, doctrine, and structures. A lexicon of terminology for multi-agency, local strategic operations is maintained by the Civil Contingencies Secretariat and published at https://www.gov.uk/government/publications/emergency-responder-interoperability-lexicon.

Document glossaries, whether national, regional, or local, must be terminologically faithful to this lexicon.

Information to Media and Public
Any emergency will result in widespread media interest and public concern. It is, therefore, essential that structures and processes exist to manage the demands of the media and to ensure that messages given out are consistent. It is similarly essential that the public receives appropriate advice, warnings, and information to provide reassurance and a basis for any necessary action.

3.3.1.6 Integration
Responding to, and recovering from, emergencies is a multi-agency activity that may involve many organisations. Their involvement, role and relative prominence may change between phases of the emergency. Depending on the nature and severity of the event or situation, there may also be involvement from sub-national and national levels. It is crucial that the contributions of respective organisations are integrated.

The range of organisations involved in emergency response and recovery can pose difficulties for the effective management of local operations, and this underlines the importance of putting in place clearly defined structures to ensure that key agencies can:

- Combine and act as a coherent multi-agency group.
- Consult, agree and decide on key issues.

- Issue instructions, policies and guidance to which emergency response partners will conform.

This will only be achieved if structures and processes are formulated through careful planning and embedded through operations and regular training and exercising (see RDG-OPS-ACOP-010 IEM, Preparation).

Some emergencies may affect large areas, and some may have national or even international implications (e.g., maritime pollution or atmospheric radiological pollution). It is important that mechanisms are in place to manage emergencies which straddle Local Resilience Areas and regions that affect more than one part of the UK (i.e., England, Wales, Scotland, or Northern Ireland)

3.3.1.7 Co-operation

Emergency response and recovery is a multi-agency activity. The management of emergencies brings together a wide range of organisations which are not bound by hierarchical relationships. Although one agency may take the lead in relation to an emergency, phase or aspect of that emergency, decision-making processes should always aim to be inclusive and, wherever possible, arrive at consensual decisions.

Mutual trust and understanding are the building blocks of effective multi-agency operations. Organisations must understand each other's functions, ways of working, priorities, and constraints. This will facilitate the open dialogue that is essential for common aims and objectives to be developed, agreed, and worked towards. Furthermore, openness between agencies must be supported and assured by a commitment to the confidentiality of shared information when dealing with third parties or the public at large.

Unauthorised disclosure of information or unilateral action will not only prejudice cohesion but may also undermine operational effectiveness.

3.3.1.8 Continuity

Emergency response and recovery arrangements in the UK are founded on the premise that those organisations undertaking functions on a day-to-day basis are best placed to exercise them in the demanding circumstances of an emergency. The experience, expertise, resources, and relationships they have established will be crucial, even though they may be deployed in a different way or supported by neighbouring areas. For this reason, the CCA imposes a duty on those organisations to plan for emergencies in respect of their everyday role.

Effective response and recovery will be grounded in tried and tested arrangements built on everyday working practices. Wherever possible, response and recovery arrangements should preserve established structures and ways of doing things that people know well. By their very nature, emergencies require the special deployment of staff and resources. Wherever roles, responsibilities and organisational arrangements are different in emergency mode, these should be embedded through training and exercising.

3.3.2 Levels of Emergencies

Typically, the police lead in coordinating the local response to a multi-agency major incident, where a crime has been committed, or if there is a threat to public safety. The local multi-agency response is coordinated through a Strategic Co-ordinating Group (SCG) located in the Strategic Co-ordination Centre (SCC).

The chair of the SCG, regardless of lead agency, is known as the Strategic Coordinating Group Chair. This may colloquially be referred to by some responders as a 'Gold Commander', however this practice stems from the Police Gold Commander often simultaneously holding the role of SCG chair and single agency commander. In the role of SCG chair they are exercising a co-ordination function, not a command function.

More information on the structure and organisation of the local response can be found in Chapter 4 Command and Control.

The principle of subsidiarity emphasises the importance of local decision making supported, where necessary, by co-ordination at a higher level. To aid planning, further understanding, and provide guidance to responders and central government planners on when they might expect central government involvement in responding to an incident, three broad types (or levels) of emergency have been identified (Figure 3) which are likely to require direct central government engagement in addition to those emergencies which are solely managed locally. These are:

Significant emergency (Level 1) has a wider focus and requires central government involvement or support, primarily from a lead government department (LGD) or a devolved administration, alongside the work of the emergency services, local authorities, and other organisations. There is however no actual or potential

requirement for fast, inter-departmental/agency, decision making which might necessitate the activation of the collective central government response, although in a few cases there may be value in using the Cabinet Office Briefing Room (COBR) complex to facilitate the briefing of senior officials and ministers on the emergency and its management.

Examples of emergencies on this scale include most severe weather-related problems. In addition, most consular emergencies overseas fall into this category with the Foreign & Commonwealth Office (FCO) providing advice and support to those affected alongside the authorities in the country affected.

Serious emergency (Level 2) is one which has, or threatens, a wide and/or prolonged impact requiring sustained central government co-ordination and support from a number of departments and agencies, usually including the regional tier in England and where appropriate, the devolved administrations.

The central government response to such an emergency would be co-ordinated COBR, under the leadership of the lead government department. Examples of an emergency at this level could be a terrorist attack, widespread urban flooding, widespread and prolonged loss of essential services, a serious outbreak of animal disease, or a major emergency overseas with a significant effect on UK nationals or interests.
Examples of emergencies on this scale, include the H1N1 Swine Flu pandemic, the 2007 summer floods, and the response to the 7th of July bombings in London.

Catastrophic emergency (Level 3) is one which has an exceptionally high and potentially widespread impact and requires immediate central government direction and support, such as a major natural disaster, or a Chernobyl-scale industrial accident. Characteristics might include a top-down response in circumstances where the local response had been overwhelmed, or the use of emergency powers were required to direct the response or requisition assets and resources. The Prime Minister would lead the national response.

As noted above, most incidents are managed at the local level, with little or no involvement from central government nationally. However, the increasingly complex and inter-dependent nature of society means that there are sometimes significant knock-on consequences even from apparently straightforward events necessitating central government engagement. This could include, for example, providing guidance, coordination, people, expertise, specialised equipment, advice, or financial support. These decisions will be taken on a case-by-case basis depending on the nature of the emergency and its impact. In practice, the level of central government engagement may change over time (both up and down) as the demands of the emergency change.

For example, an emerging incident may escalate through each of these stages as understanding of its impact and public interest grows, requiring visible coordinated action at a Government level or resources beyond the capability of local responders.

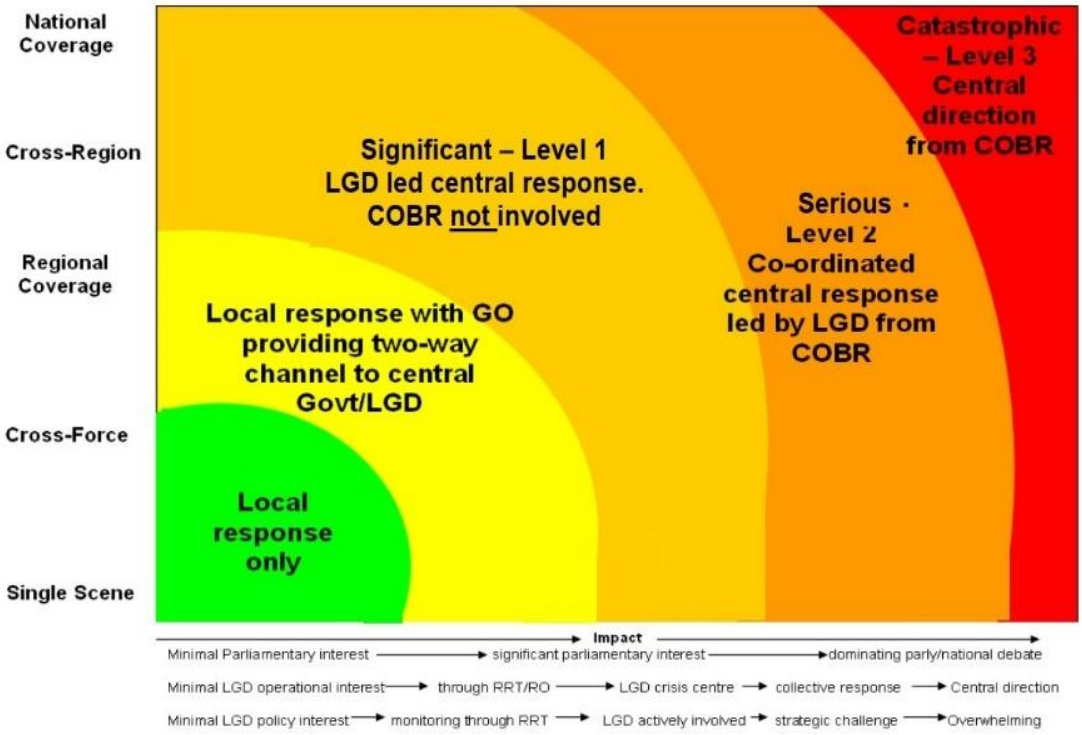

Figure 3 Likely form of central government engagement based on the impact and geographic spread of an emergency in England (Source: Central Government Arrangements for Responding to an Emergency: Concept of Operations (CONOPS) (2013)).

3.3.3 Emergency Powers

Planning and response arrangements must assume that emergency powers will not be used.
Emergency powers are provisions for specific reserve or emergency powers contained within certain primary legislation, such as the Energy Act 1976 which allows the regulation or prohibition of the production, supply, acquisition, or use of fuel during an emergency affecting fuel supplies.

Under Part 2 of the CCA, there are wider powers which the Government can draw on to make special temporary legislation (emergency regulations) as a last resort in the most serious of emergencies where existing legislation is insufficient to respond in the most effective way. Emergency regulations may make provision of any kind that could be made by an Act of Parliament or by exercise of the Royal Prerogative, so long as such action is needed urgently and is both necessary and proportionate in the circumstances.

The regulations may extend to the whole of the UK, one or more area of England, and / or one or more of the devolved administrations. In England, 'Nominated Co-ordinators' will be appointed to facilitate the co-ordination of activities under the emergency regulations. In devolved administrations, they will be known as 'Emergency Co-ordinators'.

Emergency powers allow the Government to respond quickly in emergency situations where new powers or amendments to existing powers are needed and there is not time to legislate in the usual way in advance of acting. They ensure the Government can act legally and accountably in situations where temporary new legal provision is required without the time for Parliament to provide it beforehand.

Emergency powers legislation is not a panacea for difficulties faced in responding to or recovering from emergencies. It is a legislative mechanism for making temporary changes to the law within clearly defined limits.

The decision to use emergency powers, or not, and the content of emergency regulations, are matters for central government and will be handled by the relevant Lead Government Department (LGD) in collaboration with other government departments. It is subject to collective agreement. In considering the options, the government will have to satisfy itself that conditions within the Act are met.

Foremost, the government has to be satisfied that the conditions which define an emergency are met. The Act

states that emergency powers can only be used if an event or situation threatens one or more of the following:

- Serious damage to human welfare in the UK, a devolved territory or region.
- Serious damage to the environment of the UK, a devolved territory or region.
- The security of the UK, from war or terrorism.

An emergency within the definition given above must have occurred, be occurring or about to occur in order to permit consideration of the use of emergency powers. This is, however, only the starting point in the process. For an event or situation to be judged to fall within the definition of emergency does not mean that emergency powers should or could be used. Additional safeguards have been built into the process to ensure that emergency powers can only be considered as an option if: it is necessary to make provision urgently in order to prevent, control or mitigate an aspect or effect of the emergency when existing powers are insufficient and it is not possible to bring forward a Bill in the usual way and there is a need to make the provision by other means; and emergency regulations must be proportionate to the aspect or effect of the emergency they are directed at.

It is not possible to state in advance the exact threshold at which emergency powers may legitimately be considered as this will depend on the unique circumstances prevailing at the time.

Emergency powers are a matter for the UK Government, but arrangements are in place to ensure effective consultation and co-ordination with the devolved administrations. These are set out, in detail, in separate concordats with the Welsh and Scottish administrations.

Source: Emergency Response and Recovery, Non statutory guidance accompanying the Civil Contingencies Act 2004 (October 2013): Chapter 14 — Emergency Powers.

3.3.4 Resilience Framework

The national framework for managing the local multi-agency response to emergencies is detailed within Chapter 4 of Emergency Response and Recovery Non-statutory guidance accompanying the Civil Contingencies Act 2004 (October 2013). The guidance describes the single-agency and multi-agency management tiers that comprise the local framework; their roles and responsibilities; the interaction between the tiers; and the interaction between individual agencies within the tiers.

Command, control, and co-ordination are important concepts in the multi-agency response to emergencies and the framework guidance distinguishes between single agency command and control structures (often termed gold, silver, and bronze) and the multi-agency co-ordination structures that may be convened at strategic, tactical and, exceptionally, at operational levels (Figure 4).

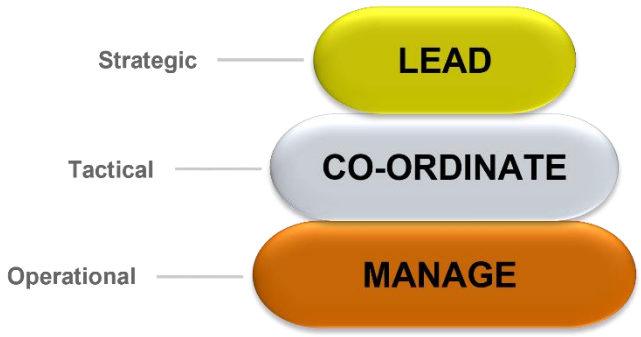

Figure 4 Command and Control Structure

It is a generic framework and the principles and procedures underpinning it are flexible enough to be used to manage a wide range of emergencies. Further guidance is given on the considerations that may apply in relation to:

- Localised emergencies
- Wide-area emergencies
- Terrorist incidents
- Animal health outbreaks
- Maritime emergencies
- Procedures and considerations for the management of evacuations.

Source: Emergency Response and Recovery, Non statutory guidance accompanying the Civil Contingencies Act 2004 (October 2013): Chapter 4 — Responding to Emergencies.

A general distinction is made between localised and wide-area emergencies. Localised emergencies will typically have a clearly identifiable scene such as the location of a signal failure or track debris, partial derailment or, a major Rail incident such as a high-speed collision or system-wide power outage. Wide-area emergencies can be divided into those comprised of incidents at multiple sites that are spread over a wide area, and emergencies where wide areas are affected to some degree.

Within the UK, there is substantial experience of managing emergencies that occur within the bounds of relatively small geographical areas (e.g., explosions or major fires) and have primarily localised effects. It is important to note that localised incidents have the potential for widespread disruption if there are knock-on consequences or interdependent impacts, for example arising from the loss or disruption of a key rail line / network.

To bring order to the response and reduce the potential for confusion, it is important that the emergency services establish control over the immediate area and build up arrangements for co-ordinating individual agencies contributions to the response.

Each agency needs to establish its own control arrangements; continuous liaison between them is essential. Effective response depends on good communication and mutual understanding, which is built up through planning, the development of protocols and joint exercises (see RDG-OPS-ACOP-010 IEM, Preparation). It is generally accepted that the first members of the emergency services to arrive on the scene should make a rapid assessment and report back to their control room. The control room that receives the initial report should, in accordance with established plans, alert the other emergency services and relevant partner agencies. In accordance with their own procedures, those agencies will then alert personnel or activate appropriate response and recovery plans to the level they judge necessary. Further detail on planning for emergencies is contained within RDG-OPS-ACOP-010 IEM, Preparation.

Agreed protocols should be in place to alert any commercial or industrial organisations whose premises, services or personnel could be affected, or required as part of the response and recovery effort. Voluntary sector organisations that may be required to support the response and recovery effort should be informed at the earliest opportunity, in accordance with established plans.

Some functions will by their nature be discharged outside cordons and away from the scene but remain essential components of an integrated response. Similarly, it may be appropriate for emergency services and other organisations to be represented within the local authority’s emergency/crisis management centre, which provides the focus for the management and co-ordination of local authority activities and the recovery effort.

If an incident occurs within the perimeter of an industrial or commercial establishment, public venue such as railway stations, airport, or harbour, it is essential that a site incident officer from the affected organisation establishes liaison with responding organisations. Such a representative can ease access to facilities within the establishment and act as a link between the establishment’s senior management and the emergency management structure.

It is essential that plans and arrangements are in place to deal with emergencies that are not limited to a single, local scene. The framework for managing wide-area emergencies will follow the same generic framework that is applicable to all emergencies, and many of the challenges faced will be similar to emergencies where there is an identifiable scene. It is probable that inter-agency strategic management will be required in such circumstances, leading to the activation of SCGs in all or most affected areas.

In the early stages of the response, information management is likely to represent a significant challenge. Responders may be faced with large quantities of potentially relevant information or very little information, information of uncertain provenance and quality or indicators that are ambiguous or otherwise hard to interpret. In this scenario, multi-agency co-ordinating groups at the strategic and tactical levels will have an especially important role in collating, evaluating, and monitoring situational and contextual information to build Situation Reports (SITREPs) and a Common Recognised Information Picture (CRIP).

In a densely populated country like the UK, where wide-area emergencies are likely to affect large numbers of people, self-help will be the first response. Wide-area emergencies can overwhelm local resources, disrupt telecommunications and other essential services, and cut off access or egress routes. Further blockage of routes may occur as people attempt to leave an affected area.

Business continuity management will also be a particular challenge. Primary office locations and emergency control centres may have been affected or made inaccessible. The likelihood of a protracted response and recovery effort will also place a heavy burden on staff and resources. Wide-area emergencies may affect large parts of one or more LRF area or regions, and therefore pose challenges in terms of communication, co-ordination, and integration. Where several SCGs are established, they will need to work closely together to ensure the response is integrated and co-ordinated. There may be a role for the sub-national tier, or devolved governments, in supporting or co-ordinating the local response, and a Lead Government Department (LGD) may become involved.

Not all emergencies occur suddenly. The emergency management framework set out in the Emergency Response and Recovery, Non statutory guidance accompanying the Civil Contingencies Act 2004 (October 2013) is adaptable to slow-onset (or rising tide) emergencies such as a disruption to the supply of fuel. In such circumstances, it becomes more likely that the response will be led from the top-down rather than from the bottom-up, with SCGs being convened at the request of, and working within, a strategic framework set by central government.
Under certain circumstances central government will be:

- Better sighted on an emerging risk (e.g., through intelligence reports, international liaison, or access to specialist advice).
- Well positioned to maintain an overview of the situation as it develops (e.g., patterns of disruption).
- Able to help ensure a coherent, integrated, and robust response (ensuring that pre-emptive action is taken where necessary and scaled appropriately).

Effective top-down leadership of an emergency presumes robust and timely information flows upward and downward. Sub-national Teams, and the Devolved Administrations, will play a crucial role in ensuring that this happens, activating crisis management arrangements. There may be a particular role for these levels in co-ordinating the flow of information from utility providers which are unable, for resource or other reasons, to attend multiple SCGs in a wide-area emergency.

When in communication with Government liaison roles during an emergency, these civil servants may not have a detailed understanding of railway operations and terminologies and so explanations of issues should be in clear English.

3.3.4.1 Response Framework for Terrorist Incidents

Responding to, and recovering from, the consequences of a terrorist incident will be similar to that adopted in relation to non-malicious incidents. It may be necessary for the police to take executive action in respect of the entire terrorism incident. The impact of terrorist events on public confidence, and the possibility of further attacks, will make the provision of warnings, advice, and information to the public particularly important. Separate guidance documents detail the specific response and recovery arrangements in relation to terrorist incidents. Most of these are protectively marked and are distributed to those organisations that require them rather than being made publicly available. Rail Entities can request to obtain guidance documents from the National Rail Security Programme (NRSP).

3.3.4.2 Response Framework for Evacuation

The possible need for evacuation of the public from the immediate vicinity may also have to be considered at a very early stage. It may be necessary to advise the public on whether they should evacuate a given area or remain and shelter in place / indoors. Such circumstances include risks to life or health from:

- Acts of terrorism.
- Release or threatened release of radioactive materials or other hazardous substances.
- Spread of fire.
- Risk of explosion.
- Damage caused by severe weather.
- Risk from serious flooding.
- Risk of environmental contamination.
- Transport failures.

It is normally the police who recommend whether to evacuate and define the area to be evacuated. Their recommendation will take account of advice from other agencies. The police can only recommend evacuation and have no power (except within the inner cordon in response to a terrorist incident) to require responsible adults to leave their homes. In any decision to evacuate or not, the over-riding priority must be the safety of the public and emergency responders, and it is necessary to assess whether bringing people outdoors may

put them at greater risk. Buildings can provide significant protection against most risks and the public may be safer seeking shelter in the nearest suitable building.

Similarly, in the case of chemical, biological, or radiological release, taking shelter would normally be the preferred initial option. In the case of flooding, it may be safer to advise people to seek refuge in the upper storeys of a building rather than run the risk of being overcome by the flood waters. Multi-agency co-operation is a guiding principle for evacuation planning, and Local Resilience Forums should develop a generic evacuation plan and consider how best to structure their evacuation planning activities, for example, by establishing a sub-group to focus specifically on evacuation and shelter issues. Similarly, the rail industry should establish a focus group specifically on evacuation and shelter issues for rail infrastructure, to consider how best to structure evacuation planning activities and developing cross industry and rail entity specific evacuation plans.

In 2006 the Cabinet Office published Evacuation and Shelter Guidance This guidance should be used by emergency planners to develop scalable and flexible plans that enable a co-ordinated multi-agency response in a crisis. The guidance is designed to inform on the roles and responsibilities relating to evacuation and shelter and give more information on the key issues relating to evacuation and shelter, including those that have proved problematic in past exercises or real-world events.

As detailed in the Evacuation and Shelter guidance plans should consider the following:

- Transporting people and traffic management.
- Shelter and rest centre accommodation.
- Supporting people sheltering in situ.
- Assisting groups with specific needs.
- Developing multi-agency crime prevention strategy.
- Pets and livestock.
- Business continuity.
- Protecting items of cultural interest and high value.
- Special considerations for flooding, chemical, biological, radiological, or nuclear/hazardous (CBRN) materials and pandemic flu.
- Return and recovery.
- Communications.

In the event of larger scale evacuation, local emergency responders may need to call on aid from outside their area, which can be prepared for by developing mutual aid arrangements. See Cabinet Office and the Local Government Association published Mutual Aid: A short guide for local authorities.

The Department for Culture, Media and Sport published Humanitarian Assistance in Emergencies: Non-statutory guidance on establishing Humanitarian Assistance Centres. This guidance is designed to give advice about how to structure the humanitarian response to an emergency with major consequences. See RDG-OPS-ACOP-001: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident for rail specific humanitarian assistance guidance and Section 5.5.2 for responder requirements in relation to humanitarian assistance.

Logistic operations refer to the co-ordination of the acquisition, distribution, and replenishment of supplies essential for the response and recovery to an emergency. Emergencies, especially when sustained and affecting a wide area, can pose serious logistical challenges to local responders. See Cabinet Office guidance for emergency planners on Logistic Operations for Emergency Supplies with the objective of establishing a common understanding of the options available to emergency planners for the co-ordination, prioritisation, and acquisition of emergency supplies.

Further guidance on evacuation and shelter can be found in Evacuation and shelter guidance: Non-statutory guidance to complement Emergency preparedness and Emergency response and recovery (2014).

Guidance on dealing with a train accident and train evacuation should be sought via Rail Safety and Standards Board (RSSB) Rule Book Module M1 GERT8000-M1 Issue 7: Dealing with a train accident or train evacuation.

3.3.4.3 Identifying Vulnerable Persons During a Crisis

The most effective way to identify vulnerable people is to work with those who are best placed to have up-to-date records of individuals and who will be aware of their needs. This may range from care homes (older people), those in other residential care settings, to the local hotel industry (tourists).

It is also recommended that lists of organisations and establishments are made, who can then be contacted in the event of an emergency to provide relevant information.

Once relevant agencies have been identified and networks developed, agreed data sharing procedures can be put in place, which should have the flexibility to adjust to changing circumstances with clear agreed triggers between responders.

By building networks and agreeing data sharing protocols, the potential scale of requirements of vulnerable people can be estimated in advance of an emergency, without divulging information about individuals. This information can then feed into emergency planning in terms of resources and equipment.

See Chapter 6 on Data Sharing and Vulnerable People for further information.

There are also difficulties in evacuating people who are frail or vulnerable. Those responsible for the care of vulnerable people in an emergency should develop a local action plan to identify people who are vulnerable in a crisis (see the Cabinet Office guidance Identifying People Who are Vulnerable in a Crisis: Guidance for Emergency Planners and Responders) for more details. RDG-OPS-ACOP-001 Issue 17 – June 2021: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident also provides more guidance on responsibilities for rail entities in relation to humanitarian assistance.

3.3.5 Integration of Response and Business Continuity

Rail Entities should have in place an internal Response Structure that ensures the organisation has a documented and well-understood hierarchy of teams for responding to an emergency, regardless of its cause. The Response Structure goes beyond the ability to recover BAU processes. The Response Structure establishes command, control, and communication to help the organisation manage the emergency and minimise its impact.

To maximise the organisation's ability to simultaneously respond to an emergency and ensure the best possible continuity its own services, Business Continuity should be an integral part of this Response Structure (Figure 5). **It is not a separate or stand-alone activity** and contributes to the successful resolution of an incident.

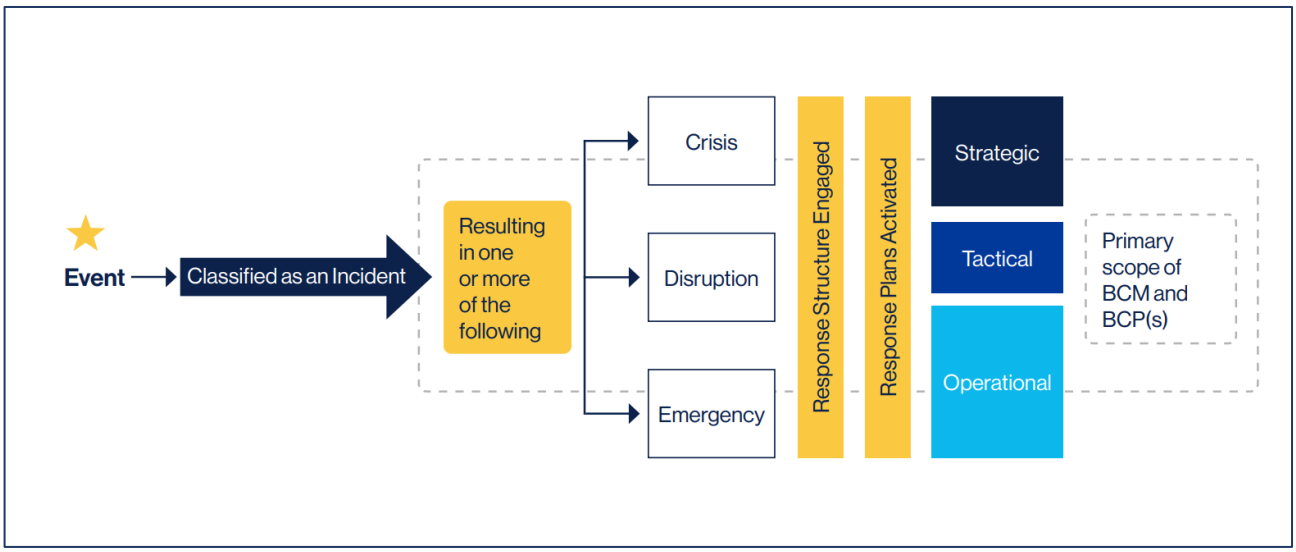

Figure 5 Business Continuity Response Structure (Source: Business Continuity Institute Good Practice Guidelines 2023)

An effective organisational response capability can be achieved if BC professionals collaborate with other professionals accountable for managing the response in their respective management disciplines. This has the added advantage of contributing to an improved BC culture, encouraging those collaborating to embrace better BC.

The response structure identifies:

- The roles, responsibilities, and authority of the teams responsible for response activities.
- The leadership of each team.
- The documented procedures to support the teams.

Rail Entities should develop a response structure that meets its own needs. The response structure should be closely aligned with the existing management and organisational structures as this will help align with existing chains of command and responsibilities. The result is clearly defined roles and responsibilities when responding to an emergency.

Rail Entities should establish a response structure that is proportionate to the size, complexity, and profile of the organisation and scalable for the foreseeable risks that entity would be required to manage.

While the focus of BC is the resumption of prioritised business activities, this is only one type of instant the response structure must be able to manage. Therefore, when developing the response structure, include all teams that may be required to respond to incidents. For example, teams from the areas of emergency environmental response, ICT DR, Supply Chain Continuity Management (SCCM), health and safety, or cyber incident response teams.

All members of the response structure must be trained and must participate in exercises.

An organisation’s response structure should be agile and capable of dealing with a variety of emergencies. Emergencies may have an immediate impact but, in other situations, the impact could develop slowly over time. Therefore, emergencies need to be monitored and early action taken to prevent them from escalating further.

The critical requirements for an effective response structure include:

- The ability to recognise and assess threats when they occur.
- Clear procedures for escalation when an incident has occurred or may occur soon.
- Individuals and teams with the authority and capability to develop and select an appropriate response to an incident.
- Clearly understood procedures in place to activate and control the response to an incident.
- Responsible personnel with the authority and competency to invoke the agreed response, which may include implemented solutions.
- A plan to communicate effectively with internal under external interested parties.
- Access to sufficient resources to support the response.
- Knowledge of when key external suppliers and regulators should be notified and included in the response.
- An agreed budget for supporting the response structure, including training.

Some organisations build their response structure to use existing levels in a hierarchy (for example, strategic, tactical, and operational). The strategic, tactical, and operational teams in the response structure undertake different levels of activity and align with those described in Chapter 4.

The **strategic team** focuses on issues threatening the organisation’s reputation and viability. This includes impacts on the organisation’s core objectives or products and services. The strategic team is always led by top management. At the strategic level, it is important to recognise the following considerations:

- Crises are abnormal situations that threaten the organisation’s viability and integrity. They require a flexible and creative response by experienced managers with the authority to apply the organisation’s complete resources to the response.
- The strategic team is often called the crisis management team. It is primarily responsible for addressing incidents impacting the organisation at strategic level, which may be formally declared as a crisis.
- While crisis management is a separate discipline, it is often established and coordinated by the BC professional – particularly in smaller organisations.
- The strategic team may also provide guidance and decision-making during less severe incidents and support tactical and operational teams.
- Complex organisations may have local, regional, and global strategic teams. In smaller organisations,

the strategic team may also perform the tasks of the tactical team.

Tactical teams enable the coordination of response activities when several operational teams are involved. The are responsible for several tasks:

- Providing support for the strategic team.
- Passing on directives from the strategic team to the operational teams.
- Consolidating information from the operational teams and relaying this to the strategic team.

Operational teams focus on the continuity of the business activities and the availability of resources that deliver the prioritised products and services. Operational teams also deal with the immediate effects of an incident by containing it when possible and managing the direct consequences. Operational teams may also manage the recovery of the resource is the business activities.

Table 4 below describes the various types of strategic, tactical, and operational plans.

*Examples of possible owners are provided (NB there should only be one owner of each plan).

Source: The Business Continuity Institute Good Practice Guidelines 2023

Table 4 Various types of strategic, tactical, and operational plans and their respective response teams (Source: The Business Continuity Institute Good Practice Guidelines 2023)

Plan Type	Plan Name	Definition	Typical Owner*	Response Team
Strategic	Crisis management plan	Defines the framework for managing strategic issues resulting from an incident.	Crisis management team leader	Crisis management team
	Crisis communications plan	Sets out how communications to key stakeholders (internal and external) will be managed at the time of the incident.	Public relations manager, external affairs manager, communications manager	Crisis communications team
Tactical	Alternate work area plan	Describes how to coordinate the preparation of one or more facilities in anticipation of relocating multiple business units, including remote work capability.	Facilities manager	Facilities team, ICT team
	Transportation plan	Describes how the transportation of personnel and products from multiple business units to one or more alternate facilities will be coordinated.	Facilities manager	Facilities team, corporate security
	Procurement plan	Describes how resources will be sourced and allocated when a supplier disruption affects multiple business units.	Procurement manager	Procurement team
Operational	Business unit recovery plan	Provides direction on continuing business activities (and processes) to deliver products and services when a facility, technology, people, or supplier are unavailable.	Business unit manager	Individual business units
	Emergency response plan	Describes the steps to be taken to protect life and safety and to secure the facility.	Facilities manager	Emergency response team

	Technology recovery plan	Identifies the steps to be taken in response to the loss and for the subsequent recovery of the technology infrastructure, such as network, systems, applications, data, and telecommunications to support business activities.	ICT manager Facilities manager, HR Manager, or ICT manager	ICT disaster recovery team
	Warning plan	Describes how to notify people of an incident, or the possibility of an incident, so that they can take action to protect themselves and/or participate in the response to an incident.	BC business unit manager	Facilities team, HR team or ICT team
Recovery return to BAU plans	Recovery plan	Describes how to return the business processes to a normal state from the temporary measures deployed during the response to the disruption.	Managers of: quality, regulatory, operations, or production department.	Crisis management team
Scenario specific plan	Pandemic plan	Describes how to manage a disease outbreak	Health and safety manager	Pandemic team (comprises BC, HR, facilities, health, and safety)
	Product recall plan	Sets out the procedures to be followed when there is a health or environmental issue with the product.	Information security manager	Product recall team
	Hazardous material spill	Describes the procedures for managing a spill that may impact health, safety, and environment safety.	Health and safety manager	Health and safety team
	Cyber incident response plan	Describes how to manage compromised systems or data at the technical level.	Information security manager	Information security team

4 Command & Control

4.1 Overview

Emergency Response and Recovery Non-Statutory Guidance accompanying the Civil Contingencies Act 2004 (October 2013) provides a framework which identifies the various tiers of single-agency and multi-agency management in emergency response and recovery (see Figure 6). It defines the relationships between tiers and individual agencies within the tiers. It provides a common framework within which individual agencies can develop their own response, recovery plans and procedures.

Command, Control and Coordination are important concepts in the multi-agency response to emergencies. This section distinguishes between single agency command and control structures and multi-agency coordination structures.

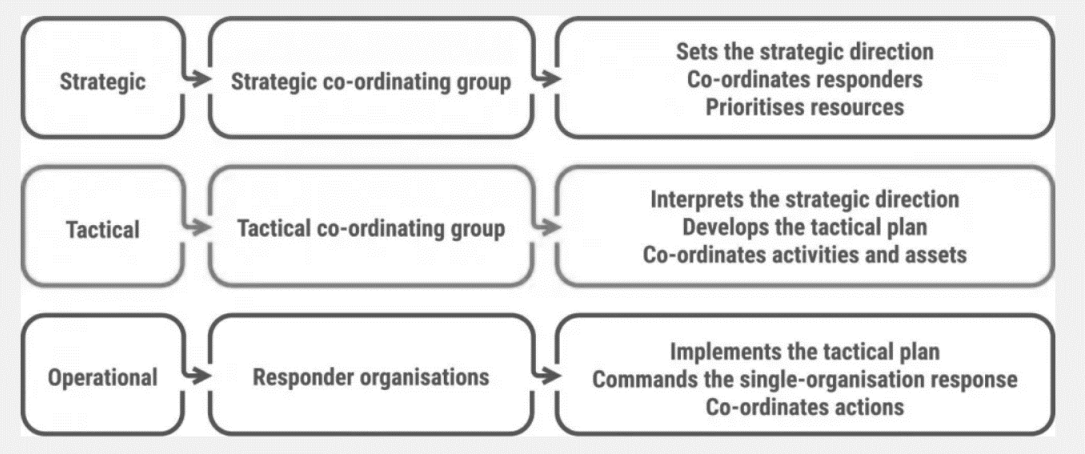

Figure 6 Command and control structure (Source: JESIP Joint Doctrine Edition Three)

Command is the exercise of vested authority that is associated with a role or rank within an organisation, to give direction in order to achieve defined objectives.

Control is the application of authority, combined with the capability to manage resources, to achieve defined objectives. Some organisations define command and control together. A key element of control is the combination of authority, with the means to ensure command intent is communicated and results monitored. While command cannot be exercised by one organisation over another, the authority to exercise control of an organisation's personnel or assets, for a specified period to attain defined objectives can be granted or delegated to another organisation. This granting of control does not imply that the responsibility for those resources has been transferred.

Co-ordination is the integration of multi-agency efforts and available capabilities, which may be interdependent, to achieve defined objectives. The co-ordination function will be exercised through control arrangements and requires that command of individual organisations personnel and assets is appropriately exercised in pursuit of the defined objectives.

4.1.1 Single Agency and Multi-Agency Structures

Across civil protection communities it is important to distinguish between the respective functions of single and multi-agency groups. Single agency groups have the authority to exercise a command function over their own personnel and assets. Multi-agency groups are convened to co-ordinate the involved agencies' activities and, where appropriate, define strategy and objectives for the multi-agency response. No single responding agency has command authority over any other agency's personnel or assets.

Where multi-agency co-ordinating groups are established to define strategy and objectives, it is expected that all involved responder agencies will work in a directed and co-ordinated fashion in pursuit of those objectives. Source: *Emergency Response and Recovery Non-Statutory Guidance accompanying the CCA 2004, October 2013.*

The management of the emergency response and recovery effort, in a multi-agency environment, is undertaken at one or more of three ascending levels: Operational, Tactical and Strategic. Within a single agency structure this is often recognised as Bronze, Silver, and Gold, see Figure 4 in Section 3.3.4 or Figure 8 in Section 4.3.1.

In planning stages each organisation will need to recognise the tiers of emergency management and their support requirements. It important to note that not all tiers, single or multi-agency, will necessarily be convened for all emergencies. The tiers of management do not predetermine the rank or status of individuals involved but act as descriptors of their functions.

4.1.2 Strategic Coordinating Groups

If the scale and nature of an incident is such that it requires strategic guidance, this will be provided through a Strategic Co-ordinating Group (SCG), a multi-agency body that will be formed in the Strategic Coordination Centre (SCC), normally located within that LRF area. Operating alongside but separate from the SCG will be individual agencies' own command structures, in many cases headed up by each agency's own 'Gold Commander'. For example, the Rail Incident Commander (RIC) who will feed into the multi-agency SCG as the rail industry strategic lead role.

Emergencies can place considerable demands on the resources of responding agencies and can pose significant challenges in terms of business continuity management. Furthermore, they may have long-term implications for communities, economies, and the environment. These require the attention of senior leadership and management.

Lessons identified from emergencies show that establishing SCGs at an early stage on a precautionary basis can be extremely helpful in ensuring local responders are ready if a situation suddenly worsens. Precautionary SCGs need not physically convene at the outset but can instead use other appropriate means to share and assess information on the extent of the emergency.

4.1.3 Technical Advisory Sub-groups

Within a multi-agency SCG sub-groups may be convened at the request of the chair. These usually include:

- A Recovery Co-ordinating Group, led by the relevant local authority, to prepare for the recovery phase and advise the SCG on response decisions that can potentially affect longer-term recovery activity.
- A Science and Technical Advisory Cell (STAC), led by the relevant expert organisation with representation from other leading scientific and technical organisations.

Individual agencies strategic groups may also convene sub-groups on specific areas essential to the response and recovery efforts.

4.1.4 Strategic Command (Gold) – Lead

The purpose of the Strategic level is to consider the emergency in its wider context:

- Determine longer-term and wider impacts and risks with strategic implications.
- Define and communicate the overarching strategy and objectives for the emergency response, within the response structure and to external parties, the media, and the public.
- Establish the framework, policy, and parameters for lower-level tiers.
- Monitor the context, risks, impacts and progress towards defined objectives.

Individual responder agencies may refer to the Strategic level as Gold. Where an event or situation has an especially significant impact; substantial resource implications; involves many organisations; or lasts for an extended duration, it may be necessary to convene a multi-agency co-ordinating group at the strategic level.

See Section 4.3.4 for further guidance and Section 5.5.3.1 for strategic responder requirements for Category 2 responders under the CCA and specific to the rail industry.

4.1.5 Tactical Command (silver) – Coordinate

The purpose of the tactical level is to ensure that the actions taken by the operational level are co-ordinated, coherent, and integrated in order to achieve maximum effectiveness and efficiency. Individual responder agencies may refer to the Tactical level as Silver.

While a single agency will usually be identified at an early stage to be the lead responder, they do not have

the authority to command the personnel or assets of other involved responders.

Where formal co-ordination is required at the Tactical level, then a Tactical Co-ordinating Group (TCG) may be convened. This will usually comprise the most senior officers of each agency committed within the area of operations and will undertake tactical co-ordination of the response to the event or situation.

See Section 4.3.5 for further guidance and Chapter 5 for additional responder requirements for Category 2 responders under the CCA and specific to the rail industry.

4.1.6 Operational Command (bronze) – Manage

Operational is the level at which the management of immediate, hands-on work is undertaken at the site(s) / scene of the emergency or other affected areas. Individual responder agencies may refer to the Operational level as Bronze.

First responders will take immediate steps to assess the nature and extent of the problem. Operational commanders will concentrate their effort and resources on the specific tasks within their areas of responsibility – for example, the police will concentrate on establishing cordons, maintaining security, and managing traffic. They will act on delegated responsibility from their parent organisation until higher levels of management are established.

See Section 4.3.6 for further guidance and Chapter 5 for additional responder requirements for Category 2 responders under the CCA and specific to the rail industry.

4.1.7 Decision making

One of the difficulties facing responders is how to bring together the available information, reconcile potentially differing priorities and then make effective decisions together under pressure.

The Joint Decision Model (JDM) was developed by JESIP (Joint Emergency Services Interoperability Programme) to resolve this issue. The JDM is designed to help make effective decisions together, as commanders establish shared situational awareness (Figure 7).

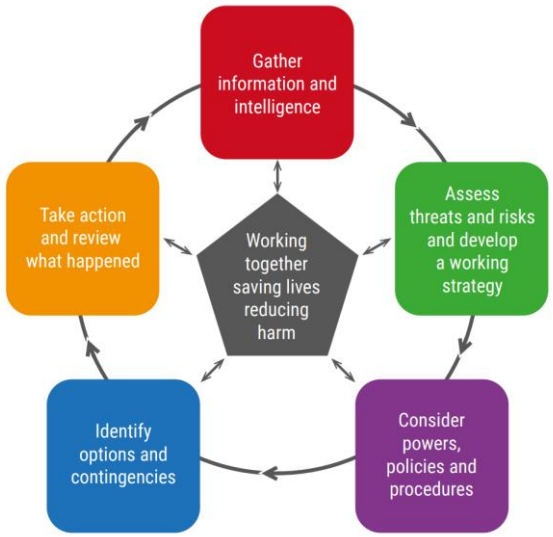

Figure 7 The Joint Decision Model (Source: JESIP Joint Doctrine: the interoperability framework).

All responder organisations may use various supporting processes and sources to provide information, including any planned intentions, this supports joint decision making. All decisions, the rationale behind them and subsequent actions should be recorded in a joint decision log. Rail entities should also ensure individual decision logs are recorded and maintained.

For further guidance on decision making see section 4.3.7.

4.1.8 Common Operating Picture (COP)

A COP is a single display of information collected from and shared by more than one agency or organisation that contributes to a common understanding of a situation and its associated hazards and risks along with the

position of resources and other overlays of information that support individual and collective decision making. During emergencies which affect multiple response partners the LRF will normally generate a COP with input from the various agencies involved, this COP is then published on Resilience Direct or circulated via email.

See Section 4.3.7.3, Section 4.3.9, and Section 4.3.10 for further guidance on COPs.

4.1.9 Communication and Coordination

Meaningful and effective communication between responders and responder organisations underpins effective response to emergencies and joint working. Communication links start from the time of the first call or contact, instigating communication between command levels and control rooms as soon as possible to start the process of sharing information.

For further guidance on communications see Section 4.3.10.

Control rooms should engage in multi-agency communications at the earliest opportunity to carry out the initial actions required to manage the incident. Co-ordination involves control rooms and responders of all levels, be they on scene or at a TCG or SCG, discussing the available resources and activities of each responder organisation, agreeing priorities, and making joint decisions throughout the incident.

Co-ordination underpins joint working by avoiding potential conflicts, preventing duplication of effort and minimising risk. Control rooms should ensure that initial actions required to manage the incident are carried out, including engaging in multi-agency communications. They will continue to respond to any actions that may arise during the incident and maintain communications with on-scene responders, as well as other agencies, to ensure they consistently achieve effective co-ordination.

For further guidance on coordination see Section 4.3.10.

4.1.10 Common understanding of risk

Different responder organisations may see, understand, and treat risks differently. Each organisation should carry out their own risk assessments, then share the results so that they can plan control measures and contingencies together more effectively.

Individual dynamic risk assessment findings may be used to develop the analytical risk assessment for the incident. This process applies if military assets are taking tactical direction from civil authorities, while remaining under military command. However, this does not absolve military commanders from their own assessment of the risks; indeed, risk should be assessed and agreed through the Defence duty holder chain of command rather than the operational chain of command.

By jointly understanding risks and the associated mitigating actions, organisations can promote the safety of responders and reduce the impact that risks may have on members of the public, infrastructure, and the environment.

Source: JESIP Joint Doctrine Edition Three.

For further detail on the management of risk, see RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance and RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP).

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document.

4.2 Provisions

4.2.1 Rail Entities ***MUST*** ensure their warning and informing arrangements include the ability to communicate an incident, as an example warning and informing details ***COULD*** include [4]:

a) Location.
b) Access/egress routes.

c) Date/time.
d) Any rolling stock involved, plus its route.
e) Incident timeline.
f) Casualties/fatalities.
g) Number of people involved.
h) Damage caused.
i) Prevailing weather conditions.
j) Dangerous goods on-board.
k) Crew on-board.
l) Railway property owner.
m) Staff responsible for movement of the rolling stock.
n) Number and type of vehicles involved.
o) Emergency services in attendance.
p) Incident Commander's contact details.

4.2.2 Rail Entities ***SHOULD*** ensure Gold and Silver levels of command are clearly distinguished from the multi-agency coordinating groups that exist at the corresponding level. [1]

4.2.3 Rail Entities ***SHOULD*** apply the principle of subsidiarity (i.e., decisions should be taken at the lowest appropriate level, with coordination at the highest necessary level). [1]

4.2.4 Rail Entities ***SHOULD*** activate a Strategic Group on a precautionary basis before standing it down (this is deemed better practice than being forced to activate a Strategic Group belatedly under the pressure of an emergency). [1]

4.2.5 Rail Entities ***SHOULD*** start communication from a position of considering the risks and harm if they do not share information. [5]

4.2.6 Decision-making processes ***SHOULD*** always aim to be inclusive and, wherever possible, arrive at consensual decisions. [1]

4.2.7 Rail Entities ***SHOULD*** consider inputting to a SCG Science and Technical Advice Cell (STAC) to provide timely and co-ordinated advice on scientific and technical issues. [1]

4.2.8 Rail Entities Strategic Commander role holders ***SHOULD*** refer to RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers during an emergency response.[8]

4.2.9 Responders ***SHOULD*** work together to build shared situational awareness.[15]

4.2.10 Rail Entities ***SHOULD*** ensure all decisions during an emergency response are recorded by a trained loggist.[15]

4.2.11 Rail Entities ***COULD*** use the JESIP Joint Decision Model to ensure interoperability with other responding agencies.[15]

4.2.12 Responder organisations ***SHOULD*** consider and not discount sources of local or specialist knowledge, as they may be able to provide information about the incident or the location.[15]

4.2.13 Rail Entities ***COULD*** utilise the JESIP M/ETHANE structured model to collate and share information about an incident.[15]

4.2.14 Rail Entities Strategic Commanders ***COULD*** use the JESIP process for developing a working strategy during an emergency response.[15]

4.2.15 Responders ***COULD*** utilise the JESIP decision controls, to enable decision making during an emergency response.[15]

4.2.16 Responders ***COULD*** utilise the IIMARCH mnemonic as a briefing tool during an emergency response.[15]

4.2.17 Rail Entities ***SHOULD*** make use of Common Operating Picture during an emergency response to provide an overview of an incident which is accessible through a secure common information sharing

platform.[15]

4.3 Guidance Notes

4.3.1 Single & Multi-Agency Structures

Within the Emergency Response and Recovery non-statutory guidance, national framework, the management of the emergency response and recovery effort is undertaken at one or more of three ascending levels: Operational, Tactical and Strategic, or often known as Bronze, Silver, and Gold within a single agency response structure (see Figure 8).

Each LRF, Local Resilience Partnerships (LRP) (Wales), Regional Resilience Partnership (Scotland) and responding agency will have its own triggers and thresholds for when to establish each of the levels of command structure.

It is important to distinguish between the respective functions of single and multi-agency groups. Single agency groups have the authority to exercise a command function over their own personnel and assets. Multi-agency groups are convened to co-ordinate the involved agencies' activities and, where appropriate, define strategy and objectives for the multi-agency response. No single responding agency has command authority over any other agency's personnel or assets. Where multi-agency co-ordinating groups are established to define strategy and objectives, it is expected that all involved responder agencies will work in a directed and co-ordinated fashion in pursuit of those objectives.

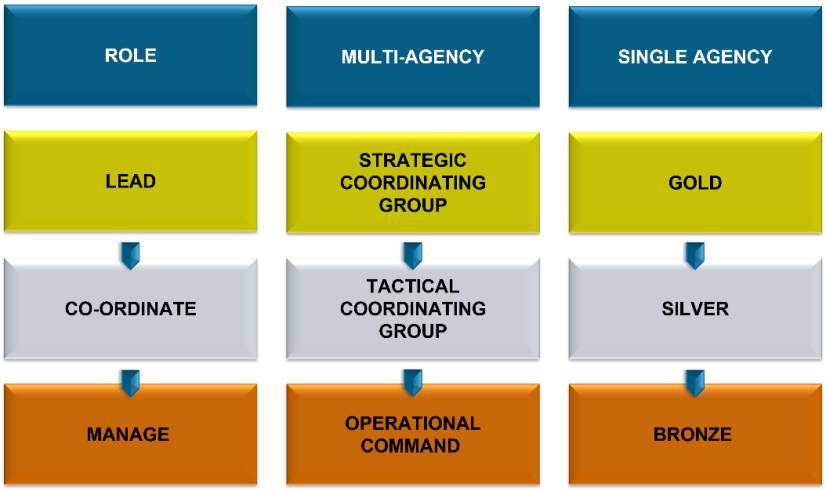

Figure 8 Explanation of roles across the responding levels.

Operating below the local (multi-agency) Strategic Co-ordinating Group are three levels of command at a single agency level – operational (Bronze), tactical (Silver) and strategic (Gold). Often these will be implemented without the need for multi-agency co-ordination through the SCG with any necessary co-ordination taking place at silver or bronze level. The need to implement one or more of these response levels will depend on the nature of the incident, but normally incidents will be handled at the operational level, moving to the tactical or strategic level if required depending on the scale or nature of the incident.

An example of a practical application of this three-tier command structure can be seen in Figure 9 below, with designated roles at Gold, Silver, and Bronze within a single agency.

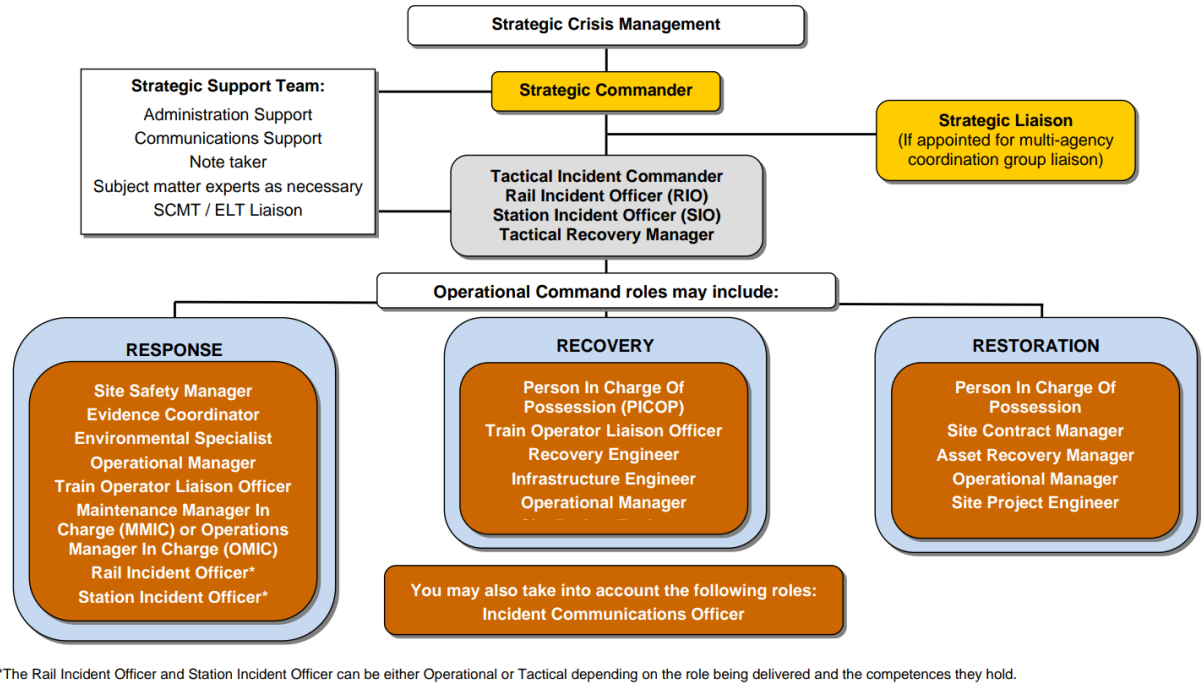

Figure 9 Rail Industry incident command structure (Source: Specification – Network Rail National Emergency Plan, Ref: NR/L/OPS/250, Issue 8, June 2021).

Although a multi-agency SCG may colloquially be known by some responder bodies as a 'Gold Group', it is ambiguous to refer to the SCG simply as 'Gold' Similarly, it is ambiguous to refer to a multi-agency Tactical Co-ordinating Group (TCG) simply as 'Silver'; Gold and Silver describe single-agency levels of command, and they should be clearly distinguished from the multi-agency co-ordinating groups that exist at the corresponding level. Further, it is misleading to refer to the SCG Chair as 'Gold'.

It is important to note that not all tiers, single or multi-agency, will necessarily be convened for all emergencies. Additionally, the tiers of management do not predetermine the rank or status of the individuals involved but act as simple descriptors of their functions.

In rapid onset emergencies within a limited geographical area, the emergency management framework is usually constructed from the bottom up. Escalation of the event (in severity or geographical extent) or greater awareness of the situation may require the implementation of a tactical or even a strategic level. There will also be situations in which all three levels may be activated concurrently, and others (e.g., wide area, slow onset emergencies) when the response may be initiated by central government or by the sub-national tier. Decisions on the activation of management levels should be guided by flexibility and functional requirements. The principle of subsidiarity should be applied (i.e., decisions should be taken at the lowest appropriate level, with coordination at the highest necessary level). It is better to activate a SCG on a precautionary basis and then stand it down, than be forced to activate it belatedly under the pressure of events.

4.3.1.1 Train/Freight Operating Companies

Within the Rail Industry incident command structure, Train Operating Companies (TOCs) and Freight Operating Companies (FOCs) should be represented by their Control Lead within the Strategic Support Team, to ensure they can provide the necessary input at both strategic and tactical levels of command.

4.3.2 Strategic Co-ordinating Groups

The strategic group should be made up of senior representatives with executive authority. At a multi-agency SCG there should be a representative from each of the key organisations involved in the local response. It will normally be chaired by a senior police officer during the response phase, although on occasions, particularly where there is no immediate threat to life, a senior local authority official or other appropriately trained and experienced individual may assume the role.

The SCG will take strategic decisions on managing the emergency locally. Individual agencies strategic groups running alongside but separate to the SCG should follow individual agencies' own command structures and be chaired by each agency's own 'Gold Commander'.

Organisations and agencies that may be involved with the local response will all work on the following common objectives:

- Saving and protecting human life
- Relieving suffering
- Protecting property
- Providing the public with information
- Containing the emergency – limiting its escalation or spread
- Maintaining critical services
- Maintaining normal services at an appropriate level
- Protecting the health and safety of personnel
- Safeguarding the environment
- Facilitating investigations and inquiries
- Promoting self-help and recovery
- Restoring normality as soon as possible
- Evaluating the response and identifying lessons to be learned.

Source: Emergency Preparedness, Response and Recovery Guidance on Part 1 of the CCA 2004, its associated regulations and non-statutory arrangements.

If wide area or multi-SCG, devolved administration or UK tiers are convened, their role and function is to identify and address issues that require resolution or co-ordination at those levels in pursuit of the agreed objectives.

Such 'higher level' tiers do not remove the local strategic perspective from the local level, rather they consider only those issues and dimensions where value can be added by a broader or higher-level perspective. For this reason, a local strategic perspective and role (i.e., the SCG) can be distinguished from the sub-national or wide area perspective, e.g., the multi-SCG Response Co-ordinating Group (ResCG) where, for example, competing priorities for available mutual aid may need to be determined and distinguished, again from the UK-national perspective (e.g., the National Security Council (NSC), Sub Committee on Threats, Hazards, Resilience and Contingencies NSC (THRC)) where national (and potentially international) strategic issues may bear on the emergency response.

The purpose of the SCG is to take overall responsibility for the multi-agency management of the emergency and to establish the policy and strategic framework within which lower tier command and co-ordinating groups will work. The SCG will:

- Determine and promulgate a clear strategic aim and objectives and review them regularly.
- Establish a policy framework for the overall management of the event or situation.
- Prioritise the requirements of the tactical tier and allocate personnel and resources accordingly.
- Formulate and implement media-handling and public communication plans, potentially delegating this to one responding agency.
- Direct planning and operations beyond the immediate response in order to facilitate the recovery process.

As part of the tasking process, SCGs may commission the formation of a series of supporting groups to address particular issues. For example, given the likely demands of the immediate response from the SCG, it is good practice, in most emergencies with significant recovery implications, to establish a Recovery Co-ordinating Group (RCG).

Further detail on aspects of recovery can be found in RDG-OPS-ACOP-012 IEM, Recovery.

SCGs must develop a strategy for providing warnings, advice, and information to the public and dealing with the media. If a Lead Government Department is engaged in the emergency, then the co-ordination of media lines and information given directly to the public is essential if public confidence is to be maintained.

Further strategic issues that may require the formation of specific sub-groups include but are not limited to:

- Humanitarian assistance for those affected by the emergency.
- Facilitating inquiries and investigations.
- Visits by VIPs.
- International and diplomatic dimensions.
- Emergencies affecting Critical National Infrastructure (CNI) and continued operation and maintenance

of CNI.
- Emergencies involving hazardous materials and therefore requiring a specialised response.

The SCG does not have the collective authority to issue commands or executive orders to individual responder agencies. Each organisation represented retains its own command authority, defined responsibilities and will exercise control of its own operations in the normal way.

As a multi-agency group, the SCG has collective responsibility for decision-making and implementation. To achieve this, the SCG relies on a process of discussion and consensus to reach decisions at strategic level and to ensure that the agreed strategic aims and objectives are implemented at the tactical and operational levels. These discussions, including both decisions taken and not taken or deferred, must be logged for future scrutiny. Effectiveness at strategic level rests upon every member having a clear understanding of the roles, responsibilities, and constraints of other participants. The required mutual understanding and trust will be cemented through training and exercising and facilitated in a trusted environment between participants.

SCGs must comprise representatives of appropriate seniority and authority to be effective, and representatives should be empowered to make executive decisions in respect of their organisation's resources. In a long-running emergency, the need for personnel to hand over to colleagues will undoubtedly arise. This underlines the necessity for each organisation to select, train and exercise sufficient senior individuals who can fulfil this role.

It will normally, but not always, be the role of the police to co-ordinate other organisations and therefore to chair the SCG. The police are particularly likely to field a SCG chair where there is an immediate threat to human life, a possibility that the emergency was a result of criminal activity, or significant public order implications. Under these circumstances the same person may be the Police Strategic Commander and the SCG Chair. These two roles should be clearly distinguished. In other types of emergencies, for instance some health emergencies, an agency other than the police may initiate and lead the SCG.

In the transition to the recovery phase, the chair of the Recovery Co-ordinating Group (RCG) will usually pass to another agency if its role and responsibilities leave it better placed to take on the role (e.g., to the local authority). The identification of lead agencies in relation to specified emergencies and transitional arrangements in relation to the recovery phase should be agreed and exercised in the preparation phase.

The SCG should be based at an appropriate location away from the scene. The place at which the SCG meet is referred to as the Strategic Coordination Centre (SCC). This will usually, but not always be at the headquarters of the lead service or organisation (e.g., police headquarters). The location of meetings may shift if another agency takes the lead of the RCG in relation to the recovery phase. In the preparation phase, consideration should be given to the arrangements suitable for a range of scenarios and alternative locations should be identified for business continuity purposes. Part 3 of the Expectation and Indicators of Good Practice Set for Category 1 and 2 responders (Emergency Preparedness, Response and Recovery Guidance on Part 1 of the CCA 2004, its associated regulations and non-statutory arrangements, January 2006), provides a checklist of considerations for this.

4.3.3 Technical Advisory Sub-groups

The effective management of most emergencies will require access to specialist scientific and technical advice, for example regarding the public health or environmental implications of a release of toxic material, or the spread of a disease. During the response to an emergency, local responders in England are advised to consider establishing a Science and Technical Advice Cell (STAC) to provide timely and co-ordinated advice on scientific and technical issues. In Wales, public health advice for strategic co-ordinating groups is provided by Health Advisory Teams (HATs). The National Public Health Service for Wales takes the lead in the establishment of the HAT.

Local Resilience Forums (LRFs) (Local Resilience Partnerships (LRPs) in Wales and Regional Resilience Partnerships in Scotland) should have plans in place which identify a designated lead and core membership of the STAC; and set out the arrangements for its activation in the event of an emergency. Whilst the issues covered by the role of the STAC suggest that an appropriate person from the health community would be best placed to lead it, LRFs (SCGs in Scotland) will need to ensure that the person has the right knowledge and skill set to chair complex meetings and commands respect of their peers. Once the lead has been appointed, they should work with the SCG to select the core membership of the STAC, ensuring that those chosen have the knowledge and skills collectively to provide the level of scientific and technical advice required by the SCG.

The role of the STAC is to:

- Provide a common source of science and technical advice to the SCG chair and members and responder agencies Strategic Commanders.
- Monitor and corral the responding scientific and technical community to deliver on SCGs high-level objectives and immediate priorities.
- Agree any divergence from agreed arrangements for providing scientific and technical input.
- Pool available information and arrive, as far as possible, at a common view on the scientific and technical merits of different courses of action.
- Provide a common brief to the technical lead from each agency represented in the cell on the extent of the evidence base available, and how the situation might develop, what this means, and the likely effect of various mitigation strategies.
- Identify other agencies / individuals with specialist advice who should be invited to join the cell in order to inform the response.
- Liaise with national specialist advisors from agencies represented in the cell and, where warranted, the wider scientific and technical community to ensure the best possible advice is provided.
- Liaise between agencies represented in the cell and their national advisors to ensure consistent advice is presented locally and nationally.
- Ensure a practical division of effort among the scientific response to avoid duplication and overcome any immediate problems arising; and maintain a written record of decisions made and the reasons for those decisions.

Once the initial crisis response is complete, leadership of the incident will normally transfer to the Recovery Co-ordinating Group and the relevant local authority to oversee the recovery phase. In most scenarios, police response and local authority-led recovery groups will work in parallel within a single police force area until the SCG is stood down.

4.3.4 Strategic Command (gold)

The purpose of the strategic level of local emergency response management is to establish a framework to support officers operating at the tactical level of command by providing resources, prioritising demands from officers and determining plans for the return to normality.

The requirement for strategic management may not apply to all responding agencies owing to differing levels of engagement. However, emergencies almost always require multi-agency co-ordination and rarely remain entirely within the sphere of a single agency. It may, therefore, be appropriate for an agency not involved at strategic level nevertheless to send liaison officers to meetings of the SCG.

RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers states that the overall objective should be to demonstrate and deliver a response that is:

- Compassionate – acting sensitively and expressing regret for what has happened and for the impact on those involved, their families and friends.
- Competent – gaining and maintaining control of the situation.
- Confident – but not arrogant.
- Credible – being open and honest but without speculating.

With the joint aims of providing all appropriate care and support to those involved, limiting reputational damage, and minimising the effects on the rest of the business / returning to BAU as quickly and efficiently as possible.

Senior managers should remember that in many cases the rail industry will not be managing the “incident” itself (this is the responsibility of the emergency services) but will be managing the consequences of the incident. These will often be felt over a wide area away from the actual scene of the incident.

The Strategic Commander will need to be conscious of the following strategic objectives and ensure that each is being addressed, either by themselves or by others:

- Leadership – at site/within the business/publicly visible.
- Co-ordination.
- Provision of assistance/people issues.
- Communication.
- Continued operation.
- Support for investigation.

RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers relates to Strategic

Commanders within Rail and states that the Strategic Commander should remain focussed on the strategic level of incident command and not allow themselves to become drawn down into the tactical detail (unless the tactical plan is not meeting the needs of the strategy).

Their focus must be on the *WHAT?* And *WHY?* Of the response, i.e., *WHAT*, in broad terms, are we doing to respond to the situation – the 'game plan' – and *WHY* are we adopting this 'game plan', methodology or approach, rather than another one. The detail of what is being done to respond (the *HOW?*) should be left to the tactical level managers.

While clearly the focus during the initial response stage needs to be on the immediate challenges, it is also important to start thinking ahead to the recovery phase, including what is going to be needed to support this and how it might be resourced.

4.3.5 Tactical Command (silver)

Working in **co-ordination**, the responder agencies tactical commanders will:

- Determine and agree priorities for allocating available resources.
- Plan and co-ordinate how and when tasks will be undertaken.
- Obtain additional resources if required.
- Assess significant risks and use this to inform tasking of operational commanders.
- Ensuring the health and safety of the public and personnel is a priority.

Although each of the senior officers at the tactical level will have specific service or agency responsibilities, together they must jointly deliver the overall multi-agency management of the incident and ensure that operational commanders have the means, direction and co-ordination required to deliver successful outcomes.

Unless there is an obvious and urgent need for intervention, tactical commanders should not become directly involved in the detailed operational tasks being discharged by the operational level.

In a rapid onset emergency where there is a clear and identifiable scene and the emergency services are in the lead, then tactical co-ordination will usually be carried out from an incident control point (which may be termed a Forward Command Post) located nearby or directly adjacent to the scene. An alternative location should always be identified as a back-up. A Tactical Co-ordinating Group may, as the response progresses or circumstances dictate, be re-located to a point further removed from the incident site. Responder bodies should ensure that the TCG is established at the most appropriate location to carry out its function, including the convenient attendance of all appropriate responder representatives. Where co-location of tactical commanders is not possible, appropriate communications or representation to ensure a co-ordinated response at the tactical level is essential.

Arrangements that are necessary in the immediate vicinity of the scene include but are not limited to the following:

- Assessing control measures to reduce identified risks.
- Deciding the functions to be controlled by each agency after taking account of the circumstances.
- The professional expertise of the emergency services and other agencies.
- Statutory obligations.
- Overall response priorities and competing priorities management.
- The reception and engagement of utility companies' staff (e.g., gas, electricity, and water) on essential safety work, or to affect the restoration of essential services, where appropriate.
- Setting up cordons to secure the scene and provide a measure of protection for personnel working within the area.

All those entering the inner cordon should report to a designated cordon access point. This ensures that they can be safely accounted for should there be any escalation of the incident and affords an opportunity for briefing about the evacuation signal, hazards, control measures and other issues about which they need to be aware. People entering the inner cordon must have an appropriate level of personal protective equipment, while those leaving must register their departure.

If practical, an outer cordon may have to be established around the vicinity of the incident to control access to a much wider area around the site. This will allow the emergency services and other agencies to work unhindered and in privacy. Access through the outer cordon for essential non-emergency service personnel should be by way of a scene access control point. The outer cordon may then be further supplemented by a

traffic cordon.

Other issues (where relevant) that should be addressed at this level include but are not limited to:

- Establishing internal traffic routes for emergency and other vehicles (including a one-way system where appropriate).
- Deciding on the location of key functions or facilities, for example: casualty clearing station(s) to which any injured can be taken.
- Possible ambulance loading point.
- A collection/assembly point for survivors before they are taken to a Survivor Reception Centre.
- Possible helicopter landing site(s).
- A rendezvous point(s) for responding personnel, which may be some distance from the scene in the event of a bomb incident or incidents involving hazardous materials.
- A staging area for assembling vehicles and equipment.
- A secure Holding and Audit Area for Deceased People and Human Remains (HAADR) that is under cover and protected from public view.
- A media liaison point.
- Clearly identified responder welfare points, as applicable.

The effectiveness of the tactical level as a joint, multi-agency organisation rests on a systematic approach to multi-agency co-ordination. Irrespective of the pressure of operations, the TCG chair must create time for regular, structured briefings, consultations and tasking meetings with their counterparts and key liaison officers. Co-location will assist these processes. Processes should be defined, documented, and embedded through training and exercising.

When an emergency occurs without a specific scene (e.g., disruption to the fuel supply or an overseas emergency with domestic effects), a Tactical Co-ordinating Group may still be required to deliver effective multi-agency co-ordination.

In those cases where it becomes clear that resources, expertise, or co-ordination are required beyond the capacity of the tactical level (e.g., where there is more than one scene or incident), it may be necessary to invoke the strategic level to take overall command and set the strategic direction. Once this occurs, tactical commanders will continue to effect multi-agency co-ordination within their area of responsibility, while simultaneously directing tactical operations within the strategic direction and parameters set by the SCG and promulgated through their respective agencies Strategic Commanders.

4.3.6 Operational Command (bronze)

The operational level is where the management of the immediate work is undertaken at the emergency site(s) or affected area(s). Individual responder agencies may refer to the Operational level as Bronze. Personnel first on the scene will take immediate steps to assess the nature and extent of the problem and concentrate efforts and resources on the specific tasks within their area of responsibility. For example, police will concentrate on establishing cordons, maintaining security, and managing traffic. They will act on delegated responsibility from their parent organisation until higher levels of management are established. Agencies retain control of resources and personnel deployed at the scene, but each agency must also liaise and co-ordinate with other agencies, ensuring a coherent, co-ordinated, and integrated response effort.

Under some circumstances this may require the temporary transfer of one organisation’s personnel or assets under the control of another organisation.

These arrangements will usually be adequate to deal with most events or situations. Certain events that demand greater planning, co-ordination or resources might require an additional tier of management. A key function of an operational commander will be to consider whether circumstances warrant a tactical level of management and to advise their superiors accordingly. Such escalation processes can only be effectively implemented with incident escalation training and exercising. This ensures responders are both comfortable and confident in their remit of authority and decision making within their respective response tiers.

Operational commanders become responsible for implementing the tactical commander’s tactical plan within their geographical area or functional area of responsibility. To discharge this successfully, they need to have a clear understanding of the tactical commanders intent and plan, their tasks, and any restrictions on their freedom of action, on which they in turn can brief their staff.

4.3.7 Decision Making

Recording of decisions is critical and where possible should be undertaken by a trained loggist. Within JESIP when using the JDM, the priority is to gather and assess information and intelligence. Responders should work together to build shared situational awareness, recognising that this requires continuous effort as the situation, and responders' understanding, will change over time.

Understanding risk is vital in establishing shared situational awareness, as it enables responders to answer the three fundamental questions of 'what, so what and what might?'. Once the process of building shared situational awareness has begun, the desired outcomes should be agreed as the central part of a joint working strategy. If a Strategic Co-ordinating Group (SCG) is convened, they will agree and share the joint strategy for the multi-agency response. The strategic command teams from each organisation should then review and amend their single-agency strategy to be consistent with the joint strategy and support them in achieving the jointly defined outcomes, or overarching aim.

Deciding how all agencies will work towards the desired outcome reflects the available capabilities, powers, policies, and procedures (means) and the arising options, constraints, and contingencies (ways). Ways and means are closely related – some options will not be viable because they cannot be implemented, or they may be technically and logistically feasible, but illegal or ethically indefensible. These should still be logged with rationale as to why they were not achievable by the loggist.

The JDM helps responders explore these considerations and sets out the various stages of reaching joint decisions. One of the guiding principles of the JDM is that decision makers should use their professional judgement and experience in deciding any additional questions to ask and considerations to take into account, so that they can reach a jointly agreed decision. Further support is provided by considering the decision controls (see Section 4.3.7.6). Responders should be free to interpret the JDM for themselves, reasonably and according to the circumstances they face at any given time.

Achieving desired outcomes should always come before strict adherence to the stepped process outlined in the JDM, particularly in time sensitive situations. A detailed and well-practiced understanding of the JDM will help responders to think clearly and in an ordered way when under stress. The JDM can be used for both 'rapid onset' and 'rising tide' emergencies. Failing to decide and consequently doing nothing has potential life-threatening consequences.

The following from JESIPs Joint Doctrine: The Interoperability Framework summarises the questions and considerations that responders should think about when they use the JDM:

4.3.7.1 Working together, saving lives, reducing harm

The pentagon at the centre of the JDM reminds responders that all joint decisions should be made with reference to the overarching or primary aim of any response to an emergency – to save lives and reduce harm. This drives a people centred approach with a concern for public and responder wellbeing throughout the response. This should be the most important consideration throughout the decision-making process.

4.3.7.2 Gather information and intelligence

This stage involves gathering and sharing contingencies information and intelligence to establish shared situational awareness. At any incident, no single responder organisation can appreciate all the relevant dimensions of an emergency straight away. Information refers to all forms of information obtained, recorded, or processed, for example M/ETHANE messages. Intelligence is obtained from information that has been subject to:

- Evaluation, to determine its significance.
- Risk assessment, to determine the need for it to be acted on.
- Analysis, to identify critical links and associations that assist understanding of the incident.

Responder organisations should consider and not discount sources of local or specialist knowledge, as they may be able to provide information about the incident or the location. A deeper and wider understanding will only come from meaningful communication between responder organisations. Responders should not assume that others will see things, or say things, in the same way. There may need to be a sustained effort to reach a common view and understanding of events, risks, and their implications.

Decision-making in the context of an emergency, including decisions on sharing information, does not remove the statutory obligations of agencies or individuals. Decisions should be made with an overriding priority of saving lives and reducing harm.

Anyone providing sensitive information should also provide an understanding about how it can be used, shared, and stored. M/ETHANE is a structured model for responder organisations to collate and pass on information about an incident (Figure 10).

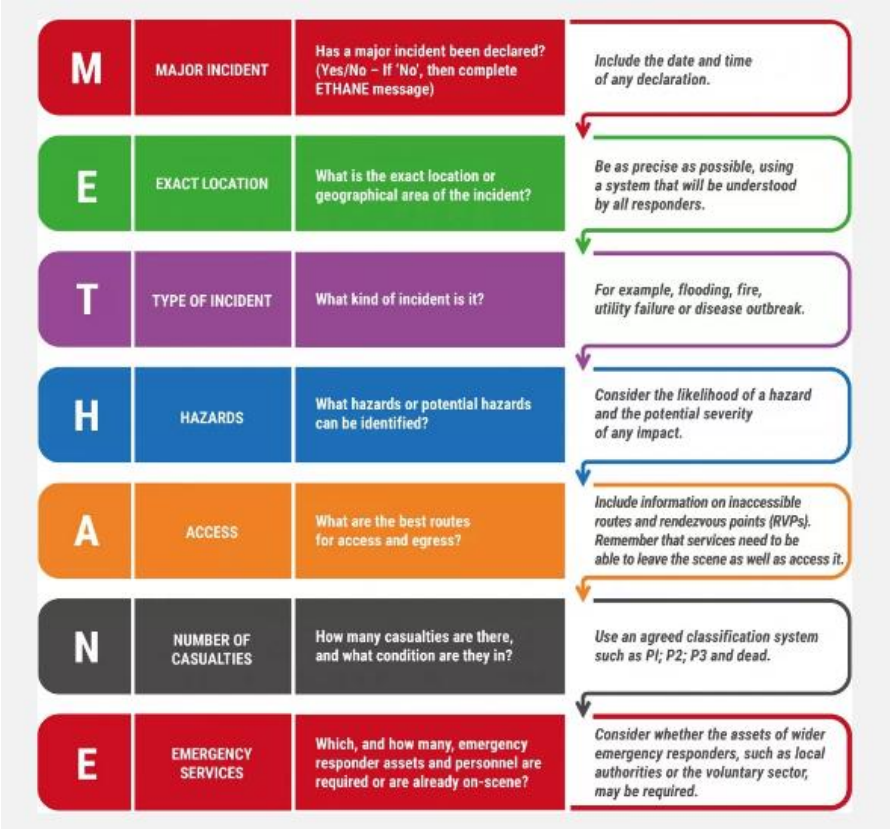

Figure 10 M/ETHANE Model

4.3.7.3 Assess threat and risk and develop a working strategy

This analytical stage involves responders jointly assessing the situation, including any specific threats, hazards, and risks. Responders should consider how risks may increase, reduce, or be controlled by any decisions made and subsequent actions taken. At any incident, each responder organisation will have a unique insight into those risks. By sharing what they know, responders can establish a COP; this allows for informed decision-making on deployments and the risk control measures required. Time critical tasks should not be delayed by this process.

The risk control measures to be employed by individual services must also be understood by other responder organisations, to ensure any potential unintended consequences are identified before activity commences. This increases the operational effectiveness and efficiency of the response as well as the probability of a successful incident resolution. It is rare for a complete or perfect picture to exist for a rapid onset incident especially at the early stages of a response. The working strategy should therefore be based on the information available and reviewed on a continual basis.

Further guidance on the Anticipation, Assessment and Prevention of risk can be found in RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP).

When developing a working strategy to guide the stages of the JDM and set out what responders are trying to achieve, considering the need for immediate action to save lives and reduce harm, responders should:

- Apply decision controls.
- Share single service risk assessments.
- Record and agree the joint assessment of risk, in a suitable format.

When developing a working strategy, responders should consider these questions:

- What: Are the aims and objectives?
- Who by: Police, fire and rescue service, ambulance service, other organisations?

- When: Timescales, deadlines, and milestones?
- Where: Locations?
- Why: What is the rationale? Is it consistent with the overall strategic aims and objectives?
- How: Will these tasks be achieved?

For an effective integrated multi-agency operational response plan, objectives and priorities must be agreed jointly. Each organisation will then prioritise their plans and activity. Figure 11 below outlines the process for developing a working strategy.

Figure 11 JESIP Process for developing a working strategy.

4.3.7.4 Consider powers, policies, and procedures

This stage relates to any relevant laws, procedures or policies that may impact on the response plan and the capabilities available to be deployed. Decision-making in an emergency will focus on achieving the desired outcomes. Various constraints and considerations will shape how this is achieved. Powers, policies, and procedures may affect how individual agencies operate and co-operate to achieve the agreed aims and objectives, which should reflect their statutory duties.

A common understanding of relevant powers, policies and procedures is essential, to ensure that the activities of responder organisations complement rather than compromise each other.

4.3.7.5 Identify options and contingencies

There will almost always be more than one way to achieve the desired outcomes. Responders should work together to evaluate the range of options and contingencies. Potential options or courses of action should be evaluated, considering:

- Suitability: Does it fit with the strategic direction?
- Feasibility: Can it be done with the available resources?
- Acceptability: Is it legal, morally defensible, and justifiable?

Whichever options are chosen, responders should be clear on what they need to carry out. Procedures for communicating any decision to defer, abort or initiate a specific tactic should also be clearly agreed and documented.

Contingency arrangements should be put in place to address reasonably foreseeable events that may occur as a result of action taken or not taken. For example, strong evidence may suggest that an emergency is being managed appropriately and the impacts controlled in line with current risk assessments, but there remains a potential that the situation could deteriorate and have a significant impact. If changes do occur, it is essential that these are shared between responders to maintain a joint understanding of risk.

4.3.7.6 Decision Controls

Decision-making in incident management should be a continuous process that follows a general pattern of:

- Working out what is going on (situation)
- Establishing what your objectives are and what you need to achieve (direction)
- Deciding what to do about it (action), all informed by a statement and understanding of overarching values and purpose, including which organisations are required.

Decision-making can be time critical. As part of the decision-making process, decision makers should use decision controls to ensure that the proposed action is the most appropriate. Decision controls support and validate the decision-making process. They encourage reflection and set out a series of points to consider before making a decision. Note that points (a) to (d) in the following diagram (Figure 12) are intended to structure a joint consideration of the issues, with 'E' suggesting some considerations for individual reflection.

Once the decision makers are collectively and individually satisfied that the decision controls validate the proposed actions, these actions should be implemented. As the JDM is a continuous loop, it is essential that the results of these actions are fed back into the first box, 'Gather and share information and intelligence', which sets out the need to establish and sustain shared situational awareness. This will, in turn, shape any change in direction or risk assessment as the cycle continues.

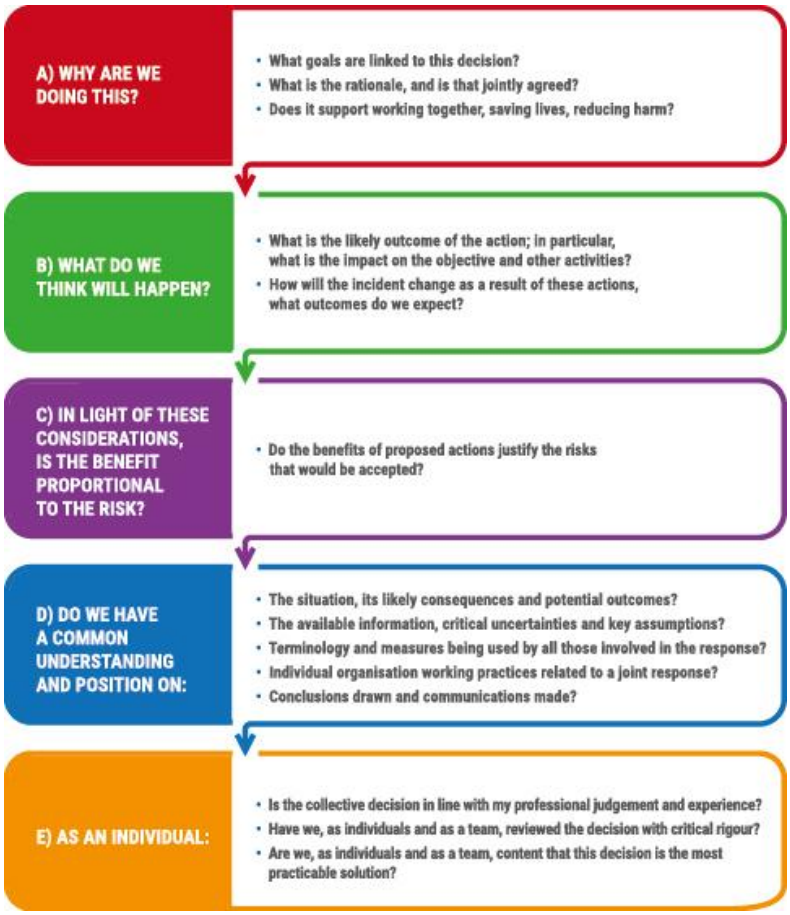

Figure 12 JESIP Decision Controls.

4.3.7.7 Briefing

Once decisions have been made and actions agreed, information should be relayed in a structured way that can be easily understood by those who will carry out actions or support activities. This is commonly known as briefing. In the initial phases of an incident, the JDM may be used to structure a briefing. As incidents develop past the initial phases, or if they are protracted and require a handover of responsibility, then a more detailed briefing tool should be used.

The mnemonic 'IIMARCH' is a commonly used briefing tool. Using the IIMARCH headings shown in Figure 13 as a guide, information can be briefed in appropriate detail.

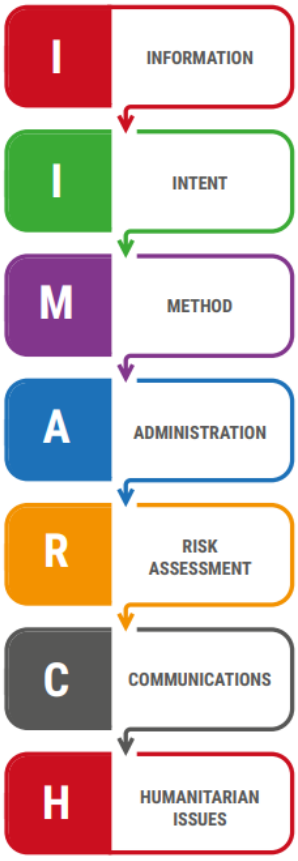

Figure 13 JESIP IIMARCH Headings

4.3.7.8 Take action and review what happened

Building shared situational awareness, setting direction, evaluating options, and making decisions all lead to taking the actions that are judged to be the most effective and efficient in resolving an emergency and returning to a new normality. Actions and the subsequent outcomes should be regularly reviewed. As information or intelligence becomes available or changes during the incident, responders should use the JDM to inform their decision-making until the incident is resolved.

4.3.7.9 Recording Decisions

All decisions, including the rationale behind them and action to be taken, should be recorded in an appropriate format. While each organisation should maintain its own records, there may be a local agreement to have a joint decision log. The JESIP Joint Decision Log provides an example. If decisions and relevant supporting information are not recorded in an appropriate way, it is difficult to prove and justify actions that have been taken. Legal cases are often focused on the recording of information, especially key decisions.

As an absolute minimum, decision logs should contain the:

- Decision – what decision has been made and by whom?
- Rationale – what is the rationale behind this decision, including consideration of other options?
- Action – what action is required to implement the decision, by whom and by when?
- Date and time – the decision was made.

Further information on decision logs can be found in Chapter 6 Data Handling.

4.3.8 Decision-making: support, skills, and resources

In many incidents there will not be a need, or any time, for formal arrangements to be set up to support decision makers. But some incidents will be highly complex and strategically significant, involve considerable levels of uncertainty, have hard-to-predict consequences and unclear choices. In these circumstances, it will be necessary to implement pre-established arrangements to manage information and support multi-agency decision-making at tactical and strategic levels.

Regulations are in place about the sharing of data; however, this should not prevent responders sharing relevant information to save lives and reduce harm.

Source: JESIP Joint Doctrine: The Interoperability Framework, Edition Three, October 2021.

Assessing the information received, using proven criteria, will establish its quality and suitability for the task in hand. This is critical to ensure that decision-making is based on the best possible information and to identify where critical uncertainties lie. In an emergency or crisis, much of the information decision makers receive will be unreliable or of uncertain quality. There are many ways in which responder organisations can assess information. If agencies use the same information assessment framework, interoperability will be enhanced.

As a minimum, information should be assessed for:

- Relevance: In the current situation, how well does the information meet the needs of the end user?
- Accuracy: How well does the information reflect the underlying reality?
- Timeliness: How current is the information?
- Source reliability: Does previous experience of this source indicate the likely quality of the information?
- Credibility: Is the information supported or contradicted by other information?

If decision makers are concerned or dissatisfied with the information assessment, they should issue clear direction and take steps to update, reconcile and check the information, or to seek further information, potentially drawing on other channels and sources. The behaviour of individuals and teams, and the effectiveness of interaction, will either enable or impede them in developing shared situational awareness.

Achieving shared situational awareness is more likely if people:

- Freely share what they know.
- Make uncertainties and assumptions absolutely clear.
- Challenge their own understanding of what they are being told and challenge the understanding of others.
- Are critical and rigorous.
- Feel comfortable to do the above and are trained and exercised appropriately to do so.
- Accept that they cannot know every infinite detail.

An organisation responding to a crisis or incident should:

- Gather relevant information about the incident.
- Evaluate that information in terms of quality and relevance.
- Filter, analyse and make sense of that information.
- Communicate the information inside their organisation and inform other relevant organisations.
- Present the information to decision makers in an appropriate form.

4.3.8.1 Common information sharing platform

A common information sharing platform is the means to share and manage information collaboratively to support joint decision-making. Any commonly understood, effective system can be described as a common information sharing platform. These are further enhanced where organisations have in place agreements to use such platforms.

There are considerable advantages to using an electronic system. For example, automating aspects of sourcing, combining, analysing, and displaying data will be much more useful and efficient for those using the data collected.

Further information on decision logs can be found in Chapter 6 Data Handling.

The precise form of a common information sharing platform will reflect local requirements and existing capabilities, JESIP advises that responder organisations should consider ResilienceDirect™, a widely used

and secure platform with a range of functions to support joint working. ResilienceDirect™ is provided to all responder organisations by the government. Consideration should be given to organisations that are unable to access the required information on ResilienceDirect, by using alternative ways to share common information with them.

4.3.8.2 Multi-Agency Information Cell

It is critical on the build up to and during an incident that decision makers know what is happening and have one source of information to work with. Having the same 'picture' allows shared situational awareness in a complex and ever-changing incident. Partners should be willing to share information during an incident, using a principle of sharing by default rather than restricting by default. Information can be shared between partners up to Official Sensitive using Resilience Direct [15].

The Multi-Agency Information Cell (MAIC), which can be a physical or virtual cell, can provide that capability, across tactical and strategic levels, for all organisations involved in the incident. The purpose of the MAIC is to provide situational awareness by gathering information, analysing, and then delivering it in an intelligible and recognised product, or COP. It is essential that the COP is made as widely available as possible to those involved in the Incident and especially the SCGs and TCGs. Collating and sharing any product in the most timely and efficient method is key to ensuring a successful outcome for the MAIC.

Setting up a function to gather information from partners is essential; this should be scheduled to happen prior to the meeting of a co-ordinating group. All relevant information from each individual organisation should be used to build brief and concise reports that highlight issues and progress. Reporting into a MAIC should be kept simple, highlighting the level of readiness or ability to respond to allow briefings to focus on the priorities. This should be achieved by using a 'red, amber, green' (RAG) status approach. The RAG status is an honest and defensible appraisal of three dimensions of the emergency:

- The situation
- The response to it
- Foreseeable developments

The three dimensions are separated but are combined into a single indicator, and in the absence of a prescribed method of doing so, the RAG status will reflect the collective judgement of the organisation. This will be reflected in the situation report for the SCG.

Indicators of the three levels are defined as follows:

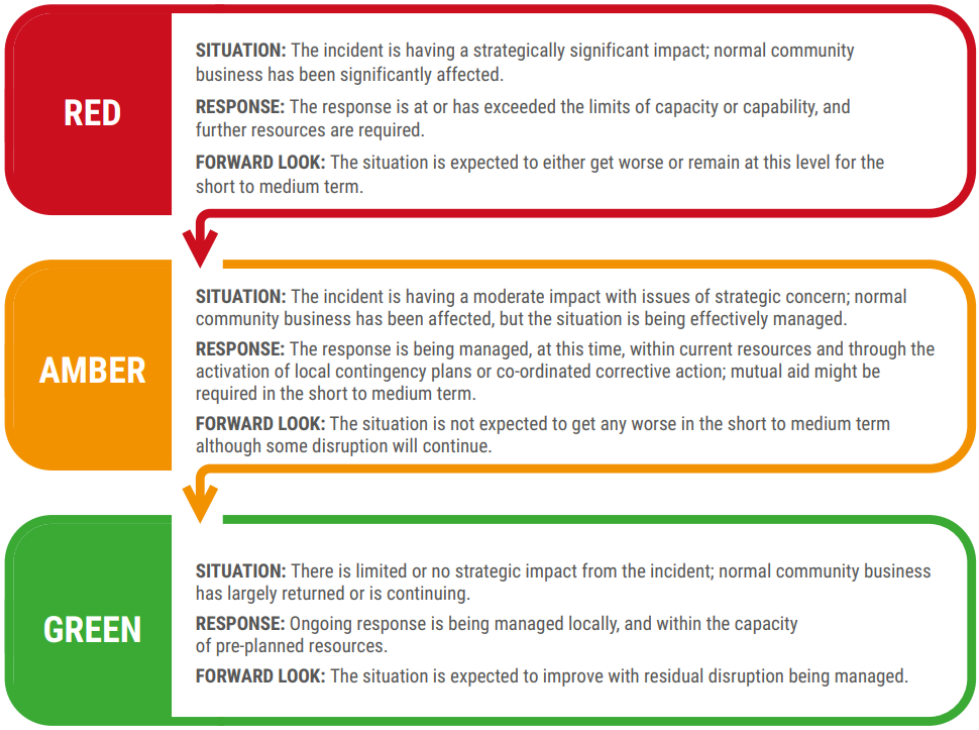

Figure 14 RAG status approach

The MAIC should gather all individual submissions and create one SITREP;

this will become the COP. The ResilienceDirect™ platform provides a response function well-suited to managing reporting, and using standardised templates, which can be very effective for sharing information to many users at the same time. The MAIC should be flexible and scalable particularly for protracted incidents, such as the COVID-19 pandemic, or high-impact spontaneous incidents, such as major flooding.

4.3.9 Common Operating Picture (COP)

Shared situational awareness is a common understanding of the circumstances, immediate consequences, and implications of the emergency, along with an appreciation of the available capabilities and the priorities of the responder organisations. Achieving shared situational awareness is essential for effective interoperability.

A COP has been defined as a common overview of an incident that is created by assessing and fusing information from multiple sources, and is shared between appropriate command, control, and co-ordinating groups to support joint decision-making. The form of the COP will differ between areas, but it should provide an overview of the incident which is accessible through a suitably resilient and secure common information sharing platform. In the early stages of an incident a situation report (SITREP) may form the totality of a COP, but as further information becomes available the COP will develop as a dynamic dashboard, or common reference point, and may include graphics, maps, and contextual information. The COP is a continuously evolving but common point of reference that includes a summary of:

- What is happening now and what is being done about it?
- So what does all of that mean and what effects will it have?
- What might happen next or in the future?

There is no set format for the COP, which will reflect local requirements and practices, but whatever is developed should be user friendly and easy to navigate and geared to the requirements of busy decision makers who are under pressure.

Establishing shared situational awareness is important for developing a COP at all levels of command, between incident commanders and between control rooms. Communications between control rooms greatly assists the creation of shared situational awareness in the initial stages and throughout the incident. Talking to commanders before they arrive on-scene and throughout the incident, will contribute to shared situational awareness. The process should include identifying risks and hazards to all responders.

Discussion between control rooms should be frequent and cover the following key points:

- Is it clear who the lead organisation is at this point? If so, who is it?
- What information and intelligence does each organisation hold at this point?
- What hazards and risks are known by each organisation at this point?
- What assets have been, or are being, deployed at this point and why?
- How will the required agencies continue communicating with each other?
- At what point will multi-agency interoperable voice communications be required, and how will it be achieved?

Whenever possible, control rooms should use electronic data transfer to share information (e.g., M/ETHANE). This can reduce congestion on voice channels, prevent misunderstandings and eliminate ‘double keying’ information. Direct data transfer does not, however, remove the need to establish early dialogue between control room supervisors to achieve shared situational awareness. As an incident progresses, consideration should be given to ensuring that all responder organisations who are appropriate to the incident are included within the command-and-control processes, especially command meetings.

Source: JESIP Joint Doctrine: The Interoperability Framework, Edition Three, October 2021.

4.3.10 Communication and Coordination

Communication links start from the time of the first call or contact, instigating communication between command levels and control rooms as soon as possible to start the process of sharing information The ‘talk not tell’ process involves control room personnel passing information and asking other organisations what their response to the incident will be. This is achieved by:

- Sharing information from all available sources along with immediate resource availability and decisions taken in accordance with each organisation’s policies and procedures.
- Nominating a point of contact in each control room and establishing a method of communication between all of them; this should be achieved by using the most appropriate form of communication,

for example the Emergency Services Inter Control (ESICTRL) Talkgroup.
- Co-ordinating the setting up of multi-agency interoperable voice communications for responders and operational working if necessary.

Sharing information in a way that can be understood by the intended recipient aids the development of shared situational awareness, which underpins the best possible outcomes of an incident.

The following supports successful communication between responders and responder organisations:

- Exchanging reliable and accurate information, such as critical information about hazards, risks, and threats.
- Ensuring the information shared is free from abbreviations and other potential sources of confusion.
- Understanding of the responsibilities, capabilities, and limitations of each of the responder organisations involved.
- Clarifying that information shared, including terminology and symbols, is understood, and agreed by all involved in the response at multi-agency incidents, responders may use interoperability ‘talk groups’, which are held by the emergency services. The use of these ‘talk groups’ are usually assigned to key roles, for example, incident commanders. Where appropriate, Defence responders and other non-blue light agencies involved should be included.

For effective co-ordination, one organisation generally needs to take a lead role. To decide who the lead should be, factors such as the phase of the incident, the need for specialist capabilities and investigation, during both the response and recovery phases, should be considered. There is specific guidance for some types of incidents, highlighting which organisation should take the lead role, such as Cabinet Office: The Lead Responder Protocol (2011). The decision on who takes the lead role should be recorded, as should any changes to the lead organisation as the incident develops.

The lead organisation should chair and set the frequency of future meetings. If military assistance is required, Defence will assume a supporting role. At all levels, when deployed in support of the civil authorities, Defence personnel will be responsible for identifying themselves at the earliest opportunity to the senior civil authority commander or co-ordinator and should establish effective co-ordination with them to ensure tasks are allocated appropriately.

Source: JESIP Joint Doctrine: The Interoperability Framework, Edition Three, October 2021 & Cabinet Office: The Lead Responder Protocol.

5 Responder Requirements

5.1 Overview

5.1.1 Civil Contingencies Act (CCA)

Emergency response and recovery are not duties under the CCA. Expectations on Category 1 and 2 responders are not mandatory. However, the CCA is intended to ensure better preparedness and enable more effective response and recovery.

Responders should view the Act in the wider context of IEM. Expectation on Category 1 and 2 responders is based on the non-statutory Emergency Response and Recovery guidance, which focuses on practical arrangements, operational doctrine, information, and guidance found on the UK resilience section of the Cabinet Office website. Expectations are based around 10 guiding principles (see Section 3.3.1):

- Anticipation (Section 3.3.1.1)
- Preparedness (Section 3.3.1.2)
- Subsidiarity (Section 3.3.1.3)
- Direction (Section 3.3.1.4)
- Information Management (Section 3.3.1.5)
- Integration (Section 3.3.1.6)
- Cooperation (Section 3.3.1.7)
- Continuity (Section 3.3.1.8)

The following two principles are also considered important for emergency response and recovery:

- Sustainability – the ability to sustain the use of facilities. Equipment and staffing arrangements, which is important because emergencies sometimes require a prolonged response and / or recovery effort.
- Resilience – the ability to ensure facilities, equipment (including telecommunications) and staffing arrangements can withstand the unexpected, which is important because emergencies often lead to essential services being compromised.

Source: Expectation_and_Indicators_of_Good_Practice_Set_for_category_1_2_Responders.pdf (publishing.service.gov.uk)

See Section 5.5.1 for further guidance on expectations for response and recovery under the CCA.

5.1.2 Rail responsibilities under the CCA

The CCA Category 2 responders overview of sectors and emergency planning arrangements are provided at in the Civil Contingencies Act – Category 2 Responders: overview of sectors and emergency planning arrangements – GOV.UK (www.gov.uk). This provides a portal for Category 2 sectors to pro-actively publish information regarding their respective industries to promote awareness among front-line responders.

Relevant to the Rail Industry is the ‘Introducing Rail Incident Care Teams’ documentation. This is available on the portal and details the roles and responsibilities of Incident Care Teams, including how, when and where the Incident Care Teams will function (See Section 5.5.1.2 for further information).

5.2 Multi-agency, JESIP requirements

JESIP and its models have become the standard for interoperability in the UK. JESIP is the thread amongst the UK emergency planning and response community that runs through all plans, response to, and recovery from emergencies (Figure 15). All incident phases need to consider multi-agency working, best served by following the Principles.

The JESIP *Joint Doctrine: The Interoperability Framework* sets out a standard approach to multi-agency working. Whilst the initial focus is on improving the response to major incidents, JESIP is scalable, the principles for joint working and models can be applied to any type of multi-agency incident.

Commanders should use the Joint Decision Model (JDM) (Section 4.1.7) to bring together the available information, reconcile objectives and make effective decisions together.

See Chapter 4 for guidance on JESIP, multi-agency working and interoperability in the UK. Chapter 4 includes the key components of the JESIP Joint Doctrine including:

- Principles for Joint Working
- M/ETHANE – a common method for passing incident information between services and control rooms.
- Joint Decision Model (JDM)

The structure for managing the local multi-agency response to emergencies is based on the CCA (2004). The Act is supported by two sets of guidance: Emergency Preparedness and Emergency Response and Recovery. Emergency Preparedness deals with the pre-emergency (planning) phase (see rail-specific guidance in RDG-OPS-ACOP-010 IEM, Preparation). Emergency Response and Recovery describes the multi-agency framework for responding to, and recovering from, emergencies in the UK.

Details of the operation and coordination of emergency response can be found in the Cabinet Office Concept of Operations and the relevant chapters of Emergency Response and Recovery.

The JESIP Joint Doctrine complements the Emergency Response and Recovery by focusing on the interoperability of the emergency services and other responder agencies in the response to an emergency.

See Figure 15 below for a visualisation of this documentation hierarchy.

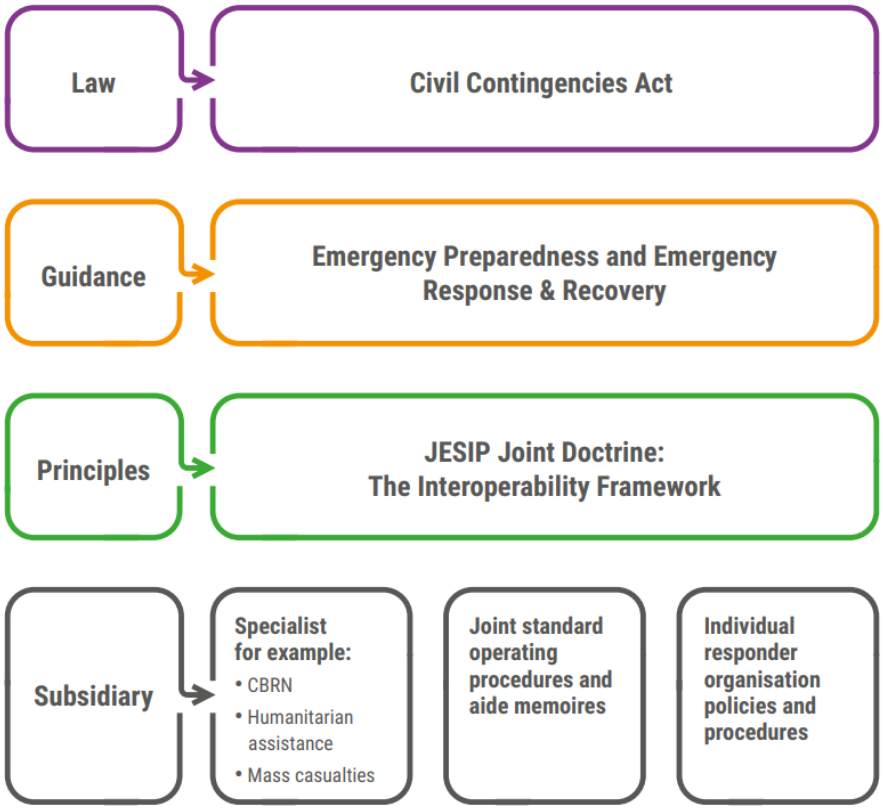

Figure 15 UK Emergency Response Documentation Hierarchy

5.3 Responder Requirements

Across the rail industry and multi-agency partners, there is the need for command and control during incident management. Each plan or set of emergency arrangements needs to have:

- A role responsible for development and delivery of the plan and emergency arrangements.
- A role accountable for the enactment of emergency arrangements.
- Roles consulted and informed, as identified in RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance provisions (Page 37).

Training and exercising of staff in their relevant command roles, whether at strategic, tactical, or operational levels internally or in a multi-agency setting, is imperative to ensure a coordinated structured response. Chapter 4 provides guidance on the command-and-control structure from JESIP recognised across multi-agency responders in the UK.

Rail-Incidents_Guidance-to-the-Emergency-Services-for-Access-to-the-Railway-Infrastructure (networkrail.co.uk) provides guidance to the emergency services for access to railway infrastructure, specific information for response to an incident on the railway, key actions, context, and terminology. This has been jointly developed by Network Rail and JESIP.

Further information on rail specific response, roles and responsibilities is found at 5.5.2.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document.

5.4 Provisions

5.4.1 Rail Entities ***MUST*** cooperate with all Category 1 agencies involved in responding to emergencies. [1]

5.4.2 Rail Entities ***MUST*** cooperate with all Category 2 agencies involved in responding to emergencies. [1]

5.4.3 Rail Entities ***MUST*** cooperate with agencies within the wider resilience community who may be involved in responding to emergencies. [1]

5.4.4 Rail Entities ***MUST*** ensure any response follows emergency plans whereby arrangements specify to provide permitted inspectors (RAIB) access to the incident site and instruction that no evidence shall be removed (except in very limited exceptions and having notified the RAIB. [6]

5.4.5 Rail Entities ***SHOULD*** assist category 1 responders in making arrangements to warn and communicate with the public to ensure that they are made aware of emergencies. The public ***SHOULD*** be provided with information and advice, as necessary, if an emergency is likely to occur or has occurred. [7]

5.4.6 Rail Entities' Strategic Commanders ***SHOULD*** adopt the following behaviours set out in RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers:

- Be strategic – the Strategic Commander should seek to ensure that neither they, nor other members of the Crisis Management Team succumb to the temptation to actively involve themselves in providing the detailed response.
- Be positive.
- Be active.
- Be reassuring.
- Be apologetic – it is important to say you are sorry (noting that this is not the same as accepting responsibility).
- Be visible, e.g., visit hospitals, emergency assistance centres, staff areas and the incident site as appropriate.[8]

5.4.7 Rail Entities' Strategic Commanders ***SHOULD*** either complete the actions (set out in RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers, and Section 5.5.3) themselves or else satisfy themselves that they have been completed, during an emergency response. [8]

5.4.8 Rail Entities' Primary Support Operators ***SHOULD*** complete the actions set out in RDG-ACOP-016 Incident Response Duties of Primary Support Officers during an emergency response. [11]

5.4.9 All Rail Entity responders ***SHOULD*** utilise guidance for response roles and responsibilities and actions and tasks during an emergency response within relevant the guidance notes. (Such as RDG-ACOP-016 Incident Response Duties of Primary Support Officers, RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers, RDG-OPS-GN-034 RDG Guidance Note: Logging

and Loggists, RDG Guidance Note RDG-GN016 – Competence of Train Operator Liaison Officers and RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident).[8,10,11,16]

5.4.10 Rail Entities ***SHOULD*** maintain response arrangements for extreme weather events and consult RDG-OPS-GN-015 Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems for actions during the response. [9]

5.4.11 During periods of extreme hot weather, Rail Entities ***SHOULD*** seek to maintain acceptable station and train environments. See guidance at RDG-OPS-GN-015 Extreme Weather Arrangements for considerations. [9]

5.4.12 Each Rail Entity ***SHOULD*** define who has responsibility for declaring a Major Incident or Critical Incident for rail industry response.[16]

5.4.13 The Owning Operator of the train involved in an emergency ***SHOULD*** assume immediate responsibility for leading and managing the humanitarian assistance response. [16]

5.4.14 Where trains of two or more Rail entities are involved in an emergency, the Rail entities concerned ***SHOULD*** agree which will provide the overall leadership and management of the combined humanitarian assistance response - normally this will be the Rail entity whose passengers are perceived as likely to have suffered the greatest number of casualties. [16]

5.4.15 The identity of the Rail entity leading and managing the humanitarian assistance response ***SHOULD*** be advised to Network Rail Route Control immediately. [16]

5.4.16 Following a Major Passenger Rail Incident, actions listed in Appendix C of RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident ***SHOULD*** be considered as it provides a simple checklist of requirements. [16]

5.4.17 Network Rail Managed Stations ***SHOULD*** provide Rail entities which operate within the station concerned with copies of current emergency plans and any proposed changes to these plans. [16]

5.4.18 In the event of an incident occurring at or near a large, multiple operator station, the Station Incident Officer ***SHOULD*** immediately call together the operator's representatives and provide accommodation, facilities and staff as agreed to operate RDG-OPS-ACOP-001. [16]

5.4.19 Smaller Rail entities ***SHOULD*** ensure that they are able to provide overall response leadership / management and therefore, as a minimum, maintain 2 - 3 persons who have sufficient understanding of the role of the ICT and how it will be deployed and are able to provide strategic direction to the Deployment Manager. [16]

5.4.20 Rail entities ***SHOULD*** hold details of ICT members centrally and ensure that these can be made quickly available within their own, and to other Rail entities in the event of an incident to supplement On Call arrangements. [16]

5.4.21 A Train Operator Liaison Officer (TOLO), reporting initially to and maintaining liaison with the Rail Incident Officer (RIO), ***SHOULD*** be appointed at the incident site by the Primary Support Operator. [16]

5.4.22 The ICT Strategic Lead and the ICT Deployment Manager ***SHOULD*** liaise to identify which of the following roles are necessary and ensure staff with competence as ICT members are nominated to undertake these roles: [16]

- At the Casualty Bureau - a Rail entity representative with an understanding of the role and capabilities of the ICT and a general railway knowledge.
- At a hospital - a Rail entity representative to provide a single point of contact between the hospital authorities.
- At a Survivor Reception Centre - Survivor Reception Centre Liaison lead
- At a nominated station(s) or other location - Humanitarian Assistance lead
- At a Family & Friends Reception Centre – Family & Friends Reception Centre Liaison lead.
- At a Humanitarian Assistance Centre - Humanitarian Assistance Centre Liaison lead.
- With Local Authorities - A Local Authority Liaison lead. [16]

5.4.23 Rail entities ***SHOULD*** ensure records are maintained to ensure that proper care and post-incident follow-up takes place as well as ensuring prevention against false claims. It is strongly recommended that this be done by means of a database system which complies with the requirements set out in the specification produced by RDG - Incident Care Team Survivor Relationship Management (SRM) System Requirements Specification, v1.1 dated 16 September 2019). [16]

5.4.24 The capturing, recording and retention of personal data by Rail entities ***MUST*** comply with current GDPR (General Data Protection Regulation requirements) guidance on how this should be approached within the context of ICT deployment is provided in RDG-OPS-GN-038 Data Protection Requirements During and After Incidents. [16]

5.4.25 An accurate log ***SHOULD*** be maintained of all activities undertaken as part of the humanitarian assistance response to an emergency. [16]

5.4.26 No employee, visitor or contractor on site ***SHOULD*** respond to an emergency by taking actions for which the individual is not trained or qualified which puts the individual or others at risk. [13]

5.4.27 Rail Entities ***COULD*** appoint a liaison with the task of transmitting information and facilitating communication between separated teams. [13]

5.4.28 Rail Entities ***SHOULD*** select team leaders with training experience and knowledge of the emergency procedures and forms. [13]

5.4.29 Responders ***SHOULD*** be briefed by the emergency preparedness and response plan coordinator on the assessment needs, response strategy and procedures, priorities to be observed and safety issues. [13]

5.4.30 Appropriate personal protective equipment ***SHOULD*** be distributed according to the context of the response required. [13]

5.4.31 Periodic breaks during the response ***SHOULD*** be established and enforced. [13]

5.4.32 Reporting procedures to the response command staff ***SHOULD*** be specified. [13]

5.4.33 In the early stage of an emergency, timely and accurate information ***SHOULD*** be provided for effective decision-making. [13]

5.4.34 Where there are no identified priorities in an affected area, decisions about what to retrieve or protect in situ ***SHOULD*** be made by assessing which items are most at risk of damage or which require stabilisation most urgently. [13]

5.4.35 The incident classification ***SHOULD*** be made by the first responder(s) to the incident or by those personnel most familiar with what has happened in discussions with first responders and/or the incident coordinator. [13]

5.4.36 Response ***SHOULD*** be guided by the response plan, ensuring that the plan is applicable to the on-going situation. [13]

5.4.37 A comprehensive record ***SHOULD*** be kept of all events, decisions, reasoning behind key decisions and actions taken. A daily log ***SHOULD*** be kept in a chronological order. [13]

5.4.38 Facilities on site where people can be held and/or treated for a few hours ***SHOULD*** be considered for no-notice events when [13]:

- There is no time to evacuate before the hazard occurs.
- Moving people would expose them to greater harm or dangerous conditions.
- Immediate risk is unclear.

5.5 Guidance Notes

5.5.1 Civil Contingencies Act 2004

Since emergency response and recovery are not duties for Category 2 responders under the Act, excepting communication and cooperation, the expectations outlined in this section are not mandatory. Expectations outlined in this section represent a list of practical considerations which should be thoroughly acted on if emergency response and recovery is to be effective. See Expectation and Indicators of Good Practice Set for Category 1 & 2 Responders.pdf (publishing.service.gov.uk) for further detail. Whilst there are no legal duties to respond, there is a moral obligation to do so.

It should be noted that whilst some of the duties and expectations below are of Category 1 responders only:

"Cooperation for Category 2 responders includes looking at how delivery of the emergency duties under their own legislation, such as risk assessment, emergency planning and exercising, can most easily match with the similar CCA duties of the Category 1 responders. Category 2 responders need to be fully integrated into multi-agency planning at all levels including cooperation with each other where it helps local level preparedness by the Category 1 responders."

(CCA Enhancement Programme, Chapter 2).

5.5.1.1 Anticipation

i. Continuing to assess and manage risk during any emergencies that occur – this assessment should assist rather than obstruct effective operations. The assessment should therefore provide an analysis of, and possible solutions to, anticipated problems before they arise. All emergencies have disparate direct and indirect impacts that may not be immediately apparent amidst the pressure, uncertainties, and demanding circumstances of emergencies. Risks are dynamic and, during emergencies, new risks emerge, established risk recedes and the balance between risks changes. (Category 1 responders only).

5.5.1.2 Preparedness

i. Ensuring emergency plans include appendices that cover the following considerations:

- Proposed locations or plans for providing primary and back-up locations for strategic, tactical, and operational response.
- Who is required and secretariat support arrangements for strategic operational functions.
- A protocol for dealing with sensitive information (see Chapter 6 Data Handling).
- Telecommunications plan.

ii. Carefully considering roles and responsibilities for each level of response (i.e., strategic, tactical, and operational) and for single and multi-agency coordination groups. At the strategic and tactical levels, staff should be adequately senior and experienced to be able to make decisions. At the operational level, staff should be adequately skilled to provide the service or response required. The Cabinet Office website provides further guidance on the roles and responsibilities of the main responding agencies and sectors that are likely to become engaged in the response to emergencies. Details of agencies and sectors likely to become involved in recovery can be found in the National Recovery Guidance, Recovery Plan Guidance Template.

iii. Having recovery plans in place, which cover all the aspects highlighted above. Recovery Coordinating Groups (RCGs) are the equivalent of Strategic Coordination Groups and will need to operate in parallel to the SCG, until the SCG stands down and responsibility is transferred to the RCG. Having a sign-off certificate for this transfer in responsibility is highlighted as an example of good practice in the National Recovery Guidance. This guidance provides further details on, and some templates for, the recovery planning process.

iv. Having plans in place for setting up, activating, and accommodating a Science and Technical Advice Cell (STAC) if the nature of the emergency requires it. These plans should cover who would need to be involved, roles and responsibilities, any equipment requirements, where and how it will be accommodated within the Strategic Coordination Centre (SCC) and how it will be activated. See Provision of Scientific and Technical Advice in the Strategic Coordination Centre – Guidance to local responders for further information.

v. Complying with other statutory regimes in the field of civil protection (as required). A particular set of risks is excluded from the CCA regime because they are covered by other legislation. These are:

- The Control of Major Accidents Hazards (COMAH) regulations 1999.
- The Pipeline Safety Regulations 1996.
- The Radiation (Emergency Preparedness and Public Information) Regulations 2001. (For details see www.statuelaw.gov.uk).

vi. Having a clear, well tried, and robust process for:

- Getting facilities up and running.
- Setting up meetings.
- Contacting on-call staff.
- Briefing staff.

vii. Ideally this should include crisis coordination arrangements that are consistent with those used in other areas.

viii. Setting activation targets for facilities. In setting these targets, it should be clearly defined what is considered 'activated'. Activation targets set should be coherent with those of other responders at local and (if relevant) a national level.

ix. Ensuring that the SCC can support and accommodate a Government Liaison Team (GLT) if necessary. Rail Entities should support these requirements.

x. Having integrated and resilient telecommunications and IT equipment within the organisation and the response and recovery facilities. This should enable Rail Entities to:

- Share data (e.g., computers with network access links, extranet, networked printers, email) within your organisation and with partners.
- Communicate with on-call staff (e.g., mobiles, pagers, landline)
- Communicate with the central and regional tiers (e.g., video conference and teleconference links, email)
- Communicate with relevant stakeholders.

xi. Having additional security controls for any dedicated high security telecommunication rooms (see Section 8.2 of the Appendices for guidance on Security Control Rooms and Crisis Management Suites).

xii. Developing a training programme for staff that will play a role in response and/or recovery which will ensure that they are adequately trained for proposed roles. Training might include:

- Familiarising staff with the community risk register and emergency plans
- Familiarising staff with their proposed roles during response and recovery
- Logistical planning capabilities
- Leadership skills for those chairing meetings
- Familiarisation with how to use telecommunications equipment such as Satellite and Airwave technology.

xiii. Checking that all equipment within response and recovery facilities works. This can be achieved through frequent exercises based in the various facilities or by using these facilities for other purposes during normal working. Recording any faults that are identified and taking and recording actions to rectify them.

xiv. Ensuring that strategic, tactical, and operational facilities are accessible to the on-call staff that will be deployed there.

xv. Identifying any capability gaps within the organisation that will result in an inability to treat risks identified in the risk assessment and devising an action plan to fill these gaps where possible. This might include training, recruitment, and/or mutual aid agreements. (Category 1 responders only).

See RDG-OPS-ACOP-010 IEM, Preparation for further information on preparedness.

5.5.1.3 Subsidiarity

i. Being aware of and respecting the concepts set in: Central Government Arrangements for responding to an Emergency - Concept of Operation (CONOPS). (Category 1 and 2 responders).

5.5.1.4 Direction

i. Being aware of Central Government Arrangements for Responding to an Emergency – Concept of Operations (CONOPS).

ii. Being familiar with strategic aims in relation to sudden impact emergencies, slow-onset emergencies and in relation to the media.

iii. Being aware of the responsibilities, capabilities, and priorities of other category 1 and 2 responders, especially those within the same local resilience area. (Category 1 and 2 responders).

5.5.1.5 Information management

i. Complying with the information sharing, provisions during response and recovery operations as well as during normal times.

ii. Having a protocol for managing and presenting information which:

- Is easy to use.
- Tracks incident and resources to provide a strategic picture.
- Is standardised and consistent.
- Which ensures public safety is considered.

iii. Use appropriate nationally produced templates, as a guide, if they are provided.

iv. Being aware of who to contact at each different tier, including communicating with the regional and the national tier (via the regional tier) in accordance with communication plans. (Category 1 and 2 responders).

5.5.1.6 Cooperation

i. Complying with the cooperation provisions in the Contingency Planning Regulations during response and recovery operations as well as during peacetime.

ii. Understanding the functions, ways of working and priorities of partners. This will help facilitate the genuine dialogue that is essential to establishing shared aims and objectives.

iii. Being open and honest with partners and dealing with sensitive information appropriately. See Data Protection and Sharing – Guidance for Emergency Planners and Responders and Security vetting and protective markings: a guide for responders for further guidance. (Category 1 and 2 Responders).

Further information on Data Handling can be found in Chapter 6.

5.5.1.7 Integration

i. Understanding and having respect for the subsidiarity principle. Being familiar with how the different tiers will liaise. Being aware of the role of the national tier and being clear in what circumstances their assistance is required. (Category 1 and 2 Responders)

5.5.1.8 Continuity

i. Proposing roles and responsibilities for staff during emergency response and recovery that are not dramatically different to their day-to-day roles.

ii. Ensuring that new staff are properly inducted so that they are familiar with normal ways of working.

iii. Ensuring awareness of response and recovery procedures used by other responders.

iv. Ensuring awareness of the role of the national tier and how the organisation fits into response and recovery arrangements. (Category 1 Responders only).

v. Ensuring awareness of response and recovery procedures.

vi. Ensuring that where involvement in emergency response and recovery is required, staff whose day-to-day role is not dramatically different to the role that is required of them are sent. (Category 2 Responders only).

5.5.1.9 Resilience

i. Enhancing the resilience of everyday commercially available telecommunications. Ideally having the ability to implement telecommunication systems that are resilient against loss of the Public Switched Telephone Network (PSTN) (for instance BT or equivalent) and to the loss of the Wide Area Network (WAN) for up to 5 hours. This can be achieved by:

- Understanding the systems available and their respective strengths and weaknesses.
- Identifying and reviewing the critical communication activities that underpin response arrangements - critical activities are those that are essential to the effectiveness of response arrangements.
- Avoiding reliance on any one telecommunications system as this carries a significant inherent risk.
- Adopting layered fall-back arrangements in order to help mitigate unavailability. A fall-back system does not have to provide the same 'richness' of communication and the primary option. ‘Ensuring Resilient Telecommunications: A Survey of some Technical Solutions’, provides guidance.
- Planning for appropriate interoperability to enable seamless communications between different telecommunications systems. This is especially important for point-to-multipoint communications.
- Agreeing and adhering to communication protocols and procedures. This may take the form of call-signs and radio discipline (particularly for mobile radio communications) or procedures for managing conference calls.
- Following advice from the National Protective Security Authority (NPSA) (formerly the Centre for the Protection of National Infrastructure (CPNI)) on data security.

ii. Local Risk Assessment Guidance (LRAG) and National Resilience Planning Assumptions provide details on the risk that we face nationally regarding the loss of telecommunication systems.

iii. Where appropriate, adopting the good practice examples set out in Good Practice Guide to Telecommunications Resilience. Telecommunications.

iv. Improving the management, take-up and resilience of privileged telecommunications schemes that are accessible only to emergency responders. The schemes are:

- Privileged access to the fixed-line telephone system.
- Privileged access to mobile telephone networks.
- Access by those outside the Emergency Services to mobile communications using Airwave.
- Commercially available satellite communications equipment made available to responders through a centrally negotiated catalogue.

v. Implementing multi-agency private networks at a local level.

vi. Collaborating with other responders, setting up mutual aid agreements, and ensuring interoperability between the different telecommunication systems used.

vii. Participate in your Local Area Telecommunications Sub-Group (TSG). The Chair or point of contact for all TSGs can be found in the TSG Contact Directory.

viii. Having dedicated & separate telecommunications equipment – that is telephone private branch exchanges for the communication room in tactical and strategic facilities.

ix. Ensuring that, where possible, primary and back-up facilities are located in areas that are at minimal risk from high-risk hazards (for instance flooding).

x. Having back-up power systems. This could include:
- Having a backup generator – To be High Integrity Telecommunication Systems compliant, you should have sufficient fuel available for on-site generators for 10 days full-load use. These generators should cover all critical functions.
- Using an uninterruptible power supply (UPS) which ensures a smooth and constant transfer of power to IT equipment, preventing damage resulting from power surges and/or restarts.

xi. Having arrangements or a plan in place for water and sewerage systems failure at your response and recovery facilities. To be High Integrity Telecommunication Systems compliant, you should have sufficient water supplies for 3 days and be able to cope for 3 days without water services.

xii. Backing up all critical data and securely storing at least one back-up copy of all information off-site of operational facilities.

xiii. Ensuring that staffing arrangements for emergency response and recovery do not rely on particular individuals and include suitable arrangements for deputising.

xiv. Having succession plans in place for the loss of key staff. (Category 1 responders only)

Further information on resilient communications can be found in RDG-OPS-ACOP-010 IEM, Preparation.

5.5.1.10 Sustainability

i. Setting sustainability targets for facilities. These should relate to the period of time to be able to:
- Sustain 24/7 working arrangement; and
- Sustain extended working hours arrangements.

You should ensure that the sustainability targets set are coherent with those of other responders at local, regional, and national level. Augmenting staff rotas to reduce the burden on individuals and avoid burn-out. Having clearly defined staff change-over procedures. Considering the heating, eating, and sleeping arrangements for staff during emergency response and recovery. (In most cases, staff are likely to return to their own homes to sleep at the end of their shift. However, in some instances, this may not be possible). (Category 1 responders only).

Source: Expectation and Indicators of Good Practice Set for Category 1 & 2 Responders.pdf (publishing.service.gov.uk)

5.5.2 Rail Responsibilities under the CCA

Rail companies are well placed to support the humanitarian response provided to those individuals unfortunate enough to have been involved in or directly affected by major rail related incidents. Key to this are the Rail Incident Care Teams (ICT).

A rail ICT is a team of specially selected volunteers who are trained in how to respond to the needs of survivors in the hours and days immediately following any event requiring a humanitarian response and who would be activated accordingly. There are team members across the country who have received specialist training, refresher training and have taken part in exercises validating this training and response plans. ICTs are deployed to any rail related event where some form of humanitarian assistance is needed. Rail ICTs will work alongside and complement other responding agencies.

At the operational level, Team members will usually be working with a colleague or colleagues depending on the numbers required to provide support and assistance to the injured and their families. The intention is that they will make early contact with and work particularly closely with Police Family Liaison Officers and designated hospital contacts. The need to provide mutual support throughout the rail industry is central to the concept of Care Teams. Thus, the response to a single incident might, depending on its nature, scale, and location, directly involve Care Teams drawn from a number of individual Train Operating Companies but functioning as a single team. When deployed, Team members will display a distinctive photo-id card which identifies them not only as able to assist and support survivors but also as competent to do so, issue of the card being dependent on successful completion of the training course.

The help offered to those directly involved and their friends/relatives is focused on the practical and will typically

include the following:

- Acting as an enabler, facilitator, 'empowerer' and 'servant' for survivors
- Providing information concerning the incident
- Providing information regarding supporting agencies to enable them to make decisions about what help and advice they might need.
- Offering practical and emotional support to victims
- Communication support (e.g., internet access, phone calls, etc.)
- Arranging (and paying for) accommodation
- Arranging (and paying for) travel
- Arranging (and paying for) food
- Arranging (and paying for) replacement of lost or damaged clothes, personal items, and other essential belongings
- Arranging (and paying for) repatriation of bodies
- Working with local authorities/social services to arrange childcare, care of pets, etc.
- Assisting the Police in the return of personal effects
- Attending funeral and/or memorial services – but only if requested by family members.
- In general, responding to any other needs and concerns survivors may have and attempting to help wherever possible.

Rail Incident Care Team members will NOT provide specific counselling services (though they would be in a position to put survivors in touch with the appropriate specialist agencies).

Source: ATOC Rail Incident Care Teams, November 2006.

5.5.3 Responder Requirements, Roles, and Responsibilities

Across the rail industry and across multi-agency partners there is the need for command and control during incident management. Each plan or set of emergency arrangements needs to have; a role responsible for development and delivery of the plan and emergency arrangements, a role accountable for the enactment of emergency arrangements, and roles consulted and informed, as identified in RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance provisions (Page 37). There are a number of Guidance Notes detailing responding roles and responsibilities, some are outlined below. Those shown here are not exhaustive.

The following actions and tasks are taken from *RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers*.

5.5.3.1 Strategic Commander Role

It is vital that those who might be called on to lead the response to Major Incidents on behalf of their organisations are given appropriate training – both initial and on-going – for their role. They should also be subject to periodic assessments of their continuing competence for the role, undertaken by an appropriate agency.

One or more deputies should also be appointed to provide cover in the event of the non-availability of the person identified to take on the Strategic Commander role. They should be subject to identical training and competence assessment requirements. It is important that there is absolute clarity of who is in the lead at all times.

Senior managers should remember that in many cases the rail industry will not be managing the "emergency" itself – this is the responsibility of the emergency services – but will be managing the consequences of the incident. These will often be felt over a wide area away from the actual scene of the incident.

The Strategic Commander should either complete the following actions themselves or else satisfy themselves that they have been completed:

- Ensure the company emergency plan has been activated.
- Provide notification of the event to the Managing Director (if not the Strategic Commander), other Directors, HR On Call and parent company, also other key contacts as per the emergency plan.
- Establish a senior level Crisis Management Team and confirm its location.
- Identify immediate objectives and priorities based on review of circumstances.
- Identify and anticipate issues.
- Identify decisions that need to be taken and when.

- Identify where authority for these decisions lies and whether authority needs to be delegated to facilitate a timely response.
- Establish roles and priority actions for each Directorate.
- Provide strategic advice to company on call personnel and Duty Control Manager.
- Consider need for company representation at incident site and/or other key locations (such as major stations).
- Identify and assess the implications for the business at a corporate level and initiate measures to deal with these. This includes considering political, reputational, legal, and financial aspects as well as the media strategy.
- Consider the need to call in external resources/advisers such as disaster management and/or reputation management experts and legal support.

In larger incidents it may be beneficial to appoint a 'Chief of Staff' to support the Strategic Commander and Crisis Management Team. The role of this individual is to:

- Coordinate the activities of the team supporting the Strategic Commander.
- Act a trusted advisor or 'conscience' to the Strategic Commander concerning important decisions.
- Chair teleconferences or meetings, thus allowing the Strategic Commander to concentrate on decision making.
- Act as a 'Gate Keeper' to the Strategic Commander protecting that individual from distractions.
- Coordinate the gathering and collation of information in order to enable the Strategic
- Commander to obtain and maintain 'situational awareness' in order to drive effective decision making.

The role of Chief of Staff requires careful consideration and specific training and experience. Where possible, this person should have extensive incident command experience in their own right and be known and trusted by the Strategic Commander.

The Strategic Commander should either complete the following themselves or else satisfy themselves that they have been completed:

- Confirm notification/activation of key roles.
- Confirm appointment of Train Operator Liaison Officer (TOLO) /Station Incident Officer, that they have been assessed as suitable for the role (in light of the scale of the incident) and that resources have been deployed as necessary to assist them.

In relation to SCGs, Rail Strategic Commanders should:

- Ascertain whether such a group has been established.
- Obtain contact details.
- Make contact with rail industry resource on this group (this will usually be provided by Network Rail) or, failing that, the BTP resource.
- Confirm that all statutory bodies have been notified.
- Work with stakeholders and partners:
    - Network Rail.
    - BTP.
    - Local authorities.
    - Hospitals/medical authorities.
    - Other Rail entities.
    - Voluntary sector (Red Cross, Victim Support, WRVS, etc.).
    - Faith communities.
    - ORR.
    - DfT.
    - RAIB.
    - Finance: Liaise with insurance companies. If necessary, make arrangements for additional funding to support the response.
- Cooperate with lead agencies re press conferences and media holding areas.
- Set up regular review/update points and/or telephone conferences.
- Liaise with Owning Group, stakeholders, and shareholders.
- Liaise with leasing companies/train service providers.

The Strategic Commander should either complete the following actions themselves or else satisfy themselves that they have been completed:

- Appoint and empower a director / senior manager to assume responsibility for welfare of staff responding to the incident and who will:
  - Ensure that adequate arrangements are in place and are being worked to in respect of appropriate equipment and clothing, refreshments, rest periods and relief.
  - Request support from other Rail entities as necessary.
  - Initiate chain of care procedures as necessary.
  - Provide care, support and reassurance for staff involved in the incident, including their families (including protection from the media) – it may be appropriate to involve the Incident Care Team in this (see next section).
  - Resource and look after the Crisis Management Team itself.

A Director/senior manager should be appointed and empowered to direct the company humanitarian response and who will:

- Ensure that the Incident Care Team has been activated/deployed and that an ICT Deployment Manager has been appointed.
- In conjunction with the ICT Deployment Manager, request Incident Care Team support from other Rail entities as necessary.
- In conjunction with the ICT Deployment Manager, request Incident Care Team support from Kenyon1 as necessary.
- Initiate emergency finance.
- Initiate chain of care procedures as necessary.
- Liaise/agree with other responders (local authorities, police, hospitals) regarding joint strategy for provision of humanitarian assistance to those affected.

The Strategic Commander should either complete the following actions themselves or else satisfy themselves that they have been completed:

- Provide a single point of contact between the Crisis Management Team and Control.
- Confirm that effective communication between site (including TOLO) and the Crisis Management Team has been established – this may be through the Strategic Command structure.
- Provide a focus of peer group (i.e., senior level) communication within the industry/parent company, with Network Rail, other Rail entities, BTP/local police force, legal advisors, etc. and liaise/agree with them the initial line to take.
- Agree media response and who will lead, including initial holding statement.
- Appoint a director / senior manager to be available to front the media response.
- Ensure that press officers are available, including at incident site if appropriate.
- Release initial press statement.
- Establish who is scheduling the first press conference and assist/support as necessary.
- Cease inappropriate advertising (TV, radio, cinema, press, on-line, etc.).
- Start active monitoring of media and develop strategy for input and response.
- Establish who is setting-up a media call centre and assist/support as necessary.
- Update company website to acknowledge and express regret for the incident and remove other material that may be inappropriate under the circumstances. Request National Rail website to be similarly updated.
- Establish a secure website or websites to facilitate communication with staff responders, staff more generally and those passengers/members of the public involved.
- Address families/friends, media, and employees.
- Ensure a suitable internal communication strategy is set up with the HR Director to reassure staff.
- Issue briefings (separately as appropriate to media, staff, government, corporate level) covering:
  - Situation – where are we now?
  - Mission – where do we want to be?
  - Execution – how are we going to achieve this?
  - Service & Support – what resources and personnel do we have/need?
  - Command & Communications – who is in charge and what communications do we have?

The Department for Transport, and the part of it responsible for rail, i.e., Rail Group, will have an interest in any emergency with a significant impact on the railway.

5.5.3.2 Role of Rail Group in the event of a major rail incident

Rail Group's role is broadly two-fold:

- To support the railway in managing the incident and mitigating its effects on passengers and freight in a timely and effective manner.
- To support DfT and other Ministers by providing clear prompt and well-informed advice to inform their decision-making and communications on the issues affecting the railway.

A number of teams in Rail Group are likely to be involved depending on the type of event, and Rail Group will need to support and co-ordinate its efforts between them and industry. The Land Transport National Security team will be the main interface with Rail Entities, Network Rail and the BTP for security incidents, whereas in civil emergencies and the recovery phase, the Rail Resilience and Response team will lead. Railway Entities can also expect to be contacted by their franchise contract team within the Department as often this is where the closest links lie between the Department and the operator.

Rail Group provides a critical interface between the industry and Ministers and as a result effective management of communications between the rail industry and Rail Group is imperative. A Director/senior manager should be appointed to take overall responsibility for engaging with Rail Group.

5.5.3.3 Social Media

Social media is a not only a key communication medium but also a primary influence on how individuals react to, and form opinions about any particular situation or event. It follows that it is essential for Rail entities to engage with social media during Major Incidents and their aftermath and they should have mechanism and resources in place to achieve this. It does, however, need to be recognised from the outset that by its very nature, social media cannot be controlled and any attempt to do so will be at best futile and at worst serve to discredit the company.

There should be no doubt that a Major Incident will generate an overwhelming volume of social media messages. Useful pieces of information will be chaotically mixed with very large amounts of irrelevant and misleading material. However, properly understood, such messages have the potential to inform how an organisation responds. The messages can provide critical information about what is happening on the ground along with the public and political reaction and can also be used to respond to and help those affected. The success or otherwise of the organisation in managing and responding appropriately to social media is likely to be reflected in and increasingly determine the longer-term impact on company reputation.

The following are recommended as a starting point for what the Strategic Commander should either complete themselves or else satisfy themselves that they have been completed with regards to social media:

- Start active monitoring of social media and develop strategy for input and response.
- Issue appropriate messages through existing social media channels (firstly Twitter and then others such as Facebook).
- All staff should be reminded of the following basic principles when using social media, either privately/individually or on behalf of the company:
  - Breach of trust/confidence – information, including personal data, that comes into the possession of the company should be treated as confidential and not divulged publicly or to other parties without legitimate reason.
  - Bringing discredit to the company – staff should be mindful that even seemingly trivial comments about the company, management or colleagues have the potential to 'go viral' and become a focus of negative public and media focus.
  - Revealing information about internal company processes and practices – information pertaining to company operational, safety management, HR, commercial and similar arrangements should be treated as confidential and not divulged publicly or to other parties without legitimate reason.
  - All staff should be reminded that any information placed on the Internet or social media could potentially end up in the worldwide public domain and be seen or used by someone for whom it was not intended. It is likely that any information placed on the Internet or social media will be considered to be a public disclosure.

In support of the above, all staff should be advised to avoid initiating or responding to social media messages when off duty after consuming alcohol or otherwise when their judgement may be impaired.

5.5.3.4 Continued Operation

The Strategic Commander should either complete the following actions themselves or else satisfy themselves that they have been completed:

- Ensure a director is appointed to focus on the continuing operation of the rest of the business (and not on the incident).
- Monitor and address emerging staff concerns.
- Review marketing material, advertising campaigns, etc. and revise as necessary.
- Protect other staff from getting drawn into the incident, either directly or through requests for information.

The Strategic Commander should either complete the following actions themselves or else satisfy themselves that they have been completed:

- Understand the roles and likely activities of the ORR, RAIB and BTP with regard to the incident, its investigation and follow up.
- Quickly identify the parts of the business likely to be exposed to an investigation and secure copies of records for staff/vehicles involved.
- Ensure an evidence co-ordinator is appointed and related evidence is being gathered (on and off site) and secured, including:
  - Maintenance records of the train(s) involved.
  - Traincrew records (also any other staff who may be directly implicated)
  - Voice recordings
  - OTMR recordings.
- Arrange for copies of any documents given to the Police, RAIB, etc. to be made prior to handing them over.
- Liaise with RAIB.

5.5.3.5 Record Keeping and Logging

The Strategic Commander should appoint one or more competent individuals to the role of record keeper (loggist) - or else satisfy themselves that such an individual or individuals has/have been appointed.

The loggist should be tasked with ensuring that a record of all key decisions taken (or not taken), including the rationale behind the decision-making process, is kept.

Key individuals, particularly those exercising command authority, should also maintain their own personal log. This should be checked and correlate with the main record kept by the Loggist. All notes and sketches etc made at the time need to also be included with that log as party of that evidence trail which may be required later, such as during a public inquiry etc.

Further details of the loggist role and requirements can be found in RDG Guidance Note RDG-OPSGN-034 – Logging and Loggists.

5.5.3.6 Incident Response Duties of Primary Support Operators

The following guidance is from Incident Response duties of primary support operators RDG-ACOP016. Rail entities should initiate a response to any incident affecting the railway infrastructure in order to meet the requirements set out in Railway Group Standards GE/RT8000 and Rail Industry Standard RIS-3118-TOM, company emergency plans and in support to the infrastructure manager. In most cases this is likely to be by means of a cascaded management notification process implemented by the relevant operations control through the use of telephone communication (landline and/or mobile) and pager systems.

Passenger Rail entities responses to an incident affecting the railway infrastructure should normally be implemented by the Primary Support Operator for the line of route concerned in agreement with the Owning Operator(s) of any train(s) involved. The list of Primary Support Operators is provided as Appendix A to RDG-OPS-ACOP-001 Issue 17 – June 2021: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident.

This should not detract from the Owning Operator or a Support Operator initiating an appropriate response should they be best placed to do so in accordance with the specific location, nature, and circumstances of the incident.

5.5.3.7 Role of infrastructure manager

The infrastructure manager will normally lead and direct the rail response to an incident affecting their infrastructure. For most routes, but not exclusively, this will be Network Rail.
Network Rail will normally appoint a responsible person, or in the case of more serious incidents, a Rail Incident Officer (RIO), to co-ordinate the rail emergency response at the site of, and as appropriate to the

circumstances. For major incidents, a Rail Incident Commander (RIC) may also be appointed to take overall strategic responsibility for rail industry incident management and to support the RIO.

5.5.3.8 Role of the Primary Support Operator

The Primary Support Operator should identify significant emerging risks (such as trains trapped between stations with no power during a period of very hot weather) to its own operations and those of Owning or Support Operators and ensure that where necessary, the following arrangements are implemented as relevant to the nature and circumstances of the incident:

- Suitable, sufficient resources are identified and deployed in accordance with the level of risk and an appropriate response is determined in conjunction with the infrastructure manager.
- A command-and-control structure is established at the earliest opportunity in conjunction with the infrastructure manager.
- A TOLO is appointed to co-ordinate their own and other Rail entities responses at the incident site in support to the infrastructure manager (and specifically the RIO).
- Where an incident has a significant impact on the operation of a station, a Station Incident Officer is appointed to manage the emergency response at that location (For further guidance see RDG-OPS-GN-017 Competence of Station Incident Officers).
- Identification of and communication with Owning Operator(s).
- Identification of and communication with Support Operator(s).

The Primary Support Operator should implement any necessary arrangements for dealing with passengers (except as provided for in RDG-ACOP-011 through the deployment of an Incident Care Team), traincrew, other personnel (including contractors) and the rolling stock of any train involved in the incident. This response should reflect the nature and circumstances of the incident and may include:

- Any requirement for train and/or station evacuation.
- Customer support (such as transportation from site, refreshments, temporary shelter; use of telephones and onward transportation to home or destination).
- Welfare requirements of rail staff involved.

With regard to the train(s) involved, the Primary Support Operator should consult with the Owning Operator to reach an understanding of the response requirements, including any appropriate advice on the rolling stock that may be involved.

The Primary Support Operator should also come to an understanding with Owning and any Support Operators as to the allocation of roles and responsibilities during the incident response process to ensure the most effective use of resources. This will include determining whether there is any necessity to transfer the role of TOLO from Primary to Owning or Support Operator in order for a more effective response to be co-ordinated in accordance with the nature and circumstances of the incident, and the technical requirements for the recovery of rolling stock.

The Primary Support Operator should also implement adequate arrangements in conjunction with the infrastructure manager to manage the effects of the incident on the rest of the operational railway for which they are responsible. This may include:

- Contingency service arrangements, including rail replacement road transport and alternative routing determined in conjunction with Support Operators and other transport providers.
- Crowd management and customer support at stations directly or indirectly affected by the incident.
- Dealing with passengers stranded as a result of the incident in conjunction with the relevant Owning Operator(s) (see RDG-OPS-GN-049 Meeting the Needs of Passengers Stranded on Trains).
- Appropriate customer information and travel advice, and specifically in accordance with Passenger requirements.

In addition, the Primary Support Operator should also ensure that appropriate arrangements are put in place with the infrastructure manager, Owning and Support Operators to:

- Determine the requirements for evidence gathering and initial investigation, including any necessary co-ordination with the British Transport Police and investigatory bodies such as the Rail Accident Investigation Branch (RAIB) and the Office of Rail and Road (ORR).
- Return the incident site to normal working at the earliest opportunity.

It is recommended that a separate cost centre be set up for response over and above the Primary Support

Operator's own costs, in order to facilitate any claims for costs incurred back from the Owning Operator (and their insurers).

5.5.3.9 Charter and Freight Trains

It is recognised that some passenger-carrying trains are operated by companies that are not members of the RDG Train Operators Operations Scheme and/or are not affiliated to RDG (such as privately operated steam or diesel locomotive hauled special trains) and therefore not subject to the same interfacing arrangements.

Primary Support Operators should apply the principles of RDG-ACOP016 (Approved Code of Practice – Incident Response Duties of Primary Support Operators) in the event of an incident involving such a train on their line of route after reaching an appropriate understanding with the infrastructure manager and relevant Owning Operator.

Where an incident involves a freight train, the owning FOC will normally implement its own specialist response in conjunction with the infrastructure manager.

The infrastructure manager should consider the immediate nature and consequences of the incident and determine whether the Rail entity Primary Support Operator may be better placed to provide a quicker interim response in agreement with the FOC concerned. This is particularly relevant for incidents that require chain of care and support to be carried out with the FOC traincrew involved.

5.5.3.10 Role of Train Operator Liaison Officers

The role of the TOLO is primarily to co-ordinate responses by the Primary, Owning and Support Operators at the incident site in support to the infrastructure manager. The recommended competency requirements for a TOLO are set out in RDG Guidance Note RDG-GN016 – Competence of Train Operator Liaison Officers (TOLOs). The TOLO appointed on an initial basis does not need to have expert knowledge of the rolling stock involved but must have the ability to communicate with the Owning Operator for appropriate technical advice should it be necessary.

The Primary Support Operator should ensure that the arrangements implemented are maintained until such time that an understanding has been reached with the infrastructure manager, Owning and Support Operators that the incident has been satisfactorily concluded or responsibilities have been transferred elsewhere.

Source: Incident Response duties of primary support operators RDG-ACOP016

5.5.3.11 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident

The following information on humanitarian assistance is taken directly from RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident. The Code assumes that (passenger) Rail entities will have appropriately trained and equipped ICT in place and that these will be deployed in response to a Major Passenger Rail Incident affecting their own or another Rail entities service to meet the requirements set out in the Code and as per the RDG ICT Deployment Plan.

Should a Rail entity not have such an ICT in place, it will need to satisfy itself that it is able to meet the requirements set out in this Code by other means.

5.5.3.12 Responsibility for categorisation as a Major Passenger Rail Incident

It will be the responsibility of the Duty Control Manager in the Control of the Primary Support Operator, i.e., that is geographically responsible for the location in which an incident has occurred, regardless of which Rail entities train is involved, to categorise the incident as a Major Passenger Rail Incident for rail industry response. This should be done in conjunction with Network Rail Route Control and, if immediately possible, with the Rail entity whose train is involved, thereby activating the provisions of RDG-OPS-ACOP-001.

5.5.3.13 Responsibilities for Humanitarian Assistance Response

The Owning Operator of the train involved should assume immediate responsibility for leading and managing the humanitarian assistance response. The Duty Control Manager of the Primary Support Operator should anticipate their own Rail entity being called on to assist the Owning Operator and implement their own Rail entities humanitarian assistance response accordingly, unless it can immediately be confirmed with the Owning Operator that this is not necessary.

If the Owning Operator is unable, for whatever reason, to take on the overall responsibility for the response, then the Primary Support Operator should assume the role of Owning Operator as far as the requirements of

this Code are concerned. This may apply either throughout the period during which this Code applies or until such time as the Owning Operator is able to assume this role.

Where trains of two or more Rail entities are involved, the Rail entities concerned should agree which will provide the overall leadership and management of the combined humanitarian assistance response - normally this will be the Rail entity whose passengers are perceived as likely to have suffered the greatest number of casualties.

The identity of the Rail entity leading and managing the humanitarian assistance response should be advised to Network Rail Route Control immediately.

5.5.3.14 Appointment of Lead Director and ICT Strategic Lead by Owning Operator

The Owning Operator should immediately appoint a member of the Senior Management Team as Lead Director. The Lead Director should assume overall responsibility for the company's response to the incident at any given time and be fully empowered to take decisions and commit their Company's resources.

The Lead Director should, in turn, appoint and empower a director / senior manager as ICT Strategic Lead. The ICT Strategic Lead should take over responsibility for directing the humanitarian assistance response from the Duty Control Manager as soon as possible. This should include ensuring that there has been an activation of the ICT and appointing a suitably trained ICT Deployment Manager and Deputy. This is described in detail in the ICT Deployment Plan.

The Primary Support Operator and other Support Operators should each appoint a similarly empowered Lead Director, whose identity should be advised to the Owning Operator's Lead Director as soon as possible.

5.5.3.15 Transfer of Responsibilities to Another Operator

The Lead Director and ICT Strategic Lead of the Owning Operator may jointly agree to transfer Owning Operator responsibility to the Primary Support Operator or other Support Operator if it is considered that this would provide a more effective response. In such cases, details of any changes should be advised immediately to all concerned.

5.5.3.16 Initial Actions by Other Responding Agencies

The following table provides a summary of the actions of the Police and Local Authorities, with whom close liaison should be established and maintained, in the immediate aftermath of any emergency and over the next few hours:

Option	Trigger	Decision	Lead	Secondary
Survivor Reception Centre	Significant number of survivors/ walking wounded	Police Tactical Commander	Police	Local authority, voluntary agencies, transport industry incident care teams (where applicable)
Rest Centre	Significant number of displaced people	LA Tactical Commander	LA	Voluntary agencies
Family and Friends Reception Centre	Large numbers of calls to casualty bureau. 'Searching behaviour'	Police Tactical Commander	Police / Local authority	Voluntary agencies, transport industry incident care teams (where applicable)

Deployment of staff to A&E	Significant numbers of hospitalised survivors	Police Tactical Commander	Police	Local authority social care teams

Note: The above is taken from the London Resilience Partnership Humanitarian Assistance Framework but a similar model is likely to apply in other areas. *Source: RDG-OPS-ACOP-001*

5.5.3.17 Rail Entities Roles and Responsibilities, Humanitarian Assistance following a Major Passenger Rail Incident

Initial actions which may be required to be undertaken by the Owning Operator, Primary Support Operator and other Support Operators should be undertaken by the Duty Control Manager of the Rail entity Control concerned.

Each Rail entity should have policies and procedures to be followed in the event of any incident. Following a Major Passenger Rail Incident, it is suggested that the actions listed in Appendix C of RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident be considered as it provides a simple checklist covering the majority of envisaged requirements.

In the event of a Major Passenger Rail Incident occurring at or near a Network Rail Managed Station, the arrangements detailed within the emergency plan of the station concerned should be implemented. Network Rail Managed Stations should provide Rail entities which operate within the station concerned with copies of current emergency plans and any proposed changes to these plans. Rail entities should ensure that their staff are trained and briefed on the arrangements contained within the relevant sections of the Network Rail Managed Stations emergency plans for any Managed Station into which they operate.

In the event of an incident occurring at or near a large, multiple operator station, the SIO should immediately call together the operators' representatives and provide accommodation, facilities and staff as agreed to operate this Code. Various out-based roles will also be required in the event of a Major Passenger Rail Incident. These are all under the ultimate control of the Owning Operator, who may use Primary Support Operator or other Support Operator staff to undertake the roles. This will be entirely dependent on available resources, location of the incident, etc. It is expected that in the vast majority of cases, members of the ICT will be best placed to perform these roles as a result of the training they have received.

It is recognised that smaller Rail entities may not have sufficient resources to form an ICT of sufficient size to respond independently to more than minor incidents and will hence need to rely on the deployment of Teams from other Rail entities in the event of any other incident involving one of their own trains. They should, however, ensure that they are able to provide overall response leadership/management and should therefore, as a minimum, maintain 2 - 3 persons who have sufficient understanding of the role of the ICT and how it will be deployed and are able to provide strategic direction to the Deployment Manager.

Providing support to Survivors in the first few hours after an incident is demanding and may well be traumatic but is also critically important to their long-term recovery process. The RDG ICT Guidance Manual provides guidance on factors to be taken into account when selecting members of ICTs. Rail entities should hold details of ICT members centrally and ensure that these can be made quickly available within their own and to other Rail entities in the event of an incident to supplement On Call arrangements.

A TOLO, reporting initially to and maintaining liaison with the RIO, should be appointed at the incident site by the Primary Support Operator.

The ICT Strategic Lead and the ICT Deployment Manager should liaise to identify which are necessary in the circumstances and ensure that where highlighted below as being required, staff with competence as ICT members (i.e., have completed the initial training for the role of ICT Team Member/Team Leader and have received associated refresher training within the previous 12 months) are nominated to undertake these roles. It should be noted that the incident site is likely to be the least important location to which humanitarian assistance staff should be directed:

- At the Casualty Bureau - a Rail entity representative with an understanding of the role and capabilities of the ICT and a general railway knowledge. This role does not necessarily require ICT competence.

- At a hospital - a Rail entity representative to provide a single point of contact between the hospital authorities (and any other responding agencies present) and those providing the humanitarian assistance response on behalf of the Owning Operator (report initially to hospital supervisor/the Police). This role requires ICT Team Member competence and ideally ICT Team Leader competence.

- At a Survivor Reception Centre - Survivor Reception Centre Liaison lead (report initially to the Police or Centre manager). This role requires ICT Team Member competence and ideally ICT Team Leader competence.

- At a nominated station(s) or other location - Humanitarian Assistance lead (report initially to station manager/supervisor). This role ideally requires ICT Team Member competence – if this is not possible, then a means of directing individuals to someone with such competence with the minimum of delay and difficulty should be provided.

- At a Family & Friends Reception Centre – Family & Friends Reception Centre Liaison lead (report initially to the Police). This role requires ICT Team Member competence and ideally ICT Team Leader competence.

- At a Humanitarian Assistance Centre - Humanitarian Assistance Centre Liaison lead (report initially to the Police). This role requires ICT Team Leader competence.

- With Local Authorities - A Local Authority Liaison lead. While this role does not require ICT competence, it does need to be assigned to someone with a degree of both seniority and experience in liaising with external partners and may be well-suited to someone who is competent as a Deployment Manager.

Rail entities should be aware that Police forces deploy Police FLOs who become the single point of contact for the bereaved and seriously injured. One of their specific roles is to make contact with whoever from the rail company is providing humanitarian assistance and accordingly the Deployment Manager should, as an early priority, appoint an individual with whom such initial contact by the Police FLO Coordinator can be made. This may be themselves.

This Deployment Manager should nominate a lead to attend at the Humanitarian Assistance Centre and have authority to extend Rail entity commitment to providing for the needs of the seriously injured and relatives of the bereaved. The specific requirements of Survivors should be considered on their merits; however, all reasonable requests should be met with.

It is vital that records are maintained to ensure that proper care and post incident follow up takes place as well as ensuring prevention against false claims. It is strongly recommended that this be done by means of a database system which complies with the requirements set out in the specification produced by RDG - Incident Care Team Survivor Relationship Management (SRM) System Requirements Specification, v1.1 dated 16 September 2019). RDG has also produced such a system which is available to Rail entities. The SRM and the Resource Kits issued to Team Members for the recording of key information are closely linked – the Resource Kit is designed to capture information required by the SRM and the SRM is designed to record all information captured in the Resource Kit. The Requirement Specification sets out in detail what data should be captured and recorded (irrespective of the means by which this is done).

The capturing, recording and retention of personal data must comply with current GDPR (General Data Protection Regulation requirements – guidance on how this should be approached within the context of ICT deployment is provided in RDG-OPS-GN-038 Data Protection Requirements During and After Incidents. See Chapter 6.

An accurate log should be maintained of all activities undertaken as part of the humanitarian assistance response – it is recommended that this be undertaken by a trained loggist – see RDG Guidance Note RDG-OPS-GN-034 Logging and Loggists. In addition, individual ICT members should also discretely record details of their contact with families. An ICT Resource Kit is available for this and the above purposes.

Owning, Primary Support and other Support Operators, whilst providing staff to assist in nominated roles, will continue to provide their own train (or alternative) services on both affected and unaffected routes. Rail entities should communicate information to this effect to Network Rail, NRE, etc. to assist in efforts to avoid confusion and unnecessary problems for the Owning Operator.

Owning, Primary Support and other Support Operators should consider the hours of duty of members of their own staff and deploy resources accordingly. It will be the responsibility of the Primary Support Operator and other Support Operators to advise the Owning Operator in good time of any member of staff requiring relief.
It is particularly important for all staff, whether employed by the Owning, Primary Support, or any other Support Operator, to be made aware that no comments or statements should be made to the media until an on-call Press Officer arrives. If Control staff are contacted for information, the caller should be referred to the Press Officer. It may be appropriate to indicate that a press conference will be arranged later when a Press Officer and/or Senior Manager is available.

Standard Police practice was once not to allow non-police personnel into the Casualty Bureau, however the value of having a Rail entity representative present, primarily to provide a single point of contact with the ICT but also able to advise on rail specific information (such as geography, possible journey routings, etc.) is now increasingly recognised. As such, many Police forces – including the Metropolitan Police - will now support a Rail entity presence within the Casualty Bureau, however others may not.

5.5.3.18 Coordination of Owning Primary Support Operator and other Support Operator response

The Owning Operator will control all rail industry humanitarian assistance activities associated with a Major Passenger Rail Incident. All staff providing this humanitarian assistance, whether from the Owning Operator, Primary Support Operator, or any other Support Operator, will respond directly to the Owning Operator. Initially this will be through the Duty Control Manager of the Owning Operator Control but will default to the ICT Deployment Manager once appointed. The Owning Operator's contact point/number should be passed out via Rail entity or Network Rail Control.

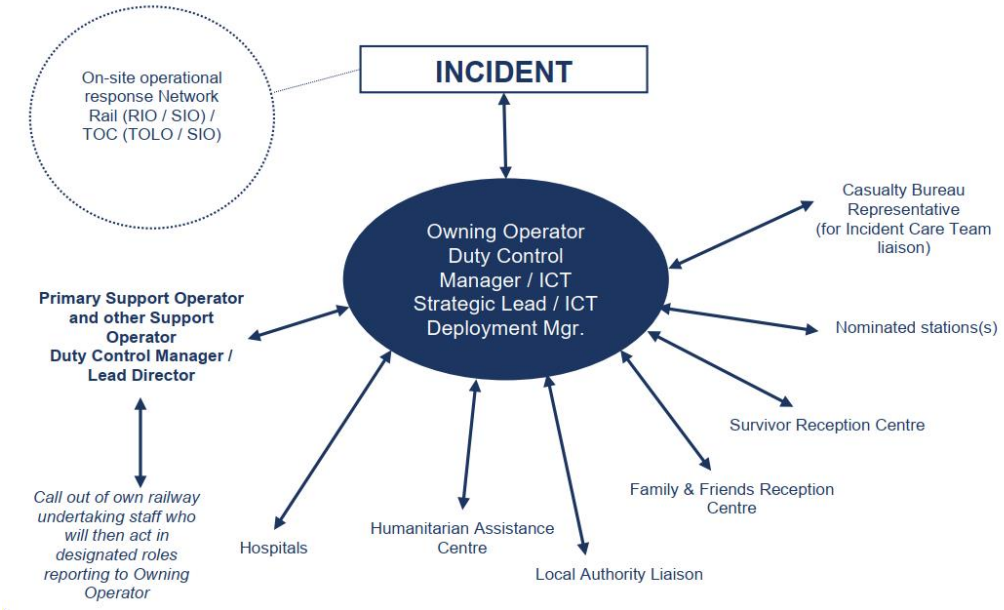

Figure 16 Coordination of Owning Primary Support Operator and other Support Operator response (Source: RDG-OPS-ACOP-001

5.5.3.19 Coordination of Public Affairs and Media Response

Public Affairs will be co-ordinated at a strategic level by the Police. However, Network Rail and Rail entities Public Affairs staff will be required to become heavily involved at an early stage on behalf of the rail industry. It should be noted that local authorities, emergency services and other affected parties may be involved in the joint Public Affairs response. The on-call Public Affairs Manager of the Rail entity whose train is involved should:

- Be aware that a senior manager of the company should be available for media response.
- Ensure that the Primary Support Operator Public Affairs Manager is aware and come to an agreement with them as to which Rail entities Public Affairs will act on behalf of all Rail entities initially.
- Ensure attendance of Press Officers at the incident site, designated station or other location, hospitals, and Survivor Reception Centres, via the Owning Operator if required.
- Coordinate all Public Affairs through Police Public Affairs.

Source: Part A – Actions during initiation phase – checklist from RDG-OPS-ACOP-001 Issue 17 – June 2021: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident.

5.5.3.20 Responder requirements during Extreme Weather

When operating train services during periods of extreme weather, Rail entities should be aware of the impact of such conditions on passengers and staff and enhance their operational arrangements appropriately, implementing pre-planned extreme weather arrangements. The purpose of this section of this guide is to promote good practice in regard to such arrangements.

Many forms of extreme weather can have an adverse effect on the ability to operate through their impact on infrastructure, rolling stock, staff, and passengers. These include:

- Extremely high temperatures.
- Extremely low temperatures.
- Snow.
- Frost.
- Icing (including ice from freezing rain).
- Strong winds.
- Extreme rainfall or thawing of snow/ice where this results in flooding.
- Lightning.
- Prolonged wet weather (in that this increases the risk of landslides and flooding).

In addition to increasing the likelihood of trains suffering extended delays or becoming stranded, they may also make responding to such events more challenging. It is possible, given the situation/failure, that a number of trains may be affected at the same time within the same area.

Temperatures of over 40°C were recorded for the first time in the UK in July 2022 and future UK climate projections indicate an increased incidence of 'extreme' events. Consideration of extremes of temperature therefore needs to form part of routine risk assessment and contingency planning. For further information please refer to Network Rail's latest Adaption Report (the third such report, published in December 2021, as of the date of issue of this Guidance Note). This sets out its understanding of the risks associated with climate change, how these impact on the performance and safety of the railway and how it is acting to enhance resilience and adapt to the impacts – see: https://www.networkrail.co.uk/sustainability/climate-change/climate-change-adaptation/.

Of the forms of extreme weather listed above, the two with the potential to directly impact on conditions inside the train in the event that on-train environment control systems are unavailable are high and extremely low temperatures.

High temperatures, particularly if combined with direct sunlight, can result in a very rapid increase in on-board temperatures to dangerous levels and there are few means of keeping people cool in such circumstances.

Extremely low external temperatures are less immediately problematic – on-board temperatures will cool at a much slower rate than that at which they rise in hot weather conditions and temperatures will at worst come to equal external temperatures rather than reach greater extremes. In addition, the train will continue to provide full protection from rain, sleet, snow, etc. and wind chill. At the same time, various options are likely to be available to keep passengers warm, for example by asking passengers to congregate together to preserve body heat. Many will, in any event, have with them additional 'outdoor' clothing that can be used.

Conversely, if evacuation to trackside is being considered, extreme cold is likely to present more of a hazard than extreme heat, particularly as it is likely to also affect conditions under foot through the presence of snow, ice, or frost.

Source: RDG-OPS-GN-015 Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems.

6 Data Handling

6.1 Overview

Information is critical to emergency response and recovery, yet maintaining the flow of information, including personal data (see Section 6.3.2), within agencies, with partners, and to the wider public, is extremely challenging under emergency conditions. The importance of information to emergency responders and those affected by events must not be underestimated.

Effective information management is dependent upon appropriate preparatory measures being in place to build situational awareness and the development of a Common Recognised Information Picture (CRIP) at the local, sub-national and national levels (if appropriate) (see previous guidance in Chapters 4 and 5). Such measures will need to support:

- The timely transmission and collation of potentially high volumes of information from multiple sources.
- The assessment of collated information to ensure its relevance, accuracy, timeliness, accessibility, interpretability, and transparency.
- The translation of available information into appropriate information products, for example, briefing the Strategic Co-ordinating Group or national groups, or release to the media for public information.

Challenges that may need to be addressed to realise the collation, assessment, validation, and dissemination of information under emergency conditions may include the following:

- Information management procedures may vary between agencies.
- Perspectives on the event or situation may differ.
- Mistakes and misunderstandings may occur under pressure.
- Communications can become overloaded.

There is a balance to be struck between ensuring that decisions are well informed and acting swiftly and decisively. Establishing systematic information management systems and embedding them within multi-agency emergency management arrangements will enable the right balance. It is important to note that voluntary and private sector organisations will typically need to be included in the multi-agency response and, as such, they must be integrated into the information management structures and processes that are established, trained, exercised, and tested. In particular, the sharing of information in a way that is responsive to the needs of emergency responders, and is compliant with data protection and other legislation, needs to be thoroughly understood and tested.

Where likely information requirements have been defined, local responders need to follow the established templates for such information products, whether these are locally determined or supplied from the sub-national or national level. Additionally, the use of such templates, and information management more broadly, should be embedded and evaluated through training and exercising.

Any emergency will result in widespread media interest and public concern. It is, therefore, essential that structures and processes exist to manage the demands of the media and to ensure that messages given out are consistent. It is similarly essential that the public receives appropriate advice, warnings, and information to provide reassurance and a basis for any necessary action.

Source: *Emergency Response and Recovery Non-Statutory Guidance accompanying the CCA 2004, October 2013.*

The CCA 2004 provides a framework for modern civil protection efforts by establishing a clear set of roles and responsibilities for local responders, giving greater structure and consistency to local civil protection activity, and establishing a sound basis for performance assessment at a local level. Though the key law governing data protection is the Data Protection Act 2018 (see Section 6.4.1), clear legal power to share data is found in secondary legislation made under the CCA 2004. The CCA 2004 (through the regulations made under it) places a duty on Category 1 and 2 responders, on request, to share information relating to emergency preparedness / civil protection work with other Category 1 and 2 responders. This duty relates to the preparedness, response, and recovery stages of an emergency. Section 2.4 of the statutory guidance supporting the Act states that:

"Information sharing is necessary so that Category 1 and 2 responders are able to make the right judgements. If Category 1 and 2 responders have access to all the information they need, they can

make the right decisions about how to plan and what to plan for. If they do not have access to all information, their planning will be weakened."

(Data Protection and Sharing – Guidance for Emergency Planners and Responders. Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery: February 2007)

This information sharing duty is not a statutory obligation to breach the common law duty of confidentiality – where the information is confidential the party considering making the disclosure must consider whether the interests of the individual or individuals will be better served by making the disclosure (i.e., is it in the public interest?). But it does provide one of the legitimising criteria for the sharing of **personal data** under the Data Protection Act 2018 (and if no duty of confidence is breached should put beyond doubt it is lawful under the first Data Protection Principle). Necessary actions taken under the CCA 2004 in accordance with the data sharing requirements of the Contingency Planning Regulations will be compliant with the Data Protection Act 1998 if:

- A legitimising condition is met (or in relation to sensitive personal data, one condition from Schedule 2 and one condition from Schedule 3 of the Data Protection Act 1998 are met).
- Information is being shared for a specific purpose.
- Information is being shared for a limited time.
- Information is only to be shared between named Category 1 and 2 responders that have a defined (as assessed by the requesting organisation or individual) need to see it.
- The data subjects are informed that their data may be shared within government for emergency response or recovery purposes unless to do so involves disproportionate effort.

The CCA 2004 does also prohibit Category 1 and 2 responders from publishing or otherwise disclosing any 'sensitive' information which they have received by virtue of the Act or created in the course of discharging their duties under the Act. Confusion has arisen over the use of the word 'sensitive' in both the Civil Contingencies and Data Protection Acts. The Acts have different definitions of what constitutes 'sensitive'. Under the CCA 2004, sensitive information relates to national security, public safety, business, or personal data. Only the latter is covered by the use of 'sensitive' in the Data Protection Act 2018. Under the CCA 2004, the only two exceptions where sensitive information can be disclosed are when:

- Consent for the publication or disclosure is obtained; or
- The information is commercially sensitive or personal data, but the public interest in disclosure outweighs the interests of the person or organisation concerned.

Category 1 and 2 responders should be aware of the differences required in handling personal data when compared to handling sensitive security-related or commercial information.

The Data Protection Act was first enacted in 1998 and applies in England, Wales, Scotland, and Northern Ireland; the Act was revised in 2018. The Data Protection Act 2018 controls how personal information is used by organisations, businesses, or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

The Data Protection Act 2018 is a framework under which personal data can be 'processed' providing it is lawful to do so. It does not apply to any information which falls outside that defined as 'personal data'. The Act aims to strike a balance between the rights of individuals and the sometimes-competing interests of those with legitimate reasons for using personal data. The way in which emergency planners and responders may use the personal data that they hold is governed by the eight Data Protection Principles; these require that information is:

1) Processed fairly and lawfully and in accordance with a legitimising condition.
2) Processed for specified and not incompatible purposes.
3) Adequate, relevant, and not excessive.
4) Accurate and up to date.
5) Not kept longer than necessary.
6) Processed in accordance with individuals' rights.
7) Kept secure.
8) Not transferred to countries outside the European Economic Area without adequate protection.

Source: Data Protection and Sharing – Guidance for Emergency Planners and Responders. Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery: February 2007.

Section 6.3 below provides ***MUST*** provisions for ensuring Data Controllers comply with these eight data sharing principles.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document.

6.2 Provisions

6.2.1 Rail Entities' Data Controllers ***MUST*** ensure that there is a legal basis for processing data. [5, 14]

6.2.2 Rail Entities' Data Controllers ***MUST*** ensure that the processing of data is fair by giving data subjects the necessary information when personal data is collected, or if this is not possible that they are exempt from this condition. [5, 14]

6.2.3 Rail Entities' Data Controllers ***MUST*** meet one of six conditions in order to process personal data as set out in Schedule 2 of the Data Protection Act 2018. [5, 14]

6.2.4 If sensitive personal data is to be processed, Rail Entities' Data Controllers ***MUST*** meet one of several further conditions set out in Schedule 3 of the Data Protection Act 2018 and regulations authorised under that schedule. [5, 14]

6.2.5 Rail Entities' Data Controllers ***MUST*** ensure that personal data is processed in accordance with the remaining principles of data protection as outlined above. [5, 14]

6.2.6 Rail Entities ***SHOULD*** keep a logbook or supply of log sheets available at a suitable location, either in or close to the room where it is expected that the Crisis Management Group will meet. [10]

6.2.7 Rail Entities ***SHOULD*** make known the location of the logbook or supply of log sheets to those likely to be members of the Crisis Management Team and also those within the organisation who have been identified as potential loggists. [10]

6.2.8 Rail Entities ***SHOULD*** document the location of the logbook or supply of log sheets within the company emergency plan. [10]

6.2.9 Rail Entities ***SHOULD*** ensure that the identified organisation loggists keep their own supply of logbooks/sheets in recognition that meetings of the Crisis Management Group may take place online. [10]

6.2.10 Rail Entities ***SHOULD*** initiate a log (or separate logs) of both events and decisions as soon as practicable once a tactical or strategic command team has been established. [10]

6.2.11 Rail Entities ***SHOULD*** maintain a log (or separate logs) until such time as the incident is concluded or responsibility passes to others. [10]

6.2.12 Rail Entities ***SHOULD*** ensure that logs comply with the following [10]:

- Be CIA (Clear Intelligible Accurate)
- Be in chronological order, with the time and date of each entry recorded (using the 24-hour clock)
- Have entries numbered consistently and methodically.
- Record facts, not assumptions/personal comments/opinions
- Record non-verbal communication (e.g., nodding or shaking of heads to indicate agreement or objection)
- Be complete, continuous, and contemporaneous (i.e., entries ***SHOULD*** be made at the time the information is received or at the earliest opportunity afterwards within a 24-hour period)
- Include accurate timings of when information is received or sent.
- If notes, maps, etc. are utilised, these ***SHOULD*** be noted within the log and as otherwise directed by the accountable person.

- Relevant faxes, emails, text messages, notifications, phone calls, etc. should be similarly recorded.
- Not include shorthand or abbreviations unless these are recognised terms (either generally or within the rail industry)
- Show clearly the correction of any errors or omissions - when an alteration is necessary, a single line ***SHOULD*** be drawn through the error, correction entered and the alteration initialled.
- No entry may be erased or obliterated.
- There ***SHOULD*** be no overwriting or double entries.
- There ***SHOULD*** be no blank pages or spaces.
- No pages may be removed or inserted.
- Must contain a signature immediately at the end of each session so that no additions can be made at a later date.
- Each individual page ***SHOULD*** be numbered separately and consecutively and be signed-off as an accurate record by the loggist and chair of the meeting along with the date/time.
- All changes of loggist ***SHOULD*** be clearly indicated by means of ruling off between the last entry made by the previous loggist and the first made by the next and with the names and signatures of both recorded on the log, along with the date/time.

6.2.13 Rail Entities ***SHOULD*** ensure that logs [10]:

- Indicate the start date/time and details of the location of the meeting for which it is being kept.
- Contain details of the loggist.
- Record names, initials, and roles of all present (including those who leave or join mid-meeting and those joining remotely, e.g., online, by phone or video link). It is good practice for name badges to be worn to assist the loggist in identifying individuals but if this is not possible or such badges are not clear, the loggist should ask for clarification of the required details.
- Record details of any actions, to whom they are assigned and when they have been completed.
- Document the allocation of individuals to any specific functions or roles.

6.2.14 Rail Entities ***SHOULD*** ensure logs record any decisions taken, consciously not taken, or deferred, and the basis for these in the form of a rationale. [10]

6.2.15 Rail Entities ***SHOULD*** keep logs in a safe and secure location for retention as a potential source of evidence in case of future proceedings. [10]

6.2.16 Rail Entities ***SHOULD*** keep a copy of all logs and those copies ***SHOULD*** be securely stored in an alternative location. [10]

6.3 Guidance Notes

6.3.1 Data Protection Act 2018

In response to lessons identified from the 7th of July London bombings in 2005, the Cabinet Office published guidance on data protection and sharing in emergencies. In the aftermath of the attacks, issues with data sharing between Category 1 and 2 responders hampered the connection of survivors to some support services. It became apparent that in some parts of the emergency response, the requirements of the Data Protection Act 1998 were either misinterpreted or over-zealously applied. As a result, the Cabinet Office worked with a wide range of stakeholders across government to develop tailored guidance for the emergency community to dispel some of the myths and provide a useful resource to inform future emergency planning, response, and recovery. The guidance has also been incorporated into training at the Emergency Planning College (EPC). The guidance contributes to the Government's vision for information sharing.

Key Principles within the guidance include:

- Data protection legislation does not prohibit the collection and sharing of personal data – it provides a framework where personal data can be used with confidence that individuals' privacy rights are respected.
- Emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information.
- Emergency responders should balance the potential damage to the individual (and where appropriate the public interest of keeping the information confidential) against the public interest in sharing the information.
- In emergencies, the public interest consideration will generally be more significant than during day-to-

day business.
- Always check whether the objective can still be achieved by passing less personal data.
- Category 1 and 2 responders should be robust in asserting their power to share personal data lawfully in emergency planning, response, and recovery situations.
- The consent of the data subject is not always a necessary pre-condition to lawful data sharing.
- You should seek advice where you are in doubt – though prepare on the basis that you will need to make a decision without formal advice during an emergency.

6.3.2 Personal Information

Whilst a great deal of information may need to be shared in relation to planning for or dealing with an emergency, only some of this will be personal data. This guidance focuses on personal data because this is where emergency planners and responders have experienced most problems. By 'personal data', we mean data falling within the definition of 'personal data' provided by the Data Protection Act 2018. This can be summarised as:

- Information relating to a living individual, from which that individual can be identified, or which can be used to identify that living individual in conjunction with other information held (or likely to be held) by a data controller. Personal data/information includes expressions of opinions about that person, or indications of intent towards them.
- Included in this is 'sensitive personal data' which comprises information about an individual's:
  - Racial or ethnic origin
  - Political opinions
  - Religious beliefs
  - Trade union membership
  - Health
  - Sexual life
  - Criminal activity

While the nature of an emergency will vary, the principles and legislative basis underpinning the sharing of information are broadly the same. This guidance does, however, highlight where there are differences – in particular in law enforcement-related emergencies where the powers of the police are particularly relevant.

While the problems arising from information sharing have been most acute during the emergency response phase, sharing of information is critical to all stages of an emergency. The principles and legislative framework explained in this guidance apply to the planning, response, and recovery phases – though as is made clear, the balance in either sharing or not sharing information can shift during phases of an emergency. During an emergency it is more likely than not that it will be in the interests of the individual data subjects for personal data to be shared.

One or more Schedule 2 conditions should be met when disclosing personal information. Data controllers need only comply with one condition – they do not become 'more' lawful by being able to meet more than one condition. In addition, the conditions are just as important as one another – just because the 'consent' condition is listed first does not mean that it is more important than any other condition. The Schedule 2 conditions are broadly that:

- The subject has given consent to share information; or
- Sharing information is necessary to protect the person's vital interests; or
- Sharing information is necessary to comply with a court order; or
- Sharing information is necessary to fulfil a legal duty; or
- Sharing information is necessary to perform a statutory function; or
- Sharing information is necessary to perform a public function in the public interest; or
- Sharing information is necessary for the legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, unless the rights or interests of the data subject preclude sharing.

When information is sensitive then one or more Schedule 3 conditions must also be met. These include that:

- The individual has given 'explicit consent' to share information; or
- Sharing information is necessary to establish, exercise or defend legal rights; or
- Sharing information is necessary for the purpose of, or in connection with any legal proceedings; or
- Sharing information is necessary to protect someone's vital interests and the person to whom the information relates cannot consent, is unreasonably withholding consent, or consent cannot

reasonably be obtained; or
- Sharing information is necessary to perform a statutory function; or
- Is in the substantial public interest and necessary to prevent or detect a crime and consent would prejudice that purpose; or
- Processing is necessary for medical purposes and is undertaken by a health professional; or
- Processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

The requirements of the Data Protection Act 2018 do not apply to data about deceased persons, including fatalities arising from an emergency, or any information from which an individual cannot be identified. Local and regional responders must though, of course, still be aware of, and take appropriate action to protect, the ethical, religious, and cultural sensitivities of processing information relating to a deceased person.

6.3.3 Consent and Legal Issues

Although different areas of law apply to data sharing – specifically the Data Protection Act 2018, the European Convention of Human Rights (ECHR) Article 8 and the common law of confidentiality – it is important to recognise that there is overlap between them. The particular rules of the various pieces of legislation cannot be ignored. These rules are explained in as non-legalese language as possible in this guidance. When considering the issues and to help get to the right decision in an emergency it is acceptable for responders to have in mind the following broad-brush and straightforward questions:

- Is it unfair to the individual to disclose their information?
- What expectations would they have in the emergency at hand?
- Am I acting for their benefit and is it in the public interest to share this information?

These suggested perspectives are not a substitute for deciding about fair and lawful processing, whether a Data Protection Act 2018 condition is met or whether a duty of confidentiality applies, but they are useful tools in getting to the right view.

Rail Entities do not necessarily need consent of the data subject to share their personal data. In terms of compliance with the Data Protection Act 2018 (and the Human Rights Act 1998), consent of the data subject is not a necessary precondition for lawful data sharing. The Data Protection Act 2018 sets out a number of criteria under Schedule 2 for the legitimate processing of personal data (and sharing, like using, is for the most part just another form of processing) and if any one of the criteria is met, the Data Protection Act 2018 test is satisfied. Consent is simply one of the criteria. Furthermore, consent in relation to personal data does not need to be explicit – it can be implied. More stringent rules apply to sensitive personal data when consent does need to be explicit if that criterion is used – criteria other than consent can still be used for sensitive personal data. Even without explicit consent for the sharing of sensitive personal data, it is still possible to share the data legitimately if this is necessary in order to exercise any statutory function (as may well be the case for responders) or to protect the vital interests of the individual where, for example, consent cannot be given. While sharing of personal data without the consent of the data subject may interfere with the right to respect for privacy under the Human Rights Act 1998 Article 8, the ECHR does allow for public authorities to interfere with certain rights under broadly defined circumstances known as ‘legitimate aims’. There must be a legal basis to share the information, the interference must be for the purpose of one of these legitimate aims and consideration must be given to whether the information sharing is proportionate and is the least intrusive method of achieving a legitimate aim.

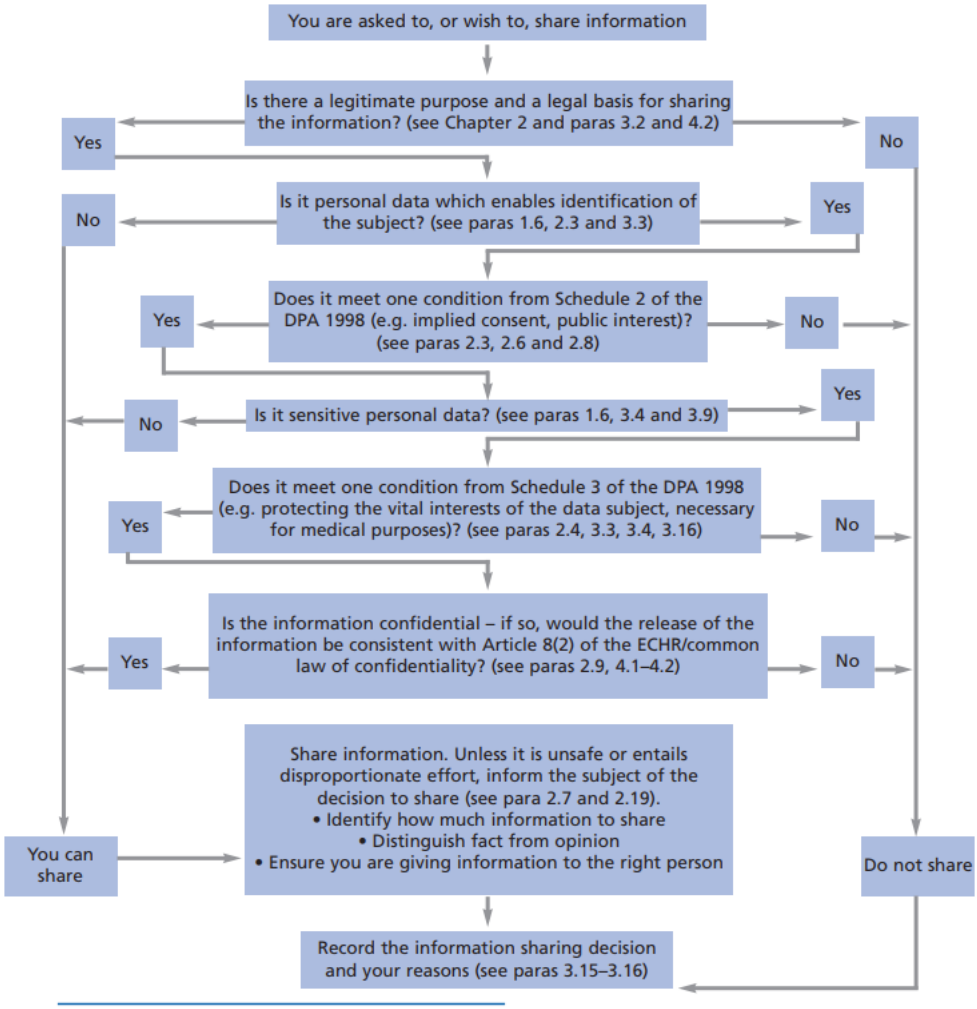

Figure 17 Flowchart of key principles for information sharing (Source: Data Protection and Sharing - Guidance for Emergency Planners and Responders)

6.3.4 Compatibility

The issue of 'compatibility' arises under the second principle of the Data Protection Act 2018. If personal data is collected by one organisation for a particular purpose, then 'compatibility' (i.e., that the information must be used for the same purpose it was collected for) is not a necessary condition. The test is one of incompatibility – i.e., is the new purpose incompatible with the original purpose? In an emergency response scenario, it is difficult to foresee circumstances where sharing personal data would be incompatible with the purposes for which they were originally collected.

6.3.5 Confidentiality and Public Interest

Local responders need to balance the common law duty of confidence and the rights enshrined within the Human Rights Act 1998 against the effect on the individual or others of not sharing the information. The common law duty of confidence relates to the duty for public bodies and individuals to respect confidential information relating to individuals. The information has to have a 'quality of confidence' – not everything that a public sector body holds on an individual will be confidential – and has to have been given in circumstances giving rise to an expectation of confidentiality.

If the data collection and sharing is to take place with the consent (either implied or explicit) of the data subjects involved, providing they are clearly informed about the purposes of the sharing, there will be no breach of confidentiality or the Human Rights Act 1998. If the information is confidential, and consent of the data subject is not gained, then the responder needs to satisfy themselves that there are grounds to override the duty of confidentiality in these circumstances. This can be because it is overwhelmingly in the data subjects' interests for this information to be disclosed. It is also possible that an overriding public interest would justify disclosure of the data (or that sharing is required by a court order or other legal obligation). To overcome the common

law duty of confidence, the public interest threshold is not necessarily difficult to meet – particularly in emergency situations.

Confidential health data carries a higher threshold, but it should still be possible to proceed where the circumstances are serious enough. As is the case for all personal data processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all the personal data need to be shared to achieve the objective?

It is recommended that Working with Disaster Survivors and the Bereaved: Code of Practice on Privacy, Anonymity & Confidentiality produced by Disaster Action should be adopted when requesting or receiving requests for information concerning individual victim or families – see http://www.disasteraction.org.uk/guidance_for_responders/.

Rail Entities are reminded that information is subject to various legislation and sometimes it may be better not to record details which might cause distress to a family if disclosed in Court.

6.3.6 Data Collection

The collection of personal data prior to or during an emergency is a key part of emergency planning, preparation, and response. Emergency planners and responders may need to maintain lists of all those people who could be affected by an emergency. So long as such a list is kept securely, with access only to those who need to see the information (in compliance with the requirements of the Data Protection Act 2018 outlined in Section 6.3.1 Data Protection Act 2018 above) and it is not used for any other purpose – then the collection will be permitted. It is important that the purposes for the collection of this personal data are in the interests of the data subject and more generally the public at large. The organisation that kept such a list would become the data controller with attendant responsibilities, including providing subject access rights. In addition, if the data is to be obtained from other data controllers these controllers must ensure that the data subjects are aware of the disclosures. The maintenance of such lists or databases (which could be linked to Geographical Information Systems – see Section 6.3.8 GIS and Data Sharing) can allow the data to be checked (i.e., quality assured) prior to an emergency – an important step to provide emergency responders confidence in decisions based upon the data. A key issue in meeting the requirements of the Data Protection Act 2018 will be maintaining the accuracy of the data; it is likely to need regular checking and sharing with those who provided it.

As an alternative to maintaining their own lists or databases of personal data to inform a response to an emergency, local and regional responders can put in place mechanisms by which they can draw upon individual organisations detailed records during an emergency (such as those of care homes, voluntary organisations, and health trusts). There are possible advantages and disadvantages to such an approach. On the negative side, they could be less responsive than the use of pre-existing aggregated lists or databases because of the bureaucratic/practical hurdles in accessing them. On the positive side, they should be more accurate given that they will be using the latest version of the organisation's records (e.g., a care home's residents list). In either case, well developed and tested arrangements should be in place to ensure that records are accessible and accurate, and that 'fair processing' procedures are in place to inform individuals that information about them is included in such a list or database.

The processing of personal data by local and regional responders must be proportionate to the requirements. Emergency planners and responders should only process personal data that they really need. As an example, during the planning stage it might be important to know the total numbers of vulnerable people in an area to ensure that adequate facilities and procedures exist. In these circumstances it should be legitimate for the planning agency to request the numbers and locations of vulnerable people, but not additional personal data which would allow identification.

It is important that the organisations involved in emergency planning establish processes to manage the disclosure or exchange of personal data effectively so that the parties involved are quite clear about both the type of information that could be shared and the circumstances providing for disclosure. The local authority, through the Local Resilience Forum (LRF) structure, is generally in the best position to lead on the establishment of multi-agency data sharing agreements. DCA has developed a toolkit for the public sector to enable effective and legitimate personal data sharing.37 For organisations that engage in large volume transfers of personal data (for example, in parts of the social security and health systems), detailed data sharing protocols may be appropriate. In general, however, more strategic agreements (or Memorandums of Understanding) setting out the high-level arrangements and principles underpinning data sharing will be more appropriate. These provide a flexible data sharing framework for multi-agency emergency management which more detailed mechanistic information sharing agreements may not. **The absence of data sharing**

agreements should not prevent Category 1 or 2 responders from sharing data particularly when responding to an actual emergency event.

6.3.7 Data Sharing and Vulnerable People

Identifying, planning for, and providing for the needs of vulnerable group will involve a large number of partners and pulling together a large amount of complicated, and changing information. Operating on a lists of lists basis may help planning.

These lists will not be a central list of individuals but a list of partners and contact numbers that can be used to gather relevant information in the event of an emergency. This approach might include:

- List of organisations (likely to be your key planning partners) who hold and maintain the key vulnerable people data, with an agreement to provide it in the event of an emergency. This approach helps avoid some data sharing difficulties (see section on data sharing protocols).
- List of types of vulnerability – identifying the potential range of vulnerable people with specific needs within a local area in advance of an emergency will assist with planning and response.
- List of vulnerable establishments in your area – identifying the key establishments likely to require additional assistance in terms of vulnerable people.

It is obviously important to ensure that lists of contacts are kept up to date, allowing the response to vulnerable people to be activated as soon as required.

Many of the vulnerable individuals concerned will be known to existing service providers (people who live or are present in vulnerable establishments such as nursing homes or day centres). There will be others who, for a variety of reasons, are more difficult to identify – such as those who live in the community as individuals, visitors to the area or the homeless. Contingency arrangements are needed to ensure they are not overlooked.

In order for emergency plans to give special consideration to the vulnerable, as required by the statutory guidance, plans must be able to distinguish this group from the self-reliant. While all people caught up in an emergency could be (and in some circumstances will be) defined as vulnerable due to their proximity to the event, planning and response arrangements should focus on those who are assessed as not being self-reliant and may need external assistance to become safe.

Potentially vulnerable individuals/groups include the following:

- Children
- Older people
- Mobility impaired
- Mental/cognitive function impaired
- Sensory impaired
- Individuals supported by health or local authorities.
- Temporarily or permanently ill
- Individuals cared for by relatives.
- Homeless
- Pregnant women
- Minority language speakers
- Tourists
- Travelling community

Being in one of these categories does not automatically denote vulnerability, and stereotyping should be avoided - whether someone is in fact vulnerable will largely depend on three things:

- The type of emergency - your plans must be tailored and proportionate to the risks faced by your constituent community, as identified in your local Community Risk Register (CRR).
- The type of response required - a response to an emergency which requires an evacuation is likely to determine a higher number of vulnerable people compared to a response which requires shelter in situ.
- The availability of the support that individuals normally receive from family/friends/carers/other social networks.

Planning to meet the needs of vulnerable people in emergencies can only be done effectively through the proper sharing of data, which requires an understanding of data sharing parameters, busting data sharing

myths, and the building of networks with relevant local and regional agencies. Reciprocally, in the response to an incident, effective data sharing ensures a timely provision of additional support for those that need it. The following section is in effect an abstract of data sharing guidance with relevance to vulnerable people in emergencies (for full details, see the Cabinet Office publication *Data Protection and Sharing – Guidance for Emergency Planners and Responders*).

Although the above guidance should be applied to the sharing of data on vulnerable people, to ensure that data protection laws are not being misinterpreted, there will be an understandable reluctance among agencies to identify vulnerable groups, and to share specific details between agencies, ahead of an incident being declared. It would in any case be impossible to maintain an up-to-date list of vulnerable people centrally. But, at the planning stage, the agencies can take two important steps:

- Share less detailed information - an indication of the type and indicative numbers of vulnerabilities that may exist in certain geographic areas. For instance, it may be enough for planning purposes to know the numbers of people within a certain geographic area that require prescription medicine. This can allow preliminary allocation of GP resource (or equivalent). The detail of who those people are (and possibly the type of prescription medicine required) may only need to be shared when an incident is imminent.
- Agree the method and format in which information will be shared in the event of an incident occur.

Individual responders and agencies should ensure that their own customised lists of vulnerable people are as up to date as possible, and in a fit state to be shared when requested in agreed circumstances prior to, during and after an incident, identifying any potential blockages, uncertainties, or ambiguities in advance.

Agencies needing to share details of vulnerable people should agree what kinds of information can be made available in advance and what categories will only be shared in the event of, or in anticipation of, an emergency. Sharing contact details allows agencies to proactively reach people who may welcome help and allows the individual to choose whether or not to take up offers of assistance. But it will not always be necessary to share or obtain the specific details of the vulnerability: if organisation *A* (social services for example) believes them to be vulnerable, then organisation *B* (emergency planning unit for example) will sometimes only need the name and location details of the subject.

While it can be very important to share basic contact details between responding agencies, there are separate issues relating to the sharing of more personal and/or sensitive information about individuals' circumstances. It is important, when dealing with information of that sort, that responders strike a balance between enabling access to support agencies and preventing any undue intrusion or transgression of privacy or dignity.

As the collection and sharing of information on groups or individuals with specific needs in a local area involves a large number of interested parties, the use of Information Sharing Protocols (ISPs) - where appropriate - can help to allay any fears partner organisations may have, although an absence of ISPs does not mean that information cannot be shared. In either case, the terms of information sharing must be clearly communicated to partners early in the planning process so that there is a common understanding of the parameters in which you will be working (particularly to dispel any limiting data sharing myths).

Trigger mechanisms should be considered for inclusion in the ISPs so that all parties agree as to what level of information will be shared and when. For example, prior to an emergency, an estimate of numbers might be shared. During a developing emergency, accurate numbers for at risk areas might be shared. In the event of assistance being required or an evacuation, some details of individuals might be shared. These triggers might be different between different organisations depending on the assessment of risk.

Further guidance on responding to vulnerable persons can be found in ATOC/GN029 – Responding to Vulnerable Persons (Issue 1, November 2015).

Source: Identifying People Who Are Vulnerable in a Crisis, Guidance for Emergency Planners and Responders, Civil Contingencies Secretariat (February 2008).

6.3.8 GIS and Data Sharing

Geographical Information Systems (GIS) are frequently used to facilitate the sharing of geographically referenced data and information. Given that in excess of 90% of corporate data is estimated to be geographically referenced in one form or another (for example, associated with an address, a postcode, or a grid reference) the application of GIS to emergency management is growing in significance, and the Emergency Planning College has published guidance on GIS and promoting its uptake. Inappropriate barriers

to sharing data between agencies have, however, impeded a number of GIS initiatives.
Many of the data-sets which GIS can utilise to support effective and efficient emergency preparation, response, and recovery fall well outside the focus of data protection legislation, for example area demographic profiles, flood risk zones, hazardous sites, and infrastructure networks. Full or partial release of data relating to some of these may of course be subject to other constraints around national security, public safety, and commercial confidentiality.

6.3.9 Other legislation

There are a variety of other pieces of legislation that relate to the collection and sharing of personal data that may be relevant to emergency planners and responders. Some of this legislation will not apply directly to the devolved administrations and different jurisdictions should take account of their own legislative arrangements. The most significant is the Human Rights Act 1998 which applies throughout the UK, and which provides people with a clear legal statement of their basic rights and fundamental freedoms. Article 8 of the ECHR was incorporated into UK law by the Human Rights Act 1998. It relates to the right to respect for private and family life, home, and correspondence. If the data collection and sharing is to take place without the consent of the data subjects involved, or if bulk transfers are being made which do not specifically relate to individuals who are involved in an emergency, then Article 8 is relevant.

The Human Rights Act 1998 does not, though, prevent the collection or sharing of personal data. The Human Rights Act 1998 provides lawful restrictions on these human rights for use by public authorities in certain circumstances such as reasons of national security, public safety, the protection of health and the prevention of disorder. Public authorities can, therefore, collect and share personal data if it is in pursuit of these lawful aims – of which sharing of personal data in an emergency is likely to be legitimate.

Other relevant pieces of legislation include the:

- Freedom of Information (FOI) Act 2000
- Environmental Information Regulations 2004
- Local Government Act 2000
- Crime and Disorder Act 1998
- Police Acts 2006 and 1997
- Children Act 2004
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Health and Social Care Act 2001
- Public Health (Control of Diseases) Act 1984

While local responders clearly need to have due regard to these other pieces of legislation, the key framework for data protection and sharing is that provided by the common law of confidence and the Data Protection Act 2018. Among the various types of personal data that local responders may need to obtain, or share is medical information which is subject to greater legislative and regulatory safeguards when compared to most forms of other ‘personal data’. Specific guidance can be referenced in the legislation cited above, but in most circumstances the key issue will remain that of balancing the duty of confidence against public interest needs.

6.3.10 Loggists

It should also be recognised that the role of the person keeping the log – referred to in this document as the loggist – is both an important and demanding one. While previous experience of Minute taking may be highly desirable, the loggist should also be ready to proactively challenge decisions and explanations as and when necessary to ensure that a good quality log is maintained.

As a minimum, the purpose of the role is to record all decisions taken, not taken, or deferred within the group charged with directing the incident response on behalf of the company, along with the rationale given by the decision-maker in each case. The title of this group is likely to be organisation dependent – for the purposes of this Guidance Note the term Crisis Management Group has been adopted, along with the term Crisis Commander for the Chair of this Group. While aimed specifically at this Group, the content of this Guidance Note will also be of direct relevance to other persons and groups making decisions in the context of incident response, for example the ICT (Incident Care Team) Deployment Centre.

The record should be of an appropriate quality and completeness to be used, if necessary, in any subsequent enquiry, whether internal or public/coronial.

In addition, it will generally be useful to include – or keep a separate log of – events during the response phase to assist with the building of a timeline.

Finally, the loggist may also be required to follow up on actions agreed at meetings of the Crisis Management Group, ensuring as far as practicable that these are being progressed, and report back to the Group accordingly.

It is important that the loggist is not seen as a general 'runner' or administrative support – to do so shows a failure to acknowledge the critical importance of the role and is liable to distract the loggist from their key purpose.

Similarly, the loggist should not be expected to take full minutes or have responsibility for undertaking any actions or decisions (beyond keeping the log itself).

6.3.11 Incident and Decision Logging

Most incidents will be dealt with effectively with the situation reverting reasonably rapidly to 'business as usual'. As stated previously in Chapter 4 Command and Control and Chapter 5 Responder Requirements, there will be a need to capture operational lessons to be learned as a result of decisions made or not made, along with elements of good practice, to influence the review and updating of plans, processes and procedures reviewed and updated as appropriate. The impact of major incidents on the railway will generally be felt internally by the affected organisation and its immediate partners. However, some incidents will lead to public inquiries or criminal investigations, with rail entities and/or their staff called to give evidence. It is therefore vital that, in respect of the response, accurate records are kept of who made what decisions, the evidence and rationale on which these were based and who carried out what actions. These records will serve not only to support any inquiry but also to offer a degree of protection to those railway entity employees involved in managing the response to the incident.

The keeping of logs pertaining to the response to significant and major incidents is important both for internal and external reasons.

Generally:

- They allow those making decisions as part of any command group to record their justifications for a course of action or decision in a contemporaneous written record of the thought process supporting such a course of action or decision.
- They provide capability for honestly held beliefs and actions taken in good faith at the time to be recorded and rationalised.

Internally:

- They provide a record of all planning, strategic, tactical, and operational decisions made, and actions taken during an incident and as such are a key input to any internal or joint post incident review.
- Externally:
- They ensure an accurate record is available in the event of any subsequent investigation, public inquiry, or litigation.

Overall, the keeping of accurate records provides protection for all involved in the decision-making process:

- They provide a note (aide-mémoire) from which to justify reasoning and decisions at a later point or date.
- They assist in promoting coherent reasoning in the exercising of discretion.

The log and all associated paperwork become legal documentation and could be used at a later date in a public inquiry or other legal proceedings. These will be disclosable but sensitive personal detail will likely be redacted or otherwise controlled.

6.3.11.1 Format and content

Within the rail industry the mnemonic "NO ELBOWS" is used to aid loggists in remembering how to order and structure their logbooks. None of the ELBOWS elements should be carried out:

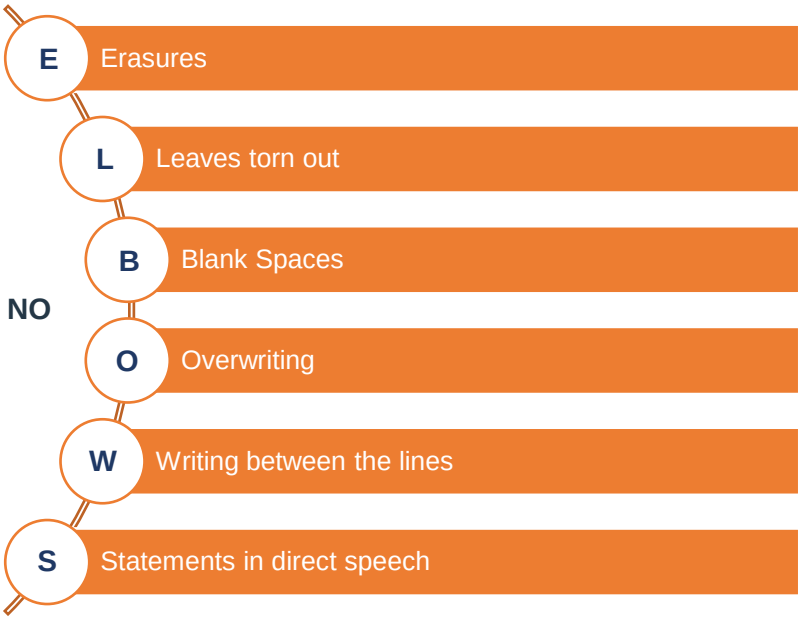

Figure 18 Mnemonic for remembering how to order and structure logbooks (Source: RDG-OPS-GN-034 RDG Guidance Note: Logging and Loggists)

Chapter 4 Command and Control details common multi-agency JESIP tools for use by loggists and decision makers. Use of multi-agency tools during a response will provide interoperability across responding agencies.

6.3.12 Rail Accident Investigation Branch (RAIB) - Sharing evidence

RAIB's response to accident and incident notification.

The Regulations place a duty on railway industry bodies (infrastructure managers, railway operators, or maintainers), involved in an accident or incident, to notify us.

“While all of our investigations are conducted completely independently of any investigations by other parties, we can share with the railway industry, and will share with other statutory investigatory bodies, technical evidence and factual information arising from tests and examinations that we carry out. We have agreed a Memorandum of Understanding with enforcing authorities to clarify our respective roles.

We will not share the identity of witnesses, their statements, or medical records relating to people involved in the accident or incident. More information about how the RAIB protects the identity of witnesses and their statements can be found in Leaflet 02 - Your witness statement.

During investigations we maintain contact with the various parties involved in the accident or incident. We aim to keep the industry and other people who are involved informed of emerging findings throughout the investigation. We may decide to update the public about progress and findings during the investigation by publishing an interim report or by updating our website.

If at any time during the investigation we become aware of any safety matter we believe requires urgent consideration, we will formally alert the industry and safety authority by issuing an Urgent Safety Advice notice.”

Source: RAIB's response to accident and incident notification.

7 References

For the purpose of developing this Code of Practice, we have consulted a variety of International Standards, guidelines, and good practice sources. This includes the following:

7.1 Provisions References

Endnote Number	Source
1	Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004
2	RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A - Governance
3	RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP)
4	The Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 4.
5	Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery
6	Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 7
7	Chapter 7 Communicating with the Public: Revision to Emergency Preparedness
8	RDG-OPS-GN-014: Major Incidents – Preparation of Aide-Mémoires for Senior Managers
9	RDG-OPS-GN-015 Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems
10	RDG-OPS-GN-034 RDG Guidance Note: Logging and Loggists
11	RDG-ACOP-016 Incident Response Duties of Primary Support Officers
12	Rail Safety and Standards Board (RSSB) Rule Book Module M1 GERT8000-M1 Issue 7, Section 2 to Section 6.
13	BS ISO 21110:2019 Information and documentation − Emergency preparedness and response
14	Data Protection Act 2018
15	JESIP Joint Doctrine Edition 3 October 2021
16	RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident

7.2 Legislation & Regulation

Name of the document	Reference number
Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009	N/A
Railways and Other Guided Systems (Safety) Regulations 2006 (ROGS)	N/A
Civil Contingencies Act 2004	N/A

Management of Health and Safety at Work Regulations 1999 (MHSWR)	N/A
Data Protection Act 2018	N/A
Health and Safety at Work Act 1974	N/A

7.3 RDG Documentation – ACOP / GN

Name of the document	Reference number
RDG Approved Code of Practice: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident.	RDG-OPS-ACOP-001
RDG Approved Code of Practice: Rail Emergency Management Code of Practice with Guidance Part A - Governance	RDG-OPS-ACOP-008
RDG Guidance Note: Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention	RDG-OPS-ACOP-009
RDG Approved Code of Practice: Incident Response Duties of Primary Support Operators	RDG-ACOP-016
RDG Guidance Note: Major Incidents – Preparation of Aide-Mémoires for Senior Managers	RDG-OPS-GN-014
RDG Guidance Note: Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems	RDG-OPS-GN-015
RDG Guidance Note: Competence of Train Operator Liaison Officers (TOLOs)	RDG-OPS-GN-016
RDG Guidance Note: Competence of Station Incident Officers	RDG-OPS-GN-017
RDG Guidance Note: Checklist for Major Incident Response	RDG-OPS-GN-023
RDG and Network Rail Guidance Note: Meeting the Needs of Passengers Stranded on Trains	RDG-OPS-GN-049
RDG Guidance Note: Critical Incident Management	RDG-OPS-GN-063
RDG Guidance Note: Emergency Management Legal & Regulatory Register	RDG-OPS-GN-064
Rail Resilience Project (RRP) Emergency Management Review: Findings & Recommendations Report. Version 1.3, September 2021.	N/A

7.4 International / British Standards

Name of the document	Reference
Security and Resilience – Crisis Management – Guidelines	ISO22361:2022
Security and Resilience – Community and Resilience – Principles and framework for urban resilience	ISO22371:2022
Governance of Organisations – Guidance	ISO37000:2021
Societal security - Business continuity management systems - Requirements	ISO22301:2019
Risk management - Guidelines	ISO31000:2018
Organisational Resilience	ISO22316:2017

7.5 Guidelines

Name of the document	Date of Issue
National Risk Register	August 2023
Rail Safety and Standards Board (RSSB) Rule Book Module M1 GERT8000-M1 Issue 7: Dealing with a train accident or train evacuation	December 2023
UK Resilience Framework	December 2022
JESIP Joint Doctrine: The Interoperability Framework Edition Three	October 2021
UK Severe Space Weather Preparedness Strategy	September 2021
Evacuation and shelter guidance: Non statutory guidance to complement Emergency preparedness and Emergency response and recovery	January 2014
Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004	October 2013
Expectations and Indicators of Good Practice Set for Category 1 and 2 Responders	October 2013
Cabinet Office Civil Contingencies Secretariat: The role of Local Resilience Forums: A reference document	July 2013
National Recovery Guidance	June 2013
Responding to Emergencies: The UK Central Government Response: Concept of Operations	April 2013
Cabinet Office: Emergency response and recovery Guidance	February 2013
Emergency responder interoperability: Lexicon of UK Civil Protection Terminology Version 2.1.1	February 2013
Lead Responder Protocol: Civil Contingencies Act 2004 Duty to Communicate with the Public	May 2007
Cabinet Office: Provision of scientific and technical advice in the strategic co-ordination centre: guidance to local responders	April 2007
Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery	February 2007
Home Office and Cabinet Office: Guidance on dealing with fatalities in emergencies	January 2006
Cabinet Office: The Lead Responder Protocol	February 2011

7.6 Good Practice Sources / Materials / Textbooks

Name of the document	Date of Issue
Cabinet Office ResilienceDirect™	2024
The Business Continuity Institute Good Practice Guidelines 2023	2023
Governance 101: assurance and reassurance	2021
Department for Business, Energy & Industrial Strategy: UK Severe Space Weather Preparedness Strategy, September 2021	2021
Office of Rail and Road RM^3 The Risk Management Maturity Model	2019

8 Appendices

8.1 Capability Maturity Model Integration (CMMI)

The maturity model below is referenced within this ACOP and is referenced from the RDG ACOP: Part A – Governance.

	AD HOC	MANAGED	STANDARDISED	PREDICTABLE	EXCELLENCE
RCS 5 Emergency Planning	1. There is no organised identification of possible emergencies and how to respond if they arise. 2. The organisation relies on the emergency services to deal with all aspects of an emergency. 3. The organisation does not consider the risks or the consequences of possible emergencies on the business or its workforce. 4. The organisation does not apply standards to support emergency planning or arrangements. 5. There is no consideration of the need for co-ordinated responses with other organisations in the event of major incidents requiring joint responses.	6. The organisation realises that emergency responses are an important part of a risk control system. 7. Major emergencies that could arise are identified and there are some plans in place to deal with them. 8. Emergency responses are the responsibility of departments or divisions of the organisation. 9. The organisation applies basic requirements to the plans for major emergencies that could arise. 10. Emergency procedures requiring multi-agency response are recognised, but there is no structured planning of responses required.	11. Potential emergencies arising from tasks are identified as part of risk assessments. 12. Control measures, including training and resources, are in place to deal with emergencies. 13. The organisation determines and provides the resources needed to support the emergency planning arrangements. 14. The organisation recognises that emergency planning is a critical part of the business and is applying the appropriate standards. 15. Joint emergency response exercises take place with other organisations involved in a task. Roles in emergency response are clear and understood.	16. Emergency responses are developed and reviewed in response to developing risks and emergency scenarios. 17. Feedback from exercise 'wash-ups' is taken into account when procedures are reviewed to make sure emergency responses remain up to date and effective. 18. The full suite of emergency arrangements has been assessed so that appropriate risk reduction strategies are evident should they be realised. Feedback from exercise 'wash-ups' is taken into account when procedures are reviewed to make sure emergency responses remain up to date and effective. 19. Changes to the emergency response procedures are based on evidence from experience and demonstrably lead to improvements. 20. Collaborative organisations are fully involved in wash-up sessions including reviews of procedures.	21. The organisation proactively looks outward when planning emergency response to identify and use good practice in a spirit of continuous improvement. 22. Emergency response arrangements are in place and reflect good practice from both within and outside the rail industry. 23. Lessons from published reports are included in procedure reviews and incorporated into revised emergency procedures. 24. The organisation actively seeks to find and share more effective ways of dealing with emergencies. 25. Information sharing is fully collaborative both with direct collaborating organisations and others with relevant information and / or experience.

People	26. Strategic leadership of IEM is not in evidence. 27. People are unaware of their IEM governance responsibilities. 28. People are assigned to IEM governance roles on an ad hoc or inconsistent basis without training. 29. There is no wider culture of resilience across the Rail Entity (or industry)	30. There is some strategic leadership for IEM. 31. People have been made aware of their IEM governance responsibilities. 32. Some people involved in IEM governance activities are suitably trained. 33. People are aware that the Rail Entity has a role to play in industry IEM	34. Strategic leadership of IEM is often evidenced. 35. People have been made aware and generally understand their IEM responsibilities. 36. People fulfilling roles within the governance framework are suitably trained on how to deliver their obligations. 37. People understand the role that their Rail Entity plays in industry IEM.	38. There is evidence of routine and consistent strategic leadership of IEM. 39. IEM governance responsibilities are documented within role profiles/ job descriptions. 40. People involved in IEM governance are trained and competent (including continuing professional development) to deliver their obligations. 41. People understand the role that their Rail Entity plays in UK IEM.	42. There is evidence that strategic leadership of IEM is embedded in the organisation. 43. Everyone in the organisation recognises they have role to play in IEM and wider resilience and feel empowered to do so. 44. People are aware how their entity's IEM governance interfaces with that of colleagues in stakeholder organisations. 45. A culture of resilience has been embedded across the Rail Entity.
Processes	46. There are no documented processes to enable IEM governance meetings across the Rail Entity. 47. There is no documented process for managing IEM skills and competency. 48. There is no documented process to support in developing situational awareness. 49. There are no documented processes to support the provision of IEM management information. 50. The is no process for assessing the maturity of a Rail Entity's IEM capability. 51. There is no process to manage the Rail Entity's engagement with other IEM stakeholders.	52. Some processes to enable IEM governance meetings are documented. 53. Some elements of an IEM skills/competence system are documented but most are ad hoc. 54. The need for situational awareness is documented but supporting processes are ad hoc. 55. The need for IEM management information is documented but processes remain inconsistent. 56. IEM maturity is partially considered in other assessment processes. 57. Process to manage IEM stakeholder engagement are partially documented / inconsistent.	58. Most processes to enable IEM governance meetings are documented. 59. Most elements of an IEM skills/competence system are documented. 60. Document processes exist for developing situational awareness. 61. There are documented processes for producing IEM management information. 62. There is a documented process for assessing IEM maturity. 63. Process to manage IEM stakeholder engagement are fully documented.	64. Processes to enable IEM governance meetings are documented predictably applied. 65. An IEM skills/competence system is documented and applied consistently. 66. Document processes exist for developing situational awareness and are consistently applied. 67. There are documented processes for producing IEM management information with predictable outputs. 68. There is a documented process for assessing IEM maturity that is consistently applied. 69. Process to manage IEM stakeholder engagement are fully documented and consistently applied.	70. There is an established (12+months) process for managing IEM governance meetings. 71. There is an established (12+months) IEM skills/competence system. 72. Document processes exist for developing situational awareness and are continuously improved. 73. Processes for producing IEM management information are embedded (12+months). 74. There is a documented process for assessing IEM maturity that is continuously improving. 75. IEM stakeholder engagement is fully embedded.

Technology	76. The only technology support for IEM governance activities are standard office applications (email, word processing etc) 77. There are no specialist technology tools to enable provision and analysis of information for IEM governance. 78. No use is made of technology for real-time monitoring of information supporting IEM governance activity e.g. Remote-condition monitoring.	79. Basic technology support is available for IEM governance activities e.g., simple spreadsheets to a capture ad analyse financial data. 80. Occasional use is made of specialist tools/systems for producing/analysing IEM data. 81. There is occasional or ad hoc use of real-time monitoring systems.	82. Standard office applications are well-utilised to document, analyse, share/present and retain information supporting IEM governance. 83. Some specialist technologies are used routinely to gather and analyse IEM related information e.g., operational performance data. 84. Some standardised use is made of real time data, but this is mainly for individual projects.	85. Standard office applications are used to their full capability (integrated data storage, remote meetings) to support IEM governance. 86. Specialist tools/systems are integrated to support IEM governance e.g., enterprise risk management software includes IEM-related risks. 87. Real time data is consistently used to support IEM governance where applicable.	88. Standard office applications are used to their full capability (integrated data storage, remote meetings) to support IEM governance. 89. There is established (12+months) integration of specialist systems to support IEM governance and drive improvements. 90. The use of real time data to support IEM is well embedded (12+months) and routinely improved.
Locations	91. Places, facilities, or premises are not relevant to the IEM governance provisions.	92. Places, facilities, or premises are not relevant to the IEM governance provisions.	93. Places, facilities, or premises are not relevant to the IEM governance provisions.	94. Places, facilities, or premises are not relevant to the IEM governance provisions.	95. Places, facilities, or premises are not relevant to the IEM governance provisions.
Suppliers	96. The impact of suppliers' activities on IEM is not considered in IEM governance activities. 97. No data on supplier's activities is included in IEM governance information. 98. Suppliers do not contribute to IEM governance activities.	99. The impact of suppliers' activities on IEM is rarely considered in IEM governance activities. 100. Data on or from suppliers to support IEM governance is considered on an ad hoc basis. 101. Suppliers contribute to IEM governance on an informal basis.	102. The impact of suppliers activities on IEM is regularly considered in IEM governance activities. 103. Data on or from suppliers to support IEM governance is considered on a regular basis. 104. Suppliers contribute to IEM governance on a formal, but infrequent, basis.	105. The impact of suppliers' activities on IEM is routinely and consistently considered in IEM governance activities. 106. Data on or from suppliers is integrated to support IEM governance activities. 107. Suppliers contribute to IEM governance on a formal and frequent basis.	108. The impact of suppliers' activities on IEM is routinely and consistently (12+months) considered in IEM governance activities. 109. Data on or from suppliers is integrated to support IEM governance activities. 110. Suppliers' contribution to IEM governance is formal and embedded (12+months).

8.2 Case Studies / Further Guidance

The following case studies / further guidance showcase real world examples of best practice from various industries when preparing for emergencies.

To protect individuals and organisations, case studies have been kept anonymous.

8.2.1 Emergency Response: Case Study #1 – UK response to Fukushima

Scientific advice and communication played a significant role in the response of the UK government to the accident at the Fukushima Daiichi nuclear power station after the Great East Japan Earthquake and Tsunami on March 11, 2011. The UK government, like many governments and organisations, used science to understand the progression of the accident and the implications for society.
In response to the emergency, the UK government activated its Scientific Advisory Group for Emergencies (SAGE). SAGE convenes in a matter of hours and typically meets once a day until the emergency situation is resolved. As such it works on a different time scale than other advisory groups within the UK. For the Fukushima accident, SAGE was responsible for helping to compile, peer review, and interpret scientific information relevant to the evolving situation, turning it into science advice for the prime minister and members of the Cabinet Office Briefing Room, which makes decisions in emergency situations.

At the time of the Fukushima incident, in order to understand the progression of the accident and its likely impact, scientists working in SAGE required information concerning the reactor designs, the state of the reactors before the accident, the release data from monitoring around Fukushima, and the forecast weather patterns. In this regard, a considerable amount of information was exchanged among similar groups in other countries and analysis was provided by the International Atomic Energy Agency, although the lack of real-time data was a problem. This exposes one big difference between delivering science advice for an emergency occurring within national boundaries as opposed to one outside. SAGE would have benefited from being better connected to decision-making groups in other countries.

Ultimately, from its assessment, the SAGE group was able to predict that the radionuclide release would be mostly confined around Fukushima. This meant that the hazard to people around Tokyo, where most UK citizens in Japan live, would be very small and thus there would be no need for an evacuation. Of course, people from areas besides Tokyo were also informed of any potential impact. Scientific evidence provided the confidence that underpinned the UK government advice to UK citizens in Japan and the decision not to mount an evacuation program for embassy staff. While the most cautious approach might seem to be to evacuate, that is associated with significant emotional, physiological, and health risks—to the people being evacuated and to their families and friends in Japan and back home.

8.2.2 Emergency Response: Case Study #2 – Waste Facility Fire

A Chinese lantern falling on a waste recycling site resulted in the ignition of approximately 100,000 tonnes of plastic and paper. The Fire Service rapidly declared a major incident, due to the scale of resources required to tackle the fire and the widespread pollution and fallout from the plume. This resulted in the establishment of all three tiers of multi-agency response, with the Fire Service declared as Lead Responder.

Operational Response
The Fire Service established an inner cordon, to ensure access to the site was limited to only responders with the appropriate Personal Protective Equipment and maintain the health and safety of responders from all agencies, many of whom were not equipped or trained for such an environment.

The Police established an outer cordon and advised the staff in nearby industrial units to evacuate the area, to ensure the health and safety of the public and create sufficient space for the Operational Commanders of each responding agency to coordinate their efforts.

The Local Authority established a vehicle cordon and set up diversion routes to minimise the impact on motorists and provide an area for responders' vehicles.

A rendezvous point (RVP) and access/egress routes were defined upwind of the site and communicated to all responding agencies.

Tactical Response
A Tactical Coordinating Group was convened at a nearby Fire Service training facility, due to its facilities for hosting large meetings, communication technology and significant outdoor space for vehicles and equipment.

The Scientific and Technical Advisory Committee, led by the Director of Public Health, also based themselves from this facility whilst deploying their water and air quality monitoring equipment around the wider area.

Strategic Response
The Strategic Coordination Group was established at the Police's Strategic Coordination Centre. All members of the LRF were familiar with this facility and encouraged to use it for incident coordination regardless of designated lead agency.

Whilst the Fire Service were Lead Responder, the Police were designated as lead agency for warning, informing and communication, to help relieve the Fire Service command structure and resources.

8.2.3 Responder Requirements: Case Study #3 – Highways Traffic Officer Service

A strategic Highways organisation established an operational response arm known as the Traffic Officer Service. Initially the organisation gained an understanding of existing traffic management related technologies and functions within other responder agencies and their control centres and developed a plan to transfer those to five new regional control centres. The main function of the regional control centres being to monitor and control traffic conditions and the Traffic Officer Service on road resources.

Traffic Officer Outstations were also located and set up around the road network with the development of operating procedures and arrangements for joint location of responding agencies. The Traffic Officer Service itself was defined along with on and off-road operations, roles, responsibilities, command, and control at regional control centres and on the road, resourcing requirements, shift patterns, staffing levels and patrol routes.

Working relationships with the emergency services were established in each region ensuring interoperability and multi-agency working, as well as the migration of technologies and functions from different agencies control rooms and the integration of multi-agency liaison officers at regional control centres.

8.2.4 Data Handling: Case Study #4 – Collision on the Railway Network: Using the DPA

A train carrying industrial waste collides with a commuter train on the outskirts of a city. The local A&E departments treat many wounded passengers. The next day it is found that the industrial waste included dangerous materials that were released during the crash. The Health Protection Agency requests lists of patients seen in the A&E departments so that it can follow-up those involved in order to advise on possible risks and to monitor for longer term health effects. A&E departments have not gained explicit consent from those individuals who have provided their personal data information. What should they do?

Outcome: The Data Protection Act 1998 allows processing for the purposes of 'vital interests' as well as for the provision of healthcare (under Schedule 3 of the Data Protection Act 1998). However, the common law duty of confidentiality does still need to be taken into account. Where the purpose of data sharing is to protect the health of the individual patient, consent could be implied as there is an expectation that data will be shared with other health professionals for this purpose. Where the purpose is the protection of the health of the wider population, a public interest case must be made for data to be shared without explicit consent. Where the HPA requires patient information because it wishes to monitor the long-term health effects of the accident on the wider population, then it should do so either with explicit consent or, where obtaining consent is impracticable, with support under Section 60 of the Health and Social Care Act 2001. While it could be argued that there is a public interest in disclosing information under the Data Protection Act 1998 to the HPA, since it is required for long term follow-up rather than an emergency response, the use of Section 60 powers would be a more appropriate approach.

Source: Data Protection and Sharing – Guidance for Emergency Planners and Responders. Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery: February 2007.

8.2.5 Command & Control: Case Study #5 – Guidance Notes – Security Control Room and Crisis Management Suite

An organisation developed guidance documentation from a Security Threat and Risk Assessment to allow for appropriate implementation and embedment of Security Control Rooms and Crisis Management Suites. Guidance included, but is not limited to:

SCR: The Security Control Room (SCR) should be considered both a high value asset and a highly critical asset. Compromise of any part of the SCR will significantly affect both the operation of the network from a continuity of service provision and / or a security perspective.

Crisis Management Suite: An alternative to providing additional space within the SCR is to provide adjoining space to act as a crisis management suite, room, or facility. The crisis management suite could be multipurpose, for example a meeting or conference room, but must be able to be switched into an operational crisis management space quickly and without any delay in reconfiguration.

Location The SCR should be located as far from any likely or identifiable threat sources as possible. This includes extreme crime threats (e.g., terrorist attacks) conventional crime threats (e.g., burglary) and resilience threats (e.g., fire, shut down of site).

Ease of access
To facilitate ease of arrival and departure, specifically during security or operational incidents, access to and from the SCR must not be hindered by large scale evacuations. Access to and from the SCR should continue in the aftermath of a significant event such as a terrorist attack. The SCR should be located away from public pedestrian and vehicle access routes and should be protected from the very events that the control room will be needed to manage and control.

Space allowances
The SCR should be designed to accommodate a population commensurate with an emergency response. Normally, unless other arrangements are in place, the SCR is the place senior decision makers will gravitate to when there is a crisis that needs managing. As a result, the population of the SCR can expand significantly and become highly charged given the nature of the event / emergency for which individuals are convened.

Welfare facilities
The SCR is to be functional 24 hours a day 365 days a year. It should include integrated and adjoining welfare facilities suitable for the highest expected population (the crisis or emergency population)
Staff working within the SCR and / or the crisis management space should not have to leave the physical high security boundary of the area to use the above welfare facilities.

Physical security
The whole control facility and the welfare facilities should be physically secured against forced intrusion / attack. Entry to the control room should be via an interlocked entry (two doors interlocked together or a single “portal” type entry system). Arrangements must be made for the entry of large items of equipment (such as computer racks and similar) whilst preserving physical security. The walls and any services penetrations (vents) should be to the same level. The primary control room should not include any windows.

Control of access
Control of access will take one of two forms:

- Access only through high security electronic access control with not less than dual factor authentication.
- Permitted access through intercom systems.
- Verified by CCTV (located before or at least within the airlock/tiger trap)

Wayfinding
The location of the SCR should not be obvious and should not be signposted. Anyone who requires access will know where it is and how to get to it without signs.

- Anyone authorised to visit should be escorted/hosted and therefore will be taken to and from the security control room.
- No purpose is served by marking the door to the security control room with its function or in signposting routes to the control room.

Fire
The SCR should be highly resistant to fire and smoke. It should represent a safe haven in the event of a widespread fire or significant terrorist event (such as a bomb blast) or security related event (such as a marauding weapons (including firearms) attack or crowd control situation.

The rooms should be constructed to resist the spread of fire for a considerable period of time (hours) and all routes to and surrounding areas should have a low of very low fire load. Water and mist fire extinguishing systems should be considered to approaches to and escape routes from the control room facility, including in spaces below and above the control facility. Water systems cannot be used in conjunction with live working electrical systems and are therefore not suitable for use within the SCR.

Video Surveillance System monitoring area
The VSS monitoring area of an active SCR should focus on the welfare and wellbeing of the operators. Display Screen Equipment Regulations will apply to the designs, both desks and the environment in which the desks sit. The area for VSS surveillance should be kept quiet and free from external disturbances. The internal environment should be suitably lit to avoid creating glare onto or reflection off the screens.

SCR / Crisis Management Suite Resilience
Where external factors pose significant difficulties, the SCR / Crisis Management Suite should be resilient enough to keep running. For example:

- Power failure – a backup power supply is required.
- Extreme / adverse weather – a resilient design should protect against flooding and other types of extreme and adverse weather.
- Loss of HVAC (heating, ventilation, and air conditioning) and other environmental problems – this could be simple responses such as providing extra clothing or water supplies.
- Staff shortages – where there is a lack of available staff, control room managers should be able to call on additional resources including staff both within and outside of the organisation (e.g., contract staff or from another organisation on a staff share agreement).

Resilience can be designed through duplication i.e., provision of two control room environments: the primary control room for use under normal operating conditions and a secondary backup control room for use in the event of a failure.

To maximise the value of the secondary control room (which may otherwise consider an expensive duplication) it could be used as the incident room unless the primary control room is unavailable. Ideally the primary and secondary control rooms are interchangeable, with duplicated security capabilities including CCTV feeds and hardware, IDS alarms, access control, all supporting infrastructure and IT.

Both control rooms should be tested and regularly maintained to the same standard.

8.3 Full Provision List

Provision Number	Provision Statement
Chapter 3. Emergency Response	
3.2.1	Emergency response and recovery arrangements ***SHOULD*** be flexible, adaptable, and tailored to reflect the circumstances. [1]
3.2.2	Emergency response and recovery arrangements ***SHOULD*** follow a common set of underpinning principles, and these ***SHOULD*** be applied at the local, subnational, and national levels [1]: • Anticipation • Preparedness • Subsidiarity • Direction • Information • Integration • Co-operation • Continuity
3.2.3	Rail Entities ***SHOULD*** follow the nationally agreed framework for managing emergency response and recovery to integrate plans and procedures within and between agencies and across geographical boundaries. [1]
3.2.4	Rail Entities' strategic aims ***COULD*** look beyond the immediate demands of the response and ***COULD*** embrace the longer-term priorities of restoring essential services and helping to facilitate the recovery of the affected communities. [1]
3.2.5	Strategic Commanders within responder organisations ***SHOULD*** establish clear aims and objectives for their organisations, to bring direction and coherence to the activities of multiple agencies under circumstances of sustained pressure, complexity and potential hazard and volatility. [1]
3.2.6	Rail Entities ***SHOULD*** establish systematic information management systems and embed them within multi-agency emergency management arrangements. [1]
3.2.7	Rail Entity Emergency Responders ***SHOULD*** include voluntary and private sector organisations in the multi-agency response and, as such, they ***SHOULD*** be integrated into the information management structures and processes that are established, trained, exercised, and tested. [1]
3.2.8	Rail Entities ***SHOULD*** put in place clearly defined structures to ensure support for key agencies to [1]: • Combine and act as a coherent multi-agency group. • Consult, agree, and decide on key issues. • Issue instructions, policies and guidance to which emergency response partners will conform.
3.2.9	Rail Entities ***SHOULD*** have in place mechanisms to manage emergencies which straddle Local Resilience Areas and regions or affect more than one part of the UK. [1]
3.2.10	Rail Entities ***SHOULD*** understand each other's functions, ways of working, priorities, and constraints. [1]
3.2.11	Rail Entities ***SHOULD*** support and assure openness between agencies by a commitment to the confidentiality of shared information when dealing with third parties and / or the public. [1]
3.2.12	Response and recovery arrangements ***SHOULD*** be reflective of trained and exercised ways of working within the rail industry and across the wider responder community. [1]
3.2.13	Rail Entities' procedures and capabilities ***SHOULD*** be well integrated between agencies and across the rail industry to ensure response and recovery work is effective. [1]
3.2.14	Rail Entities ***SHOULD*** work in a directed and co-ordinated fashion where multi-agency strategic coordinating groups are established. [1]

3.2.15	Rail Entities ***SHOULD*** consider response requirements to concurrent events and the requirements for risk-based prioritisation of emergencies in response arrangements. [2, 3]
3.2.16	Rail Entities ***SHOULD*** use Rail Safety and Standards Board (RSSB) Rule Book Module M1 GERT8000-M1 Issue 7 as a checklist when dealing with a train accident or incident. [12]
3.2.17	Rail entities ***SHOULD*** ensure terminology used during response and recovery is consistent with that used by multi-agency partners, ensuring interoperability, and reducing the risk of miscommunication.
3.2.18	Rail Entities ***SHOULD*** implement and maintain a response structure that will enable timely warning and communication to relevant interested parties. It ***SHOULD*** provide plans and procedures to manage the organisation during an incident. The plans and procedures ***SHOULD*** be used when required to activate business continuity solutions.
3.2.19	Rail Entities ***SHOULD*** implement and maintain a structure, identifying one or more teams responsible for responding to incidents.
3.2.20	The roles and responsibilities of each team and the relationships between the teams ***SHOULD*** be clearly stated.
3.2.21	Collectively, the teams ***SHOULD*** be competent to: • Assess the nature and extent of an incident and its potential impact. • Assess the impact against pre-defined thresholds that justify initiation of a formal response. • Activate an appropriate business continuity response. • Plan actions that need to be undertaken. • Establish priorities (using life safety as the first priority). • Monitor the effects of the incident and the organisation's response. • Activate the business continuity solutions. • Communicate with relevant interested parties, authorities, and the media.
3.2.22	For each team there ***SHOULD*** be: • Identified personnel and their alternates with the necessary responsibility, authority, and competence to perform their designated role. • Documented procedures to guide their actions, including those for the activation, operation, coordination, and communication of the response.
3.2.23	Rail Entities ***SHOULD*** document and maintain procedures for: • Communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate. • Receiving, documenting, and responding to communications from interested parties, including any national or regional risk advisory system or equivalent. • Ensuring the availability of the means of communication during an incident. • Facilitating structured communication with emergency responders. • Providing details of the organisation's media response following an incident, including a communications strategy. • Recording the details of the incident, the actions taken, and the decisions made.
3.2.24	Rail Entities ***SHOULD*** alert interested parties potentially impacted by an actual or impending incident and ***SHOULD*** ensure appropriate coordination and communication between multiple responding organisations.
3.2.25	Rail Entities ***SHOULD*** exercise their warning and communication procedures as part of their exercise programme.
3.2.26	Rail Entities ***SHOULD*** document and maintain business continuity plans and procedures. The business continuity plans ***SHOULD*** provide guidance and information to assist teams to respond to an incident and to assist the organisation with response and recovery
3.2.27	Business continuity plans ***SHOULD*** contain: • Details of the actions that the teams will take in order to continue or recover prioritised activities within the predetermined time frames and, monitor the impact of the disruption and the organisation's response to it. • Reference to the pre-defined threshold(s) and process for activating the response. • Procedures to enable the delivery of products and services at agreed capacity. • Details to manage the immediate consequences of a disruption giving due regard to the welfare if individuals, the prevention of further loss or unavailability of

	prioritised activities and the impact on the environment.
Chapter 4. Command & Control	
4.2.1	Rail Entities ***MUST*** ensure their warning and informing arrangements include the ability to communicate an incident, as an example warning and informing details ***COULD*** include [4]: a) Location. b) Access/egress routes. c) Date/time. d) Any rolling stock involved, plus its route. e) Incident timeline. f) Casualties/fatalities. g) No of passengers involved. h) Damage caused. i) Prevailing weather conditions. j) Dangerous goods on-board. k) Crew on-board. l) Railway property owner. m) Staff responsible for movement of the rolling stock. n) Number and type of vehicles involved. o) Emergency services in attendance. p) Incident Commander's contact details.[4]
4.2.2	Rail Entities ***SHOULD*** ensure Gold and Silver levels of command are clearly distinguished from the multi-agency coordinating groups that exist at the corresponding level. [1]
4.2.3	Rail Entities ***SHOULD*** apply the principle of subsidiarity (i.e., decisions should be taken at the lowest appropriate level, with coordination at the highest necessary level). [1]
4.2.4	Rail Entities ***SHOULD*** activate a Strategic Group on a precautionary basis before standing it down (this is deemed better practice than being forced to activate a Strategic Group belatedly under the pressure of an emergency). [1]
4.2.5	Rail Entities ***SHOULD*** start communication from a position of considering the risks and harm if they do not share information. [5]
4.2.6	Decision-making processes ***SHOULD*** always aim to be inclusive and, wherever possible, arrive at consensual decisions. [1]
4.2.7	Rail Entities ***SHOULD*** consider inputting to a SCG Science and Technical Advice Cell (STAC) to provide timely and co-ordinated advice on scientific and technical issues. [1]
4.2.8	Rail Entities Strategic Commander role holders ***SHOULD*** refer to RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers during an emergency response.[8]
4.2.9	Responders ***SHOULD*** work together to build shared situational awareness.[15]
4.2.10	Rail Entities ***SHOULD*** ensure all decisions during an emergency response are recorded by a trained loggist.[15]
4.2.11	Rail Entities ***COULD*** use the JESIP Joint Decision Model to ensure interoperability with other responding agencies.[15]
4.2.12	Responder organisations ***SHOULD*** consider and not discount sources of local or specialist knowledge, as they may be able to provide information about the incident or the location.[15]
4.2.13	Rail Entities ***COULD*** utilise the JESIP M/ETHANE structured model to collate and share information about an incident.[15]
4.2.14	Rail Entities Strategic Commanders ***COULD*** use the JESIP process for developing a working strategy during an emergency response.[15]
4.2.15	Responders ***COULD*** utilise the JESIP decision controls, to enable decision making during an emergency response.[15]

4.2.16	Responders ***COULD*** utilise the IIMARCH mnemonic as a briefing tool during an emergency response.[15]
4.2.17	Rail Entities ***SHOULD*** make use of Common Operating Picture during an emergency response to provide an overview of an incident which is accessible through a secure common information sharing platform.[15]
Chapter 5. Responder Requirements	
5.4.1	Rail Entities ***MUST*** cooperate with all Category 1 agencies involved in responding to emergencies. [1]
5.4.2	Rail Entities ***MUST*** cooperate with all Category 2 agencies involved in responding to emergencies. [1]
5.4.3	Rail Entities ***MUST*** cooperate with agencies within the wider resilience community who may be involved in responding to emergencies. [1]
5.4.4	Rail Entities ***MUST*** ensure any response follows emergency plans whereby arrangements specify to provide permitted inspectors (RAIB) access to the incident site and instruction that no evidence shall be removed (except in very limited exceptions and having notified the RAIB. [6]
5.4.5	Rail Entities ***SHOULD*** assist category 1 responders in making arrangements to warn and communicate with the public to ensure that they are made aware of emergencies. The public ***SHOULD*** be provided with information and advice, as necessary, if an emergency is likely to occur or has occurred. [7]
5.4.6	Rail Entities' Strategic Commanders ***SHOULD*** adopt the following behaviours set out in RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers [8]: • Be strategic – the Strategic Commander should seek to ensure that neither they, nor other members of the Crisis Management Team succumb to the temptation to actively involve themselves in providing the detailed response. • Be positive. • Be active. • Be reassuring. • Be apologetic – it is important to say you are sorry (noting that this is not the same as accepting responsibility). • Be visible, e.g., visit hospitals, emergency assistance centres, staff areas and the incident site as appropriate.
5.4.7	Rail Entities' Strategic Commanders ***SHOULD*** either complete the actions (set out in RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers, and Section 5.5.3) themselves or else satisfy themselves that they have been completed, during an emergency response. [8]
5.4.8	Rail Entities' Primary Support Operators ***SHOULD*** complete the actions set out in RDG-ACOP-016 Incident Response Duties of Primary Support Officers during an emergency response. [11]
5.4.9	All Rail Entity responders ***SHOULD*** utilise guidance for response roles and responsibilities and actions and tasks during an emergency response within relevant guidance notes. (Such as RDG-ACOP-016 Incident Response Duties of Primary Support Officers, RDG-OPS-GN-014 Major Incidents Preparation of Aide-Mémoires for Senior Managers, RDG-OPS-GN-034 RDG Guidance Note: Logging and Loggists, RDG Guidance Note RDG-GN016 – Competence of Train Operator Liaison Officers and RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident).[8,10,11,16]
5.4.10	Rail Entities ***SHOULD*** maintain response arrangements for extreme weather events and consult RDG-OPS-GN-015 Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems for actions during the response. [9]
5.4.11	During periods of extreme hot weather, Rail Entities ***SHOULD*** seek to maintain acceptable station and train environments. See guidance at RDG-OPS-GN-015 Extreme Weather Arrangements for considerations.[9]
5.4.12	Each Rail Entity ***SHOULD*** define who has responsibility for declaring a Major Incident or Critical Incident for rail industry response.[16]

5.4.13	The Owning Operator of the train involved in an emergency ***SHOULD*** assume immediate responsibility for leading and managing the humanitarian assistance response.[16]
5.4.14	Where trains of two or more Rail entities are involved in an emergency, the Rail entities concerned ***SHOULD*** agree which will provide the overall leadership and management of the combined humanitarian assistance response - normally this will be the Rail entity whose passengers are perceived as likely to have suffered the greatest number of casualties.[16]
5.4.15	The identity of the Rail entity leading and managing the humanitarian assistance response ***SHOULD*** be advised to Network Rail Route Control immediately.[16]
5.4.16	Following a Major Passenger Rail Incident, actions listed in Appendix C of RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident ***SHOULD*** be considered as it provides a simple checklist of requirements.[16]
5.4.17	Network Rail Managed Stations ***SHOULD*** provide Rail entities which operate within the station concerned with copies of current emergency plans and any proposed changes to these plans.[16]
5.4.18	In the event of an incident occurring at or near a large, multiple operator station, the Station Incident Officer ***SHOULD*** immediately call together the operator's representatives and provide accommodation, facilities and staff as agreed to operate RDG-OPS-ACOP-001. [16]
5.4.19	Smaller Rail entities ***SHOULD*** ensure that they are able to provide overall response leadership / management and therefore, as a minimum, maintain 2 - 3 persons who have sufficient understanding of the role of the ICT and how it will be deployed and are able to provide strategic direction to the Deployment Manager. [16]
5.4.20	Rail entities ***SHOULD*** hold details of ICT members centrally and ensure that these can be made quickly available within their own, and to other Rail entities in the event of an incident to supplement On Call arrangements. [16]
5.4.21	A Train Operator Liaison Officer (TOLO), reporting initially to and maintaining liaison with the Rail Incident Officer (RIO), ***SHOULD*** be appointed at the incident site by the Primary Support Operator. [16]
5.4.22	The ICT Strategic Lead and the ICT Deployment Manager ***SHOULD*** liaise to identify which of the following roles are necessary and ensure staff with competence as ICT members are nominated to undertake these roles:[16] • At the Casualty Bureau - a Rail entity representative with an understanding of the role and capabilities of the ICT and a general railway knowledge. • At a hospital - a Rail entity representative to provide a single point of contact between the hospital authorities. • At a Survivor Reception Centre - Survivor Reception Centre Liaison lead • At a nominated station(s) or other location - Humanitarian Assistance lead • At a Family & Friends Reception Centre – Family & Friends Reception Centre Liaison lead. • At a Humanitarian Assistance Centre - Humanitarian Assistance Centre Liaison lead. • With Local Authorities - A Local Authority Liaison lead.
5.4.23	Rail entities ***SHOULD*** ensure records are maintained to ensure that proper care and post incident follow up takes place as well as ensuring prevention against false claims. It is strongly recommended that this be done by means of a database system which complies with the requirements set out in the specification produced by RDG - Incident Care Team Survivor Relationship Management (SRM) System Requirements Specification, v1.1 dated 16 September 2019).[16]
5.4.24	The capturing, recording and retention of personal data by Rail entities ***MUST*** comply with current GDPR (General Data Protection Regulation requirements) guidance on how this should be approached within the context of ICT deployment is provided in RDG-OPS-GN-038 Data Protection Requirements During and After Incidents. [16]
5.4.25	An accurate log ***SHOULD*** be maintained of all activities undertaken as part of the humanitarian assistance response to an emergency. [16]
5.4.26	No employee, visitor or contractor on site ***SHOULD*** respond to an emergency by taking actions for which the individual is not trained or qualified which puts the individual or others at risk. [13]

5.4.27	Rail Entities ***COULD*** appoint a liaison with the task of transmitting information and facilitating communication between separated teams. [13]
5.4.28	Rail Entities ***SHOULD*** select team leaders with training experience and knowledge of the emergency procedures and forms. [13]
5.4.29	Responders ***SHOULD*** be briefed by the emergency preparedness and response plan coordinator on the assessment needs, response strategy and procedures, priorities to be observed and safety issues. [13]
5.4.30	Appropriate personal protective equipment ***SHOULD*** be distributed according to the context of the response required. [13]
5.4.31	Periodic breaks during the response ***SHOULD*** be established and enforced. [13]
5.4.32	Reporting procedures to the response command staff ***SHOULD*** be specified. [13]
5.4.33	In the early stage of an emergency, timely and accurate information ***SHOULD*** be provided for effective decision-making. [13]
5.4.34	Where there are no identified priorities in an affected area, decisions about what to retrieve or protect in situ ***SHOULD*** be made by assessing which items are most at risk of damage or which require stabilisation most urgently. [13]
5.4.35	The incident classification ***SHOULD*** be made by the first responder(s) to the incident or by those personnel most familiar with what has happened in discussions with first responders and/or the incident coordinator. [13]
5.4.36	Response ***SHOULD*** be guided by the response plan, ensuring that the plan is applicable to the on-going situation. [13]
5.4.37	A comprehensive record ***SHOULD*** be kept of all events, decisions, reasoning behind key decisions and actions taken. A daily log ***SHOULD*** be kept in a chronological order. [13]
5.4.38	Facilities on site where people can be held and/or treated for a few hours ***SHOULD*** be considered for no-notice events when [13]: • There is no time to evacuate before the hazard occurs. • Moving people would expose them to greater harm or dangerous conditions. • Immediate risk is unclear.
Chapter 6. Data Handling	
6.2.1	Rail Entities' Data Controllers ***MUST*** ensure that there is a legal basis for processing data. [5, 14]
6.2.2	Rail Entities' Data Controllers ***MUST*** ensure that the processing of data is fair by giving data subjects the necessary information when personal data is collected, or if this is not possible that they are exempt from this condition. [5, 14]
6.2.3	Rail Entities' Data Controllers ***MUST*** meet one of six conditions in order to process personal data as set out in Schedule 2 of the Data Protection Act 2018. [5, 14]
6.2.4	If sensitive personal data is to be processed, Rail Entities' Data Controllers ***MUST*** meet one of several further conditions set out in Schedule 3 of the Data Protection Act 2018 and regulations authorised under that schedule. [5, 14]
6.2.5	Rail Entities' Data Controllers ***MUST*** ensure that personal data is processed in accordance with the remaining principles of data protection as outlined above. [5, 14]
6.2.6	Rail Entities ***SHOULD*** keep a logbook or supply of log sheets available at a suitable location, either in or close to the room where it is expected that the Crisis Management Group will meet. [10]
6.2.7	Rail Entities ***SHOULD*** make known the location of the logbook or supply of log sheets to those likely to be members of the Crisis Management Team and also those within the organisation who have been identified as potential loggists. [10]
6.2.8	Rail Entities ***SHOULD*** document the location of the logbook or supply of log sheets within the company emergency plan. [10]

6.2.9	Rail Entities ***SHOULD*** ensure that the identified organisation loggists keep their own supply of logbooks/sheets in recognition that meetings of the Crisis Management Group may take place online. [10]
6.2.10	Rail Entities ***SHOULD*** initiate a log (or separate logs) of both events and decisions as soon as practicable once a tactical or strategic command team has been established. [10]
6.2.11	Rail Entities ***SHOULD*** maintain a log (or separate logs) until such time as the incident is concluded or responsibility passes to others. [10]
6.2.12	Rail Entities ***SHOULD*** ensure that logs comply with the following [10]: • Be CIA (Clear Intelligible Accurate) • Be in chronological order, with the time and date of each entry recorded (using the 24-hour clock) • Have entries numbered consistently and methodically. • Record facts, not assumptions/personal comments/opinions • Record non-verbal communication (e.g., nodding or shaking of heads to indicate agreement or objection) • Be complete, continuous, and contemporaneous (i.e., entries ***SHOULD*** be made at the time the information is received or at the earliest opportunity afterwards within a 24-hour period) • Include accurate timings of when information is received or sent. • If notes, maps, etc. are utilised, these ***SHOULD*** be noted within the log and as otherwise directed by the accountable person. • Relevant faxes, emails, text messages, notifications, phone calls, etc. should be similarly recorded. • Not include shorthand or abbreviations unless these are recognised terms (either generally or within the rail industry) • Show clearly the correction of any errors or omissions - when an alteration is necessary, a single line ***SHOULD*** be drawn through the error, correction entered and the alteration initialled. • No entry may be erased or obliterated. • There ***SHOULD*** be no overwriting or double entries. • There ***SHOULD*** be no blank pages or spaces. • No pages may be removed or inserted. • Must contain a signature immediately at the end of each session so that no additions can be made at a later date. • Each individual page ***SHOULD*** be numbered separately and consecutively and be signed-off as an accurate record by the loggist and chair of the meeting along with the date/time. • All changes of loggist ***SHOULD*** be clearly indicated by means of ruling off between the last entry made by the previous loggist and the first made by the next and with the names and signatures of both recorded on the log, along with the date/time.
6.2.13	Rail Entities ***SHOULD*** ensure that logs [10]: • Indicate the start date/time and details of the location of the meeting for which it is being kept. • Contain details of the loggist. • Record names, initials, and roles of all present (including those who leave or join mid-meeting and those joining remotely, e.g., online, by phone or video link). It is good practice for name badges to be worn to assist the loggist in identifying individuals but if this is not possible or such badges are not clear, the loggist should ask for clarification of the required details. • Record details of any actions, to whom they are assigned and when they have been completed. • Document the allocation of individuals to any specific functions or roles.
6.2.14	Rail Entities ***SHOULD*** ensure logs record any decisions taken, consciously not taken, or deferred, and the basis for these in the form of a rationale. [10]
6.2.15	Rail Entities ***SHOULD*** keep logs in a safe and secure location for retention as a potential source of evidence in case of future proceedings. [10]

6.2.16	Rail Entities ***SHOULD*** keep a copy of all logs and those copies ***SHOULD*** be securely stored in an alternative location. [10]

End of Document

Rail Delivery Group

National Rail

Rail Delivery Group Limited Registered Office, 1st Floor North, 1 Puddle Dock, London, EC4V 3DS
www.raildeliverygroup.com 020 7841 8000 Registered in England and Wales No. 08176197