Rail Delivery Group

National Rail

RDG Approved Code of Practice:

Rail Emergency Management - Recovery

RDG-OPS-ACOP-012
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, and securely 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 third 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 recover from emergencies within the remits of IEM activities. The Code addresses the legal and regulatory provisions required when recovering from emergencies and reflects industry guidance and other best practice for recovery. The Code outlines these requirements across key topics of incident debriefing, post incident reporting and information dissemination, Corrective and Preventative Actions (CAPA) Management and Business Continuity Management (BCM).

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	10/04/2024	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
AACE	Association of Ambulance Chief Executives
AAD	Annual Average Damages
AAP	Anticipate, Assess, Prevent
ACOP	Approved Code of Practice
BAU	Business-as-Usual
BC	Business Continuity
BCI	The Business Continuity Institute
BCM	Business Continuity Management
BIA	Business Impact Analysis
BT	British Telecom
BTP	British Transport Police
CAPA	Corrective and Preventative Actions
CBRN	Chemical, biological, radiological, or nuclear
CCA	Civil Contingencies Act 2004
CCTV	Closed Circuit Television
CNC	Civil Nuclear Constabulary
CNI	Critical National Infrastructure
COBR	Cabinet Office Briefing Room
CoP	Code of Practice
COP	Common Operating Picture
CRIP	Common Recognised Information Picture
DCLG (RED)	Department for Communities and Local Government (Resilience and Emergencies Division)
DfT	Department for Transport
EA	Environment Agency
ECHR	European Convention of Human Rights
EES	Environmental Evaluation System
EM	Emergency Management
EPC	Emergency Planning College
ESICTRL	Emergency Services Inter Control
FAQs	Frequently Asked Questions
FCO	Foreign & Commonwealth Office
FCP	Forward Command Post
FMEA	Failure Modes and Effects Analysis
FOC	Freight Operating Company
FTA	Fault Tree Analysis
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

HAZOP	Hazard and Operability Study
HMCG	Her Majesty's Coastguard
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
JOL	Joint Organisational Learning
LGD	Lead Government Department
LoA	Lines of Assurance
LRAG	Local Risk Assessment Guidance
LRF	Local Resilience Forum
LRP	Local Resilience Partnership
MBCO	Minimum Business Continuity Objective
MCA	Maritime and Coastguard Agency
MHSWR	Management of Health and Safety at Work Regulations 1999
MOD	Ministry of Defence
MTPD	Maximum Tolerable Period of Disruption
NCC	News Co-ordination Centre
NFCC	National Fire Chiefs Council
NHS	National Health Service
NPCC	National Police Chiefs' Council
NPSA	National Protective Security Authority
NRR	National Risk Register
NRSP	National Rail Security Programme
NSC	National Security Council
NSRA	National Security and Risk Assessment
ORR	Office of Rail and Road
PCG	Public Communications Group
PDCA	Plan, Do, Check, Act
RAIB	Rail Accident Investigation Branch
RAIRR	Rail (Accident Investigation and Reporting) Regulations 2005
RCCC	Regional Civil Contingencies Committee
RCG	Recovery Co-ordinating Group
RecCG	Multi-Recovery Co-ordinating Group
RDG	Rail Delivery Group
RfLi	Rail for London (Infrastructure)
RIAM	Rapid Impact Assessment Matrix
RM^3	Risk Management Maturity Model
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RPO	Recovery Point Objective
RRP	Rail Resilience Project
RRPSG	Rail Resilience Project Steering Group

RRPWG	Rail Resilience Project Working Group
RTO	Recovery Time Objective
SCC	Strategic Co-ordination Centre
SCG	Strategic Co-ordinating Group
SIDOS	Security In the Design of Stations
SITREP	Situation Report
SPoC	Single Point of Contact
STAC	Science and Technical Advice Cell
TfW	Transport for Wales
TOC	Train Operating Company
TOLO	Train Operator Liaison Officers
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 (BC)	Capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. *(ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).*
Business Continuity Management (BCM)	Business Continuity Management (BCM) 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. *(Business Continuity Institute Good Practice Guidelines 2023).*
Business Impact Assessment (BIA)	A process of analysing the impact over time of a disruption on the organisation. *(ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).*
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)
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).*
Interested Parties	A person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22300:2021 Security and resilience – Vocabulary)*
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)*
Maximum Tolerable Period of Disruption (MTPD)	Time frame within which the impacts of not resuming activities would become unacceptable to the organisation. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).*
Minimum Business Continuity Objective (MBCO)	The minimum capacity or level of services or products that is acceptable to an organisation to achieve its business continuity objectives during a disruption / incident / emergency. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22300:2021 Security and resilience – Vocabulary)*
Organisation	Person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives. *(ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).* 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)*
Organisational Culture	The values, attitudes and behaviour of an organisation that contribute to the unique social and psychological environment in which it operates. *(ISO 22361:2022 Crisis Management)*
ORR RM³ Model	The ORR's RM³ (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 RM³ model is well understood and used across the rail industry.
Policy	Intentions and direction of an organisation as formally expressed by its top management. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).*
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)*
Prioritised Activities	Activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption / incident / emergency. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22301:2019*

	Security and resilience – Business continuity management systems – requirements).
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)*
Recovery Point Objective (RPO)	The point to which information used by an activity is restored to enable the activity to operate on resumption to pre-defined levels. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22300:2021 Security and resilience – Vocabulary)*
Recovery Time Objective (RTO)	The time frame within the MTPD for resuming disrupted activities at a specified minimum acceptable capacity. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 22301:2019 Security and resilience – Business continuity management systems – requirements).*
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).*
Risk Assessment	Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment should be conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiries as necessary. *(Business Continuity Institute Good Practice Guidelines 2023) (ISO 31000:2018 Risk Management - Guidelines)*
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	The nominated and certified person charged with the role of on-site command

Officer	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).*
Top Management	A person or group of people that directs and controls an organisation at the highest level. *(Business Continuity Institute Good Practice Guidelines 2023)*

1 Introduction

1.1 Purpose

This RDG ACOP and supporting GNs contribute to a growing body of Rail Emergency Management CoPs that seeks to address the full IEM cycle.

Building on previous documents, this ACOP sets out requirements and provisions that focus on recovery 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 recovery 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 recovery 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 recovery from 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 **recovery** 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 CoPs*, aligned to the following structure:

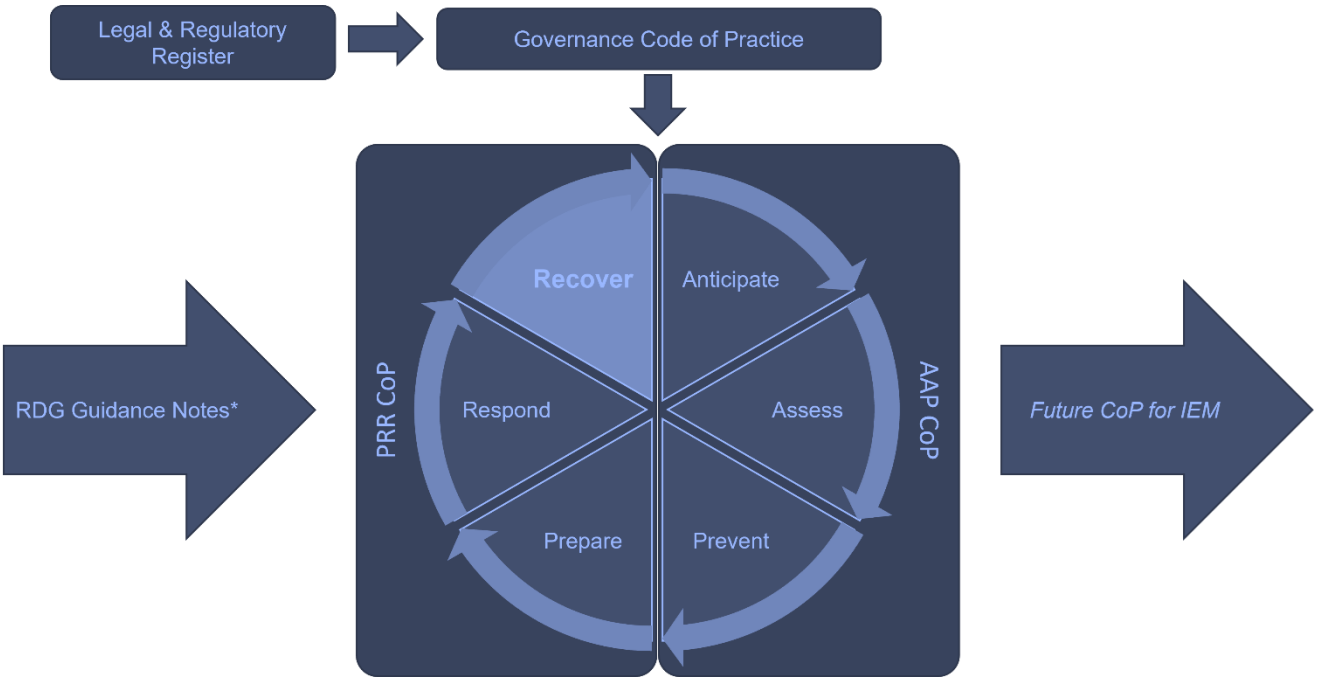

Figure 1 Document orientation

*** Other RDG Guidance Notes used to support IEM CoP 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 – Recovering from Emergencies
Chapter 4 – Incident Debriefing
Chapter 5 – Post Incident Reporting & Information Dissemination
Chapter 6 – Corrective and Preventative Actions (CAPA) Management
Chapter 7 – Business Continuity Management (BCM)
Chapter 8 – References
Chapter 9 – 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 3-7 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, recovery '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 3 – Recovering from Emergencies
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 – Recovering from Emergencies • Chapter 4 – Incident Debriefing • Chapter 5 – Post Incident Reporting & Information Dissemination • Chapter 6 – Corrective and Preventative Actions (CAPA) Management • Chapter 7 – Business Continuity Management (BCM)
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 – Recovering from Emergencies • Chapter 4 – Incident Debriefing

Table 1 Definition of provision statements.

All references consulted for this ACOP are listed in Chapter 8 References. The Provision Endnotes can be found in Section 8.1. 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 Recovery.

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.

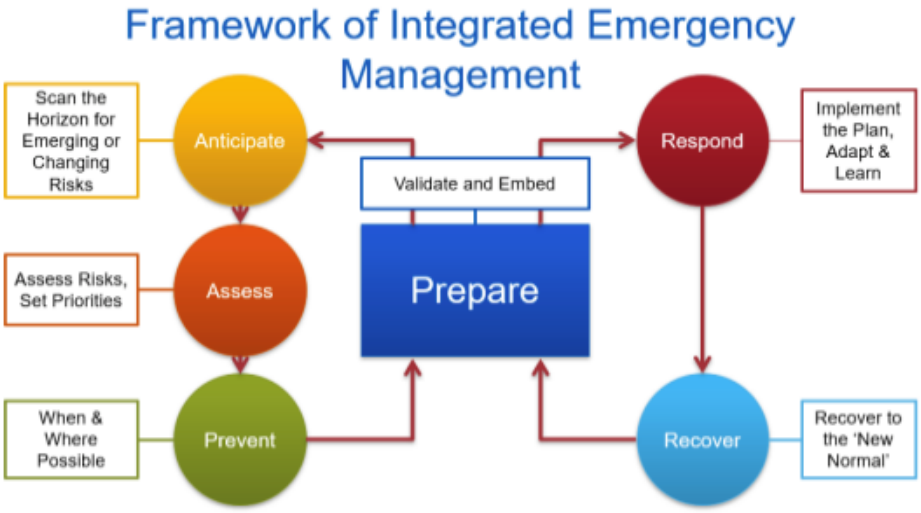

Figure 2 Framework of IEM, sourced from the Emergency Planning College.

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 CoP for Recovery.

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, issues and impacts.
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

Recovering from 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 CoP for Recovery.

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 should have existing risk management capabilities, processes, and structures in place to manage risks affecting their organisation.

The *RDG CoP 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 Register (NRR).

3 Recovering from Emergencies

3.1 Overview

Roles and responsibilities in the response phase of emergencies are well known, understood, and rehearsed. However, experience has shown that the recovery phase and the structures, processes and relationships that underpin it are harder to get right. Figure 3 demonstrates how the various structures to coordinate the recovery effort transition from the emergency response phase to the recovery phase.

Recovery is a complex and long running process that may involve many more agencies and participants than the response phase. It will be more costly in terms of resources, and it will undoubtedly be subject to scrutiny from the public, the community, the media, and politicians alike. It is therefore essential for the process to be based on well thought-out and tested structures and procedures for it to work in an efficient, coordinated, and orderly manner.

Recovery is defined as the process of rebuilding, restoring, and rehabilitating the community following an emergency, but it is more than simply the replacement of what has been destroyed and the rehabilitation of those affected. It is a complex social and developmental process rather than just a remedial process. There are four interlinked categories of impact that individuals and communities will need to recover from: Humanitarian (inc. Health); Economic; Infrastructure; and Environmental. The manner in which recovery processes are undertaken is critical to their success. Recovery is best achieved when the affected community can exercise a high degree of self-determination. Recovery can also look to improve what may have previously existed and potentially design-in more resilient infrastructure and processes, which must also be coordinated across the various organisations and their respective functional teams.

Previous emergencies have highlighted the need for effective co-ordination and communication between local responders and transport providers to manage an effective recovery within the transport sector should the need arise.

The recovery phase should begin at the earliest opportunity following the onset of an emergency, running in tandem with the response to the emergency. ‘Earliest opportunity’ is not defined in the national level guidance; however, the process continues until the disruption has been rectified, demands on services have returned to normal levels, and the needs of those affected (directly and indirectly) have been met. While the response phase to an emergency can be relatively short, the recovery phase may endure for months, years or even decades. Figure 3 illustrates how the structures to coordinate recovery efforts will change during the transition from response to recovery. Actual timescales and how the groups operate will be dependent on the circumstances of the event within the rail industry, the complexity of the recovery and the scale of infrastructure repairs required. Infrastructure managers, TOCs and FOCs will likely have different areas of focus within the recovery management structure but will likely all be involved to some extent.

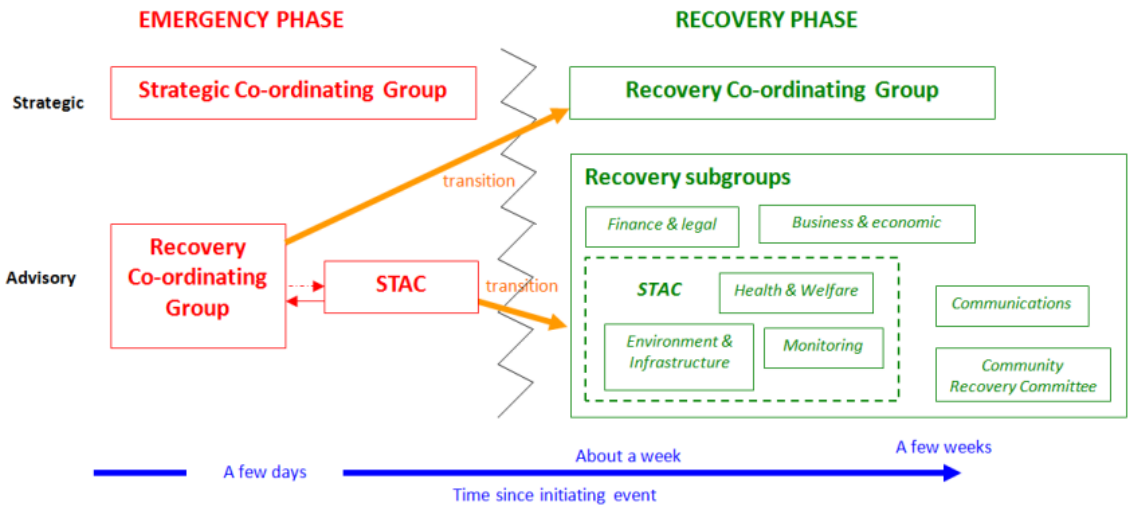

Figure 3 How the structures to coordinate the recovery effort will change during the transition from response to recovery.

Restoration of significantly damaged services can take time (weeks, months, or even years). Depending on

the equipment, structures and other infrastructure damaged, post-incident remedial work may need to be undertaken in phases and interim arrangements, such as reduced services or types of traction, may need to be introduced. In some cases, strengthening or stabilisation works may need to be undertaken prior to the removal of damaged rolling stock, structures, etc.

Responders and transport providers need to work together to provide support to the affected communities. The restoration of transport services should be seen as an important step in the return to normality after an emergency. Critical to this is a joint understanding of how long services will take to restore, and in which order services will be restored.

National recovery Guidance from Cabinet Office is available at National Recovery Guidance - GOV.UK (www.gov.uk) providing a single point of reference. The guidance covers:

- Topic Sheets on a wide range of recovery issues, which are intended to be used as guidance during the planning phase, and as a quick reference note, as required, during an emergency.
- A Recovery Plan Guidance Template, which can be tailored to local circumstances and used as a basis for recovery planning (and during the recovery phase of an incident if no plan is in place).
- Over 100 Case Studies from incidents and exercises, ranging from the Aberfan disaster (1966) to the 7/7 London bomb attacks, ensuring lessons previously identified can be shared.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Chapter 8, References. The Provision Endnotes can be found in Section 8.1. A full provisions table is provided in the appendices of this document.

3.2 Provisions

3.2.1 Rail Entities ***MUST*** cooperate with all requests in relation to Public Inquiries. [4]

3.2.2 Rail Entities ***SHOULD*** ensure tested structures and procedures are in place for the recovery phase following an emergency. [1, 2]

3.2.3 Rail Entities ***SHOULD*** ensure the recovery phase begins at the earliest opportunity following the onset of an emergency, running in tandem with the response to the emergency. [1, 2]

3.2.4 Rail Entities ***SHOULD*** follow national recovery guidance from Cabinet Office National Recovery Guidance - GOV.UK (www.gov.uk) in providing appropriate representation at the RCG, as well as communicating and sharing information with the RCG when necessary. [1, 2]

3.2.5 Rail Entities ***SHOULD*** follow RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Response Following A Major Passenger Rail Incident, to ensure survivors of Major Passenger Rail Incidents are dealt with safely, efficiently, and compassionately during the recovery phase. [3]

3.2.6 Rail Entities ***SHOULD*** consider attendance and contribution to sub-groups of the RCG, including management of multiple requests for attendance at different geographical RCGs in Emergency Preparedness cross-industry arrangements. [1,2]

3.2.7 Rail Entities ***SHOULD*** ensure recovery planning and management arrangements are included in and supported by training programmes and multi-agency exercises [1, 2]

3.2.8 Rail Entities ***SHOULD*** ensure recovery planning and management arrangements are included and clarified in role specifications, responsibilities, and capability expectations for responder role-holders and senior managers who will be expected to attend RCGs and manage recovery at site. [1,2]

3.2.9 It is important to ensure that the time, resources, and effort spent on planning is effective and will make a significant difference should an event occur. Planning for recovery ***SHOULD*** be [1,2]:

- Risk-based.
- Proportionate.
- Flexible, scalable, and non-prescriptive.
- Open to lessons learned from previous events.
- Inclusive.
- Collaborative.

- Coordinated.

3.2.10 Rail Entities ***SHOULD*** identify in advance the data and information requirements to support impact assessments and facilitate the development of recovery strategies. Rail Entities ***COULD*** focus on how to access the information, rather than gathering and maintaining all the data. This ***COULD*** include identifying the custodians of the data and information, considering how this will be developed, maintained, and shared. [1,2]

3.2.11 Rail Entities, as part of planning for recovery, ***SHOULD*** consider bringing together relevant partner organisations to start the thinking on issues that will need to be addressed, and agree the criteria, steps, process, or strategy to assist the decision making, should an event occur. [1,2]

3.2.12 Rail Entities ***SHOULD*** clarify and agree communication (including media) roles and responsibilities. For example, this may be between communications specialists working at local or national level or on issues that would be the focus for partnership working. [1,2]

3.2.13 Rail Entities ***SHOULD*** develop clear communication strategies and arrangements for recovery, industry wide. [1,2]

3.2.14 Rail Entities recovery arrangements ***SHOULD*** follow a common set of underpinning principles, from National Recovery Guidance from Cabinet Office. These ***SHOULD*** be applied at the local, subnational, and national levels. [1,2]

3.2.15 Rail Entities ***SHOULD*** utilise the reporting framework (recovery-reporting-framework-1.pdf (publishing.service.gov.uk) for recovery, introduced by Cabinet Office. [1,2]

3.2.16 Rail Entities ***SHOULD*** contribute to Impact Assessments carried out by local authorities and LRFs, via the RCG sub-groups. [1,2]

3.2.17 Rail Entities ***SHOULD*** develop a media handling strategy and arrangements for recovery that can be used industry wide, ensuring it aligns to the wider multi-agency RCG strategies. [1,2]

3.2.18 Rail Entities ***COULD*** ensure senior representatives attend community engagement meetings where requested. Senior representatives should be members of the RCG, and be clear about the agreed multi-agency strategy, actions, and messages. [1,2]

3.2.19 Rail Entities ***SHOULD*** plan for planned and spontaneous memorial events and be aware of the symbolic importance and emotion that will be attached to the management of such tributes. [1,2]

3.3 Guidance Notes

3.3.1 Recovery Principles

The principles of recovering from emergencies within the National Recovery Guidance from Cabinet Office are:

- Recovery is an enabling and supportive process, which allows individuals, families, and communities to attain a proper level of functioning through the provision of information, specialist services and resources.
- Effective recovery requires the establishment of planning and management arrangements, which are accepted and understood by recovery agencies, the community, and any other stakeholders.
- Recovery management arrangements are most effective when they recognise the complex, dynamic and protracted nature of recovery processes and the changing needs of affected individuals, families, and groups within the community over time.
- The management of recovery is best approached from a community development perspective. It is most effective when conducted at the local level with the active participation of the affected community and a strong reliance on local capacities and expertise. Recovery is not just a matter for the statutory agencies - the private sector, the voluntary sector and the wider community will play a crucial role.
- Recovery management is most effective when agencies involved in human welfare have a major role in all levels of decision-making which may influence the well-being and recovery of the affected community.
- Recovery is best achieved where the recovery process begins from the moment the emergency begins. It is recommended that the Recovery Co-ordinating Group (RCG) is set up on the first day of

the emergency and run in parallel with the Strategic Coordinating Group (SCG).

- Recovery planning and management arrangements are most effective where they are supported by training programmes and multi-agency exercises which ensure that the agencies and groups involved in the recovery process are properly prepared for their role. (See RDG-OPS-ACOP-010 IEM Preparation for further details on training & exercising).
- Recovery is most effective where recovery management arrangements provide a comprehensive and integrated framework for managing all potential emergencies and where assistance measures are provided in a timely, fair, and equitable manner and are sufficiently flexible to respond to a diversity of community needs.

Rail Entities should ensure recovery planning and management arrangements are extensively covered and clarified in role specifications, responsibilities, and capabilities expectations for responder role-holders and senior managers who will be expected to attend RCGs and manage recovery. Points to consider include:

- What capabilities and knowledge do people need for their role in support of recovery from an emergency?
- Consider the needs of personnel assuming strategic, tactical, or operational, as well as technical and public facing roles.
- What training, familiarisation and refresh do they need to maintain their readiness?
- What opportunities will they have to rehearse their role?
- What support will they need to perform effectively? For example, communications, facilities, equipment, and administrative assistance.

3.3.2 Recovery Structure and Organisations

The local authority will usually lead the recovery process and chair the RCG. They will need strong support from a wide range of multi-agency local and Category 1 and 2 responders, including Rail Entities where impacted by the incident. This is likely to involve input or attendance from the full breadth of the rail industry, including infrastructure managers, TOCs and FOCs depending on the type of incident.

A likely structure for the recovery effort is shown in Figure 4 below, integrating specific areas of expertise with the four pillars of impact assessment described later in this section.

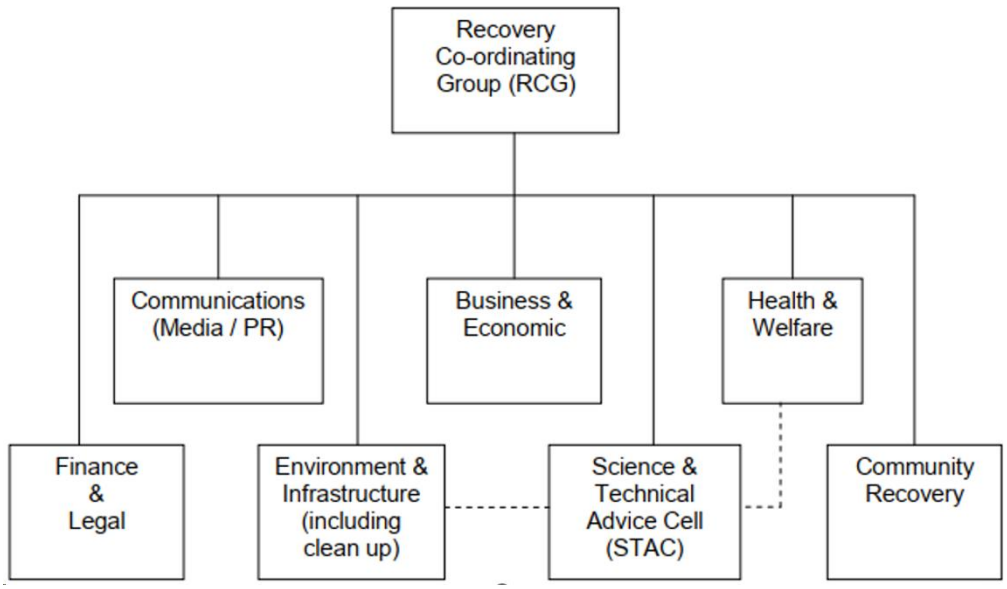

Figure 4 Recovery Coordinating Group Structure (Source: National Recovery Guidance June 2013).

Membership of the RCG and sub-groups will be decided by the local authority based on the type of emergency. Rail Entities are likely to be requested at many of these groups if the emergency is on, near or affecting the rail network. Having established a prior relationship with LRF agencies will provide a significant advantage when working through the issues which a recovery operation will present. Further guidance on working with LRFs can be found in RDG-OPS-ACOP-010 IEM, Planning and RDG-OPS-ACOP-011 IEM, Response.

Where the emergency crosses a local authority boundary but remains within one LRF area, the affected authorities will need to decide whether to establish one RCG at the LRF level, or whether to operate separate RCGs in each local authority area. To ensure there is consistency of approach, no duplication of effort, and to

reduce the burden on agencies such as Rail Entities, that cover more than one local authority area, the recommended approach is to have **1 RCG to cover all affected communities within the LRF area**. A Multi-Recovery Co-ordinating Group (RecCG) may be convened where recovery action is needed across a number of neighbouring RCGs who would benefit from over-arching co-ordination or enhanced support.

The RecCG will observe the principle of subsidiarity, recognising that decisions should be taken at the lowest appropriate level. The RecCG will not interfere in local command and control arrangements. They will provide a mechanism for ensuring that local responders can be as informed as possible in the decisions they must take.

Where the emergency crosses LRF boundaries, consideration will be given to the potential assistance that the Regional Civil Contingencies Committee (RCCC) could provide in ensuring consistency of approach, reducing duplication of effort, minimising the burden on responders, and facilitating the sharing of information, support, and mutual aid.

In the initial stages of the emergency, it is advisable to start big and then scale down. An early assessment should be made of the responding organisations capacity and resources, and mutual aid agreements should be activated as required. If co-ordination is required at the multi-LRF level, contact should be made with the DCLG RED to discuss how this may best be delivered. In Wales, contact should be made via the Welsh Government and consideration should be given to establishing a Civil Contingencies Group or Wales Civil Contingencies Committee.

In an event requiring national level recovery structures to be activated, the Civil Contingencies Secretariat (Cabinet Office) will decide the lead government department, based on the type of emergency. The regional resilience team in the relevant government office will provide the conduit for communication with the nominated lead government department. Where emergencies cross constitutional boundaries within the UK, it is clearly still vital that recovery efforts are co-ordinated. However, it should be recognised that different legislation and funding streams, as well as different structures, may be in place in the devolved administrations. Areas that border devolved administrations should, in the planning phase, agree how recovery would be co-ordinated in the event of cross-government border incidents and record this in the local plan.

3.3.2.1 Activation of the Recovery Co-ordinating Group

Activation of the RCG is initiated by the local authority, usually following a request by / agreement with the SCG. An important part of the work of the RCG during the response phase of an emergency is to develop a recovery strategy and inform the SCG of this strategy to ensure decisions made by the SCG do not compromise medium to long term recovery. The RCG reports into the SCG until the SCG stands down.

At the start of the recovery process, a clear recovery strategy should be developed and agreed by the RCG. The recovery strategy could cover some, or all, of the following key objectives:

- An impact assessment (covering impacts on residents, businesses, infrastructure, environment, etc.) if not passed down from the SCG, is carried out as soon as possible and is regularly updated.
- Determine at an early stage if there is an opportunity for longer term regeneration and economic development as part of the recovery process.
- Determine at an early stage if there is an opportunity to enhance the resilience of the area (physical, social, intelligence, data, information etc.).
- A concise, balanced, affordable recovery action plan is developed that can be quickly implemented, involves all agencies, and fits the needs of the emergency.
- The local voluntary sector organisations and the community are fully involved in the recovery process.
- All agencies work closely with the community and those directly affected, including on monitoring and protection of public health.
- Utilities (e.g., gas, water, and sewerage) and transport networks are brought back into use as soon as practicable.
- A pro-active and integrated framework of support to businesses is established.
- All affected areas are restored to an agreed standard so that they are suitable for use for their defined future purposes.
- Environmental protection and recovery issues are co-ordinated. (The communication requirements will be different from the response phase with more emphasis on two-way communication and engagement, rather than the control/command and information provision associated with the response phase).
- Information and media management of the recovery process is co-ordinated.
- Effective protocols for political involvement and liaison (parish, district / county / unitary and parliamentary) are established.

3.3.2.2 Handover from response phase to recovery phase

To ensure that all agencies are aware of the implications and arrangements for handover from the response to recovery phase, it is suggested a formal meeting is held within a few days of the start of the emergency. Membership at this meeting should, as a minimum, include the SCG Chair and the affected local authorities, and should consider:

- The criteria to be used to assess when the handover can take place from the SCG to the RCG
    - In practical terms this is likely to be a gradual process, with significant engagement required between the established SCG members and initial RCG membership.
- The process for the handover: it is recommended that a formal handover process is followed and a suggested handover certificate is shown in the *Recovery Plan Guidance Template (National Recovery Guidance recovery-plan-guidance-template).* As part of the handover process, consideration needs to be given to how information collated as part of the response phase is effectively, efficiently, and securely handed over to those responsible for managing the recovery phase and should ideally include an up-to-date impact assessment.
- Communications to other responding agencies and the community about the handover.

3.3.2.3 Location and Operation of the RCG

In the early part of the recovery phase (both when the RCG is running in parallel with the SCG, and after the lead is handed over from the SCG chair to the RCG chair), there is much merit in agencies being (and remaining) co-located, if possible, to establish communication links and ensure ready interaction between agencies can be maintained.

Once individuals return to their desks, the demand to return to the day job and catch up may become irresistible and the recovery process may falter. If the Strategic Co-ordination Centre (SCC) is not available, then alternative (probably local authority) premises should be found. That said, some agencies necessary to the recovery process may not have been involved in the response phase and will need to be integrated into the process.

The lead recovery officer from the local authority needs to manage this progression carefully and instil the importance of agencies being closely allied, especially in the early stages of recovery.

The frequency of RCG meetings will be determined by the group on a case-by-case basis. In the early stages, the group may meet two or three times a day, but this is likely to reduce over time, maybe to once or twice a week.

Source: Norfolk Resilience Forum Recovery Guidance 2020

3.3.2.4 Stand Down of the Recovery Co-ordinating Group

The Chair of the RCG, in discussion with the RCG members, will decide when it is appropriate to stand-down the Group. The needs of the community will be key to this decision and should inform the decision.

The length of time that the RCG is required to continue meeting will vary according to the nature and scale of the emergency. Some emergencies may have long term issues to consider, such as health monitoring. The RCG will be closed once there is no longer the need for regular multi-agency co-ordination and the remaining issues can be dealt with by individual agencies as a part of their normal business. Depending on the recovery issues being addressed, it may be possible for some of the RCG sub-groups to close prior to the main RCG standing down. The decision to stand-down the RCG will be communicated to all affected agencies by the RCG Chair / Secretariat.

3.3.3 Impacts of Emergencies

Emergencies affect communities in a wide variety of ways. To understand what recovery comprises it is necessary to map out who is affected and how the emergency has affected them. The impact of emergencies goes well beyond those directly affected by an emergency (e.g., through injury, loss of property, evacuation). Emergencies affect, for example, onlookers, family and friends of fatalities or survivors, response and recovery workers, and the wider community, as well as the economy and businesses, physical infrastructure, and the environment.

To understand how emergencies affect individuals and their communities and thus prioritise and scope the recovery effort, it is important to understand how emergencies impact upon the environment people live and work in. Figure 5 below is a framework for understanding these impacts and the steps that may need to be taken to mitigate them. There are four interlinked categories of impact that individuals and communities will

need to recover from. The nature of the impacts – and whether and at what level action needs to be taken – will depend in large part on the nature, scale, and severity of the emergency itself.

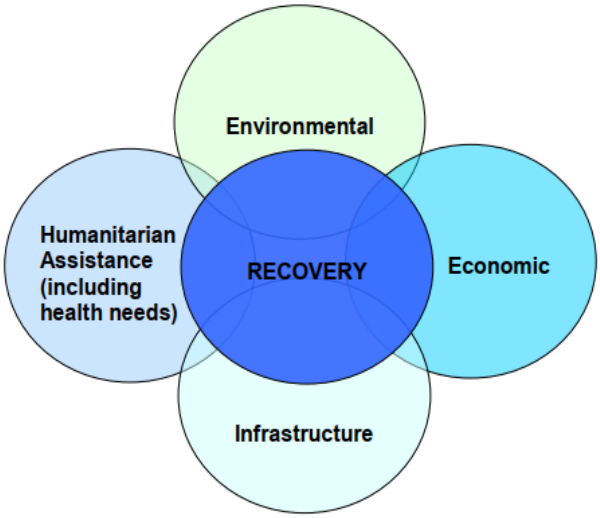

Figure 5 Framework for understanding impacts of emergencies (Source: National Recovery Guidance June 2013).

Examples of what may be included in the four categories above can be seen in the table below (Table 4). Although the scope for recovery activities is very broad, by planning in advance, recovery capability can be built around four key themes: humanitarian, economic, environmental and infrastructure.

Humanitarian (including Health)	Physical impacts (including Individuals' health, housing, and financial needs)
	Psychological impacts
	Deaths
	Community displacement
Economic	Economic and business recovery
Infrastructure	Disruption to daily life (e.g., educational establishments, welfare services, transport system)
	Disruption to utilities / essential services
	Damage to residential properties and security of empty properties
Environmental	Pollution and decontamination
	Waste
	Natural resources and habitats

Table 4 Examples of types of issues faced (Source: National Recovery Guidance June 2013).

The National Recovery Guidance includes topic sheets on each of these four themes, plus on generic recovery issues. This guidance is regularly updated and can be found at: https://www.gov.uk/national-recovery-guidance. Each topic sheet also has links to case studies from numerous incidents and exercises, highlighting how these issues were addressed and what lessons were identified from this process.

3.3.3.1 Impact Assessment

There is no UK policy on how to carry out impact assessments during the recovery phase of an emergency.

Impact assessments will usually be led by the local authority, but with support from other relevant partners in the RCG and its sub-groups. There is no specific Lead Government Department (LGD) for impact assessments, although clearly many departments will have an interest in the results of any impact assessment that is carried out following an emergency. Local authorities are expected to fund the costs of any impact assessment process. A reimbursement scheme may be applicable and/ or available depending on the nature of the emergency and the LRF and local authority involved.

An impact assessment should be started early and regularly updated. It is likely to develop over time from a rough and ready assessment, probably covering the more immediate needs of people, to a more refined assessment of longer-term humanitarian needs and economic development. It will probably be started off by the SCG who pass it to the RCG quickly once it is established.

Impact assessment involves the systematic and co-ordinated collection and sharing of information about the

overall size and scale of the impacts of an emergency. The establishment of the scale of an event is one of the most critical initial activities to be undertaken in an emergency.

To be effective, impact assessment requires a pre-determined strategy, which should include a combination of physical inspections and indicator contacts relevant to the event. A key aspect is establishing the limits of the affected area by establishing who is not affected. For a long duration event such as flooding, it can be an iterative process involving the sending out of initial assessments to others who may be able to add to the overall picture. Any such initial reports should clearly indicate where there are areas that have not been reported upon and if these areas have been affected.

The earliest information regarding any emergency usually comes via telephone calls. It is easy to overlook areas without communications, and therefore not able to report their situation. Where communications have failed or do not exist, the seeking out of information can only be done by some form of reconnaissance.

The impact assessment will enable the RCG to prioritise and resolve any resource conflicts. As part of the assessment process, the businesses that can best help the community to recover should be prioritised and addressed first. The RCG should decide what action is needed to improve the situation and monitor the progress on that action. The actions need to be SMART (Specific, Measurable, Achievable, Realistic and Time Based). The impact assessment is a continual cycle until the rail community affected has returned to normal or as close to normal as can be expected. The frequency of reassessment will gradually become longer until there is no longer any further benefit to be gained, or that the situation has been accepted or fully resolved.

The assessments would best be carried out by the specialist sub-groups of the main RCG of which the Rail Industry would be part, should there be a rail incident or emergency. There are a variety of impact assessment methods, such as:

- **Expert Judgment**: This method relies on the insights and opinions of subject-matter experts. Their informed assessments help evaluate the potential impacts of an action or intervention.
- **Quantitative Models**: These models use data and mathematical equations to predict the effects of an intervention. Quantitative models are useful for assessing complex systems or long-term impacts.
- **Cumulative Impact Assessment**: This approach considers the combined effects of multiple actions or interventions; it helps identify synergies, trade-offs, and cumulative impacts over time.
- **Matrices and Interaction Diagrams**: These visual tools map out relationships between different factors (e.g., actions, outcomes, stakeholders). They provide a structured way to assess impact.
- **Rapid Impact Assessment Matrix (RIAM)**: RIAM is a simplified method that quickly assesses the potential impacts of an intervention. See Section 7.3.3.5 on Risk Assessments and Matrices for further guidance.
- **Battelle Environmental Evaluation System (EES)**: Developed by Battelle, an EES assesses environmental impacts by considering various factors such as ecological, social, and economic aspects.
- **Business Impact Analysis (BIA)**: A BIA is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. See Section 7.3.3.1 for further guidance.

Source: International Institute for Sustainable Development 2024.

Each specialist sub-group will agree the most appropriate assessment method, based upon the type of incident and their particular area of focus.

Impact assessments ultimately aim to establish a relationship between an organisation’s inputs, outputs, and outcomes, helping make informed decisions and promote accountability to stakeholders. The RCG and its subgroups will deem the most appropriate impact assessment model.

It is possible to anticipate a range of issues that the RCG and its subgroups will need to address during the recovery phase of an emergency. These will be dependent on the circumstances of the event, the geographical location and the combination of land use, demography, and the surrounding socio-economic landscape.

3.3.4 Recovery Communications Approach

Good public communication is vital to the successful handling of any emergency and should be incorporated in contingency planning. When an emergency occurs, the key communications objective will be to deliver accurate, clear, and timely information and advice to the public, so they feel confident, safe, and well informed.

The impact of the media during crisis response cannot be underestimated, and media coverage during the recovery phase can be more of an ongoing challenge. The news media (radio, TV, print) remain the primary means of communication with the public in these circumstances. Increasingly, digital, and social media are used to provide a further source of real time information and advice for the public. It is important to note that information can be generated by official or unofficial sources, and this will need to be fully considered when developing a media handling strategy or a crisis communications plan. This could cover:

- Development of a recovery top line brief
- Identifying the events and issues for which proactive and reactive messaging may be needed.
- Identifying key audiences, messages, channels, information flows and activities.
- Planning to actively gauge public and media reaction through the monitoring of social media, broadcast, and print media.
- Consider the use of social media channel to reach key audiences with recovery briefing and messaging.
- Pre-planning and production of written 'positions' or holding statements, where possible.
- Development of recovery FAQs.
- Development of briefing and information sheets which can be adapted at short notice for particular needs.

During a recovery from an emergency, there are often public information messages which are as important as during the height of the emergency, yet the media interest may have waned or moved onto other issues. Conversely, the need to get important information out to the public remains a priority. The continued involvement of local media remains important at this stage.

Different organisations may take the media lead for the response and recovery phases. For example, the police or other emergency service may be in the lead during the response, but the recovery phase may be led by the local authority.

As a situation moves towards the recovery phase, the national media interest is likely to be confined to very significant milestones or specific events (the publication of a report or an anniversary, for example). It is at this stage that the role of the local media may become even more important.

During the recovery phase, the focus of the media will be specific areas; responsibility, costs, support for those involved, how organisation are rebuilding their business, how communities are coping. It is important to work with the media to communicate information effectively via a range of options from special programmes, slots on local radio / TV programmes, to inserts in local papers / digital / social media.

In the event of an emergency, the News Co-ordination Centre (NCC) may be established by the Cabinet Office Communications Group. The NCC is there to support the LGD in their communications management of the overall incident. The nature of the NCC's support will depend on the circumstances, but it could take the form of securing extra staff to work in the LGD or in an operations centre, helping to compile and distribute briefing material, designing, and establishing websites, forward planning, collation of requests for ministerial interviews and preparing media assessments.

Additionally, the NCC could provide a central press office to co-ordinate the overall government message. The Department of Communities and Local Government, Resilience and Emergencies Division can play a role in assisting local responders multi-LRF working arrangements.

The use of social media in an emergency can help to reach a broad range of people and organisations as it permits instant transmission of messages directly to followers. It also contributes to the public's situational awareness as an emergency unfolds and can help responders gain a more accurate picture. Through social media responders can counter erroneous information and manage speculation and rumours. However, it is important to recognise that social media cannot be used in isolation in an emergency; and that it should not be seen as an alerting tool. Rail Entities need to build up a core of followers before an emergency and ensure there is a level of trust with their followers before social media can be used effectively during an emergency. This should be undertaken in conjunction with a marketing / communications team within the entity for specific support.

During large scale / long running incidents, a decision will need to be taken regarding the establishment of an emergency media centre. Where possible, the media should be consulted on this (if the site does not work for them, they will not use it.) The requirement will depend on issues such as the potential longevity, scale, and seriousness of the incident(s). Issues such as the need for accreditation of foreign media, the availability of suitable locations (including power, parking, and IT facilities) and the opportunities for media access to the

site(s) themselves will need to be considered.

Specific issues for consideration in the recovery phase where fatalities are involved can be found in the RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident.

Emergencies place enormous demands on all involved in the response and recovery effort. Media interest can create undue stress and pressure and careful planning of staggered handovers between shifts is essential. The pooling of resources in a joint media centre may be helpful in this respect. This relates not only to operational personnel but also to those providing administrative and specialist skills, e.g., in website technology.

In the much longer term, experience has also shown that media interest will be rekindled on the anniversary of events, and provision will need to be made to consider how to work with the media in such cases.

3.3.4.1 Communicating with the public (Scotland)

As well as physical impacts, major incidents can have a lasting psycho-social effect on communities and individuals. Some areas may not return to exactly how they were prior to the incident, and the transition to a new normality can be difficult. Decisions made early in the response process can have lasting ramifications in the months and years that follow and enable a good recovery. The Scottish Government is likely to take an early interest in the recovery, public reassurance, and the support of continuity of essential services.

Response and recovery are intimately bound together and, while the emergency response will usually be the focus, both should be considered from the outset of an incident, and the communications leads for response and recovery involved in all Public Communications Group (PCG) (Scotland) meetings.

Once the immediate emergency response has concluded, there may be a formal handover where the chair of a PCG passes from the responding agency (for instance Police Scotland) to the lead agency for recovery (for instance the local authority).

At the heart of a good recovery is a focus on ensuring that individuals and communities are supported, heard, and treated with dignity and respect. This can begin early in the incident by ensuring that their basic needs are met, and in the longer term through ongoing support.

This could involve the opening of rest centres, the co-ordination of practical support and assistance, the organisation of public events, and the promotion and recognition of unity and resilience.

Many of these issues are not communications decisions in isolation but will require close working between communicators and operational leads to agree and implement.

More information on the role of the PCG in recovery can be found in the dedicated guidance Preparing Scotland - Recovering from Emergencies in Scotland.

3.3.5 Litigation / Public Inquiries

Statutory and non-statutory public inquiries may be set up for a wide variety of reasons to deal with important matters, however those relevant to recovery will be public inquiries set up to inquire into the causes of a disaster of some kind.

The primary legislation for this is the Inquiries Act 2005. This Act creates a comprehensive new statutory framework for inquiries set up by ministers to investigate matters of public concern. It replaces over 30 different pieces of legislation on inquiries, consolidating much of the current legislation and codifying past practice for inquiries. It covers the setting up of inquiries, the appointment of people to conduct them, their procedures and their powers, and the submission and publication of reports. The 2005 Act will only be used for inquiries that need to have statutory powers. There will still be a place for non-statutory inquiries. There will also be some subject areas, such as financial services, where it is appropriate to keep a specialised framework in place.

Within the 2005 Act, there is a requirement for the inquiry chairman to have regard to the need to control costs. Sections on payment of inquiry and witness expenses provide the Minister with a degree of budgetary control, while ensuring that the inquiry has adequate funds. Proposed procedure rules should strengthen a chairman's hand in controlling costs.

Under the 2005 Act, inquiries will be able to compel any information that could be compelled by a court in normal civil proceedings. Failure to co-operate will be a summary offence, and inquiry chairmen will also have the option of asking the High Court to enforce any orders that they make. During the last few years, there have been several inquiries set up to investigate the circumstances surrounding disasters.

Whilst primarily public inquiries are governed by the Inquiries Act 2005 and other legislation, public inquiries may also be established on a non-statutory basis. No guidance has been issued to local authorities on the handling of public inquiries. Inquiries can also be set up under a range of other Acts, including but not limited to the: Health and Safety at Work Act 1974, Merchant Shipping Act 1995, Railways Act 2005, and the National Health Service Act 2006. Inquiries do not determine civil or criminal liability. They are not a substitute for court proceedings, and they don't punish people or award compensation. They are a tool for establishing facts and preventing a problem from reoccurring.

It is expected that all persons called to give evidence to a public inquiry will fully co-operate. The inquiry team may offer advice to those appearing as witnesses or otherwise involved and ensure that such persons are aware of the terms of reference and what may be expected of them. In cases of doubt, the persons concerned should clarify their position. Under no circumstances should a person be expected to incriminate themselves when answering a question.

The cause of an emergency may be immediately apparent but should not be presumed until investigations (and possibly prosecutions) are completed. Whilst the rescue of survivors must take precedence, once the rescue phase is complete and the scene has been declared safe, it must be protected from interference or unnecessary movement. The site must be treated as a crime scene, and its protection is vital to preserve evidence. However, a key consideration will be to restore services at the earliest opportunity.

The purpose of any prosecution is to prove beyond reasonable doubt that an offence has been committed, rather than establishing the circumstances of an accident or incident. Witnesses are essential to investigations and prosecution and fall into the following categories:

- Survivors.
- Eyewitnesses.
- Emergency service personnel.
- Technical witnesses.
- Identification witnesses.

3.3.6 Community Engagement

Experience has shown that it is vital for responders to involve the community affected in the recovery process. This can help enable an efficient and rapid return to normality and enables a community to come to terms with a major incident.

For example, an early public meeting can allow people to air their concerns and opinions; help the community to come to terms with the consequences of the emergency; and empower people to influence the scope and order of priorities in the recovery process. Depending on the nature of the incident, the inclusion of representatives from local faith communities and other relevant groups should be considered, as they can often be the key link into minority groups, especially where there are language barriers or sensitivities within the community. Having separate meetings for affected residents and businesses can be particularly useful, bearing in mind their differing information requirements.

The elected members of the community affected have a duty as community representatives to act as a conduit for information between their communities and local responders. As civic leaders, they are involved with many aspects of community life and can provide a focus for gathering concerns, as well as providing a mechanism for responders to obtain information from the public. Their inclusion in any community discussion is essential.

Any meeting should be as structured as possible; include presentations on the situation at that time; and involve senior representatives from all the agencies involved who need to be able to answer questions authoritatively. These senior representatives should preferably be members of the RCG, and be clear about the agreed multi-agency strategy, actions, and messages.

Further guidance on the level and type of data that is permitted to be shared can be found in RDG-OPS-ACOP-011 IEM, Response.

3.3.7 Commemoration

Commemoration, whether it be a one-off event such as a memorial service or anniversary event, or a more permanent physical memorial, is an important part of the recovery process. Commemoration gives an emergency recognition and can aid those affected as part of the moving on process, particularly when those affected are able to be involved in the planning.

Memorial events

Memorial events may take place at incident sites, within local communities, or at a national level. They often occur after the initial aftermath of an incident. Events may be arranged around the time of anniversaries. For those involved in preparing these, great care should be taken to ensure communications are sensitively planned and managed.

Spontaneous memorials

Experience has shown that spontaneous memorials, including tributes such as flowers, teddy bears, and cards, are often placed at incident sites by the public. Responding agencies should plan for this and be aware of the symbolic importance and emotion that will be attached to the management of such tributes. Voluntary agencies are often able to assist in this regard, and a number have useful experiences to offer.

4 Incident Debriefing

4.1 Overview

Debriefs are a critical source of capturing lessons identified during an incident, or just as importantly, during training and exercising. Responder agencies must embed within their local debrief processes; the facility to capture lessons relating to interoperability between any organisations, the application of Joint Emergency Services Interoperability Principles (JESIP) for joint working and models / national resilience capabilities. Adoption of locally owned lessons supports the process of lessons that are identified, captured, shared, and effectively learnt for all UK responder agencies.

4.1.1 Response Debriefing

Debriefing is an integral part of any organisation's processes and should be embedded into organisational learning and development. The process enables improvements in the way Rail Entities operate and continuously develop processes, structures, and procedures.

Debriefing is not about a culture of pointing the finger, or apportioning blame. It may identify weaknesses in levels of knowledge, skills, and abilities, as well as weaknesses in organisational systems and processes. It should promote open and honest discussion and should not compromise any ongoing investigation. It is a process by which lessons can be identified, discussed, analysed, and incorporated into organisational thinking and learning, creating future good practice. In essence the debriefing process looks for answers to the following three questions:

- How well prepared were we?
- How well did we perform?
- What can we achieve better in the future?

Further information and guidance on debriefings are included in Section 4.3.

Any debrief following a Critical Incident should be a formal process with identified outcomes. It should be chaired or facilitated by an appropriate individual within the Rail Entity or multi-agency response organisation and supported by a structured debrief trained member of staff, or external debriefer.

Where there has been a considerable amount of media attention, there will be inevitable strains between media and local responders' interests. Arranging for senior media representatives to meet with senior members of the emergency services and other organisations involved in the incident, some weeks later, can assist both sides in looking at how information was provided and identifying ways in which arrangements can be improved.

4.1.2 Recovery Debriefing

It is important to ensure that a continuous evaluation of the recovery phase takes place, and that any issues identified are captured and actioned. The formal debrief process (which may be repeated at key milestones during a prolonged recovery phase) should identify issues from all partners involved in the recovery process. Consideration should also be given to obtaining views from the affected community (residents and businesses).

The recovery phase of an emergency has additional complications in that the timeline is longer, and it potentially involves more stakeholders than the response phase. Typically, it has peaks of activity, such as around the time of an anniversary, as well as routine ongoing work to address the physical and psychological effects of the emergency.

For most emergencies, it is appropriate to carry out debriefs at different stages in the recovery, when certain milestones are achieved, or a period of time has elapsed. It may be months since the emergency until the first recovery debrief can take place, but there should be a continual process for debriefs throughout recovery.

The collation of lessons identified from the recovery phase of emergencies and exercises should be the same as those used for the response phase.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Chapter 8, References. The Provision Endnotes can be found in Section 8.1. A full provisions table is provided in the appendices of this document.

4.2 Provisions

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

4.2.2 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]

4.2.3 Rail Entities ***SHOULD*** embed within their local debrief processes; the facility to capture lessons relating to interoperability, the application of JESIP Principles for joint working and models and national resilience capabilities. [6]

4.2.4 Debriefing ***SHOULD*** be honest and open, and its results disseminated widely, but should not compromise any ongoing investigation. [1]

4.2.5 Rail Entities ***SHOULD*** ensure a debrief following a Critical Incident follows a formal process with identified outcomes. It ***SHOULD*** be chaired or facilitated by an appropriately trained individual within the rail entity or multi-agency response organisation and supported by a structured debrief trained member of staff, or external debriefer if considered appropriate. [6]

4.2.6 Rail Entities ***SHOULD*** arrange for senior media representatives to meet with senior members of the emergency services and other organisations involved in the incident, some weeks later, to assist parties in looking at how information was provided and identifying improvements in the future. [2]

4.2.7 Rail Entities ***SHOULD*** ensure that a continuous evaluation of the recovery phase takes place, and that any issues identified are captured and actioned as necessary. Consideration **SHOULD** also be given to obtaining views from the affected community (residents and businesses). [2]

4.2.8 Rail Entities ***SHOULD*** ensure the collation of lessons identified from the recovery phase of emergencies and exercises is the same as those used for the response phase. [1]

4.2.9 Rail Entities ***SHOULD*** ensure hot debriefs are facilitated by an appropriately trained representative and comments from all responding organisations and roles ***SHOULD*** be captured and recorded in whatever process is considered the most appropriate for the circumstances. [6]

4.2.10 Rail Entities ***SHOULD*** ensure appropriate attendance at multi-agency cold debriefs. A review of initial and further comments received should take place, along with an action plan with accountable owners for each action. These actions ***SHOULD*** be accepted by Rail Entities and be cleared as soon as possible, where applicable. [1]

4.2.11 Rail Entities ***SHOULD*** consider utilising the JESIP multi-agency debrief template for all multi-agency incidents. [6]

4.2.12 All critical incidents **SHOULD** be subject to ongoing review and monitoring. Rail Entities ***SHOULD*** ensure reviews have senior management oversight and are managed at an appropriate level of Command. [1]

4.2.13 Rail Entities ***SHOULD*** ensure the points captured at the hot debrief are recorded on the Command and Control log as well as the relevant debrief form. [1]

4.2.14 Rail Entities ***COULD*** consider utilising the debrief process considerations, structure and meeting model detailed at 4.3.2.2. [6]

4.2.15 Rail Entities ***SHOULD*** actively seek to find and share more effective ways of dealing with emergencies. [5]

4.2.16 Rail Entities ***SHOULD*** strive for continual improvement in response to all emergencies. [5]

4.3 Guidance Notes

4.3.1 Hot Debrief

Hot debriefs occur immediately after an incident to capture key issues. This is particularly important if health and safety issues are evident. For critical incidents the facilitator is likely to be the Senior Manager responding at the scene. Comments from all responding organisations and roles should be captured and written down in whatever process is considered the most appropriate for the circumstances.

This will also allow an opportunity for individual personal reflection. Where exercises or pre-planned events have taken place, this may be in the form of an evaluation sheet. Other options include seeking a scribe to record the key points or use of a recording device, for which a transcription can be provided at a later time.

A single agency debrief will occur when an incident or emergency only involves one Rail Entity. However, some incidents may involve other agencies, which would then require a multi-agency approach to debriefing, whereby the SCG take the lead.

An internal debrief may occur when an emergency has the potential to affect the reputation, staff, or procedures of a Rail Entity. Alternatively internal debriefs will occur where a multi-agency incident has occurred, and it is important to identify issues relevant to the rail industry before engaging in a multi-agency debrief.

4.3.2 Cold Debrief

Where a multi-agency incident has occurred the multi-agency cold debrief will be the culmination of the debrief process and may occur many weeks after the event. In these circumstances it is important to establish who will deliver the debrief, in what format, who will be represented from each organisation and in what manner it will take place.

As with exercise debriefs a review of initial and further comments received should take place, along with an action plan with accountable owners for each action, and areas for improvement or lessons learnt. Each issue should fall into one or other of the following categories:

- Issues for which local resolution is appropriate,
- Issues of a generic nature for which resolution at a regional or national level is appropriate.

These issues, as modified by written comments, should be translated into agreed actions for resolution.

Actions, once accepted by the appropriate responsible organisation, should be cleared as soon as possible.

4.3.2.1 Multi-Agency Debriefing Process

The JESIP multi-agency debrief template to be used by an SCG following stand down of the response phase to an incident or emergency can be found here; Multi-Agency Debrief Template - JESIP Website. The template follows the JESIP principles of:

Co-locate

- Were commanders easily identifiable?
- What command structures were in place?
- Did commanders meet face to face?
- Was a Forward Command Post (FCP) established?
- Did commanders have timely on-scene briefings?

Communicate

- Was common terminology used?
- Was an Airwave interoperability talk group used?
- Was relevant information shared across all services and control rooms throughout the incident?
- Was M/ETHANE used to pass information to control?
- Were effective communications established between:
  - Operational & tactical commanders / Commanders and control rooms / Emergency service commanders and other responding organisations / Local emergency service control rooms / Emergency service control rooms and national co-ordinating centres.

Coordinate

- Did Commanders use the JDM as single decision model?
- Were Capabilities & Responsibilities identified?

- Were joint decisions on priorities made and if so, how were the priorities arrived at and agreed?
- Were actions joined up and therefore efficient and effective?
- Were ALL on scene resources used appropriately?
- Was there an understanding of the capability, capacity, and limitations of each other's assets?
- Did someone take the lead co-ordinators role during Multi-Agency meetings?

Jointly understand risk

- Were threats and hazards identified, understood, and treated different by each emergency service?
    - Had the risk of this incident been appropriately identified in risk registers?
    - How could this incident feed back into risk assessments to improve planning and preparation?
- Were limitations and capabilities of people and equipment identified?
- Was a joint understanding of risk achieved by sharing information about the likelihood and potential impacts of threats and hazards? e.g., sharing of risk assessments.

Shared situational awareness

- Did Commanders have a common understanding of what has happened, what is happening now and the consequences of events?
- Did each of the emergency services understand their roles in resolving the emergency?
- Was M/ETHANE regularly used to provide a Common Operating Picture (COP).
- Was the Joint Decision Model utilised identifying: Situation:
    - What is happening?
    - What are the impacts and risks?
    - What might happen and what is being done about it?

4.3.2.2 Single Agency Debriefing Process

The process for debriefing a critical incident or emergency is key to ensuring that lessons are identified, recorded, and implemented in respect of organisational learning.

There should be a transparent process that will ensure when critical incidents are declared they are properly managed and debriefed within a given timescale.

All critical incidents should be subject to ongoing review and monitoring to ensure they are being progressed and managed in a timely and efficient way. Such reviews are likely to receive senior management oversight and therefore need to be managed at an appropriate level of Command. Reviews will help shape the debriefing process particularly where the incident is protracted.

Major Incidents will always be subject to a debriefing process; however, this may take place through a number of different mechanisms such as via Public Inquiries, Boards of Inquiry etc. These may therefore be Government rather than agency led and may lead to multiple debrief processes.

Where a critical or major incident is declared a Command and Control process will be initiated. This will allow Strategic oversight of the response. Part of this Strategic oversight should be to ensure that the process of debriefing begins at the conclusion of the incident. A hot debrief of staff at the conclusion of the event should ensure the points captured are recorded on the Command and Control log as well as the relevant debrief form.

Where the incident is protracted and may overlap several shifts or responder roles then information via a hot debrief may occur more than once. In addition, this is an opportunity for referral of any issues to other departments.

A number of members of staff within an organisation should be trained in formal debriefing techniques. The actual debrief will need to consider a number of factors. For example, the numbers of persons to be debriefed and the type of incident involved. For large debriefs there should be a broad section across all Command levels (Strategic, Tactical and Operational) including a representation of the various roles involved. Once the formal debrief has occurred the findings should be provided in a written report for consideration of the contents and recommendations for the best way to capture these and inform organisational learning and good practice.

Where necessary the findings may need to be referred to other departments in order to ensure organisational learning is captured such as People Development, Health and Safety or Emergency Planning. These departments will need to update plans or consider exercising particular aspects of the report. Similarly, rail entities may need to refer aspects of the report for inclusion on Risk Registers.

In some cases, it may, due to the nature of the incident, be necessary to publicise the findings of the report or

to brief individuals who may have been affected as a consequence of the actions at the initial incident. Further information and guidance on post incident dissemination of information is included in Chapter 5.

The following considerations form the basic principles underlying the debriefing process. This will apply equally across the range of types of debrief:

- Debriefing should be tailored to the group involved and the type of operation.
- The goal of debriefing should be to facilitate personal, group and organisational learning and improvement. Essentially, debriefing requires the individual and/or group to recall and reflect on information and experience so that meaning can be drawn, and learning facilitated. Recall can be encouraged in numerous ways using writing, drawing, thinking, and talking within the context of the meeting.
- Debrief facilitators should aim to create an atmosphere where individuals feel able to be open and honest without fear of reprisal. Debriefs should not be used to apportion blame or to criticise individual behaviour. It should be recognised that everyone has the potential to make mistakes and with hindsight is always possible to see alternative methods of achieving results. A successful debrief will allow those present to critically analyse their own actions and constructively contribute to a discussion about all other elements of the event.
- The debrief facilitator should adopt a neutral stance in relation to the event or operation in order that the end product comes from the group being debriefed.
- The debrief facilitator should familiarise themselves with an overview of the incident, those attending and any issues that have already been identified. They should use this information to plan a broad structure for the debrief. This may include viewing the Command and Control log or other supporting material.
- Debriefs should be conducted in a manner that will encourage an open and honest debate which is supportive, constructive, and conducive to learning.
- The objectives of the incident should be listed, and a discussion promoted to assess whether the objectives were achieved.
- It is best to go through events in a manner that is easily understood by all participants. Generally, most debriefs will be conducted in a chronological order, so participants can follow the sequence of events. This is usually broken down into three stages. Pre-Event, During the Event and Post Event.
- The debrief needs to be controlled, directed and to the point. It should not be allowed to descend into a free for all.
- The process should be exploratory and should aim to find the reasons and thought process behind actions.
- The sequence of events should be discussed with the staff concerned for each task performed. Questions should be asked to make sense of events.
- Praise and encouragement should be given whenever individuals have performed with skill and competence.
- Health and Safety issues should be highlighted, and action required for improvement identified and assigned to an individual.
- Where individual competence has not been demonstrated to acceptable standards it is important that their training needs are identified and addressed either personally or through line management. It is important that such discussion is made outside of the debrief process so as not to cause embarrassment or invite personal criticism.
- The aim of the debrief is to examine team performance and not that of individuals. Great care must be taken to ensure that the debriefing process does not attribute blame to any individual or cause any participant to feel uncomfortable.
- Questions should be managed throughout to ensure an equal level of understanding and that all participants have an opportunity to contribute.
- Sufficient time should be allowed for the debrief to ensure it is not rushed and meets its objectives.
- All visual aids should be considered and utilised as necessary.
- Refreshments should be provided as appropriate.
- The facilitator should aim to conclude the meeting with a summary of the learning identified throughout the debrief.
- The outcomes of the debrief must be suitably recorded and where the learning would benefit other members of the force disseminated into organisational learning as appropriate.

A suggested structure for debriefing is demonstrated below:

The Planning Stage: It is important to spend time to plan the details of the debriefing process prior to the actual meeting to ensure the maximum benefit is gained. The first stage is to decide that a debriefing is to be

held and to allocate roles. There are four main roles as identified below. These could be performed by one individual or broken down into several roles.

- Initiator - The person who requests and is ultimately responsible for the debriefing process.
- Planner - The person who plans the debriefing process based on key areas and questions (Debriefer)
- Facilitator - The person who chairs and guides the debrief.
- Participants - Those who are invited and take part in the debrief process.

The following points may be used as an aide-mémoire when considering the key areas and questions that need to be considered in the planning stage:

- **Purpose**
  - What is the aim of the debrief?
  - What event is being reviewed?
  - What period of time is to be covered?

- **Authority Issues**
  - What additional role does the initiator wish to adopt?
  - Will anyone in a position of authority be taking part or wish to be present?
  - Confirm the level of disclosure or confidentiality of the material required during the debrief meeting.

- **Participants**
  - Are the participants aware of the debrief?
  - Are they willing to take part?
  - What experience do they have of debriefing?
  - Consider questions they may ask.

- **Numbers**
  - How many people were involved in the event?
  - How many people are keen to take part in the debrief?

- **Time**
  - What is the minimum and maximum time available for the debrief?
  - When does the debrief report have to be completed?

- **Location**
  - Where is the best place for the debrief to be held in the circumstances?

- **Leader**
  - Who will lead the debrief?
  - What experience does the facilitator have of debriefing?

- **Resources**
  - What maps, charts, photos, reports etc should the facilitator and/or participants have access to both before and during the debrief?
  - Visual aids required?

- **On the day**
  - Room set up.
  - Resources in place?

As with all meetings, debriefs need to be opened in such a manner as to place those present at ease and create a safe learning environment. The following is an example of a planned opening for a formal debrief:

- Welcome.
- Brief overview of incident.
- Overview of debrief aims.
- Overview of the debrief method, including potential actions following the debrief i.e., what written outcomes will be produced and how will the recommendations be acted upon.
- Opportunity for the participants to introduce themselves and their role in the incident.
- Ground rules for the debriefing process.

Events should be gone through in a chronological manner which all participants can follow using the three stages of Pre-Event, During Event and Post Event. It may be helpful to have a prepared timeline or flow chart to assist. This can be used to prompt the memory of the participants and encourage a greater range of viewpoints. There are different ways of achieving the discussion:

- By asking participants to share their thoughts on post it notes which can then be collated together for group discussion.
- Using a flip chart or whiteboard to raise and record issues.
- Breaking into groups to discuss aspects of the incident being debriefed.

The following model (Figure 6) could be used for the basis of the debriefing meeting:

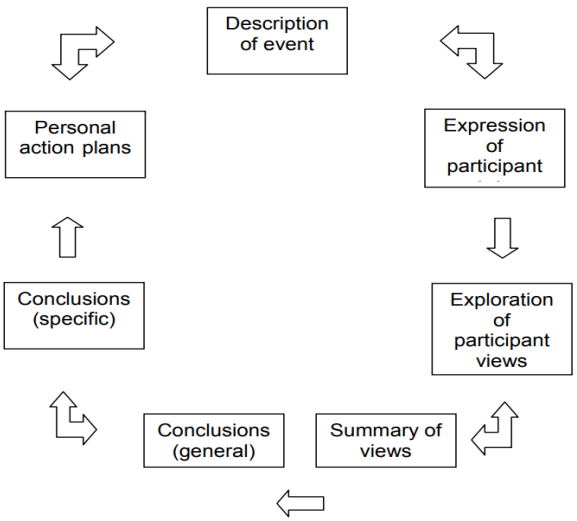

Figure 6 Debriefing Meeting Model.

- Description of Event – This stage should be used to examine the chronology of the event.
- Expression of Participant Opinions – Having established the Chronology of the event participants should be given the opportunity to reflect on their experiences for a couple of minutes.
- Exploration of Participant Views - This stage should be used to allow the participants to discuss those elements of the incident that were a success and/or required improvement.
- Summary of Views – After all participants have had the opportunity to explore both the positive and negative elements of the incident it is important to take time to summarise the views and identify any common themes.
- Conclusions (General) – This stage should be used to draw any general conclusions from the incident. These will usually be in the form of recommendations. This may involve breaking into a group phase.
- Conclusions (Specific) – This stage should be used to draw conclusions about individual actions or events during the incident that went well or required improvement.
- Personal Action Plans – Time should be allowed for participants to reflect on their own experiences and feedback to allow them to develop action plans for similar incidents in the future. These should follow the SMART principles.

After the participants have been given sufficient time to complete their action plans it is important to allow any remaining questions to be asked before bringing the meeting to a close.

4.3.3 Recovery Debriefing

There is currently no recovery-specific guidance on how to carry out recovery debriefs, but learning from those carried out following recent incidents shows that the following key points may be useful:

- Where a RCG is established to lead the recovery from an emergency, it would be sensible to hold a debrief session before the disbandment of the group (or any of its sub-groups). It is suggested that internal debriefs within an organisation are held first, with these thoughts then being brought together in a multi-agency debrief.

- A strategy for obtaining views from the community (residents, businesses, etc) should be developed and agreed with Elected Members and the RCG. Such a strategy might include the use of:
  - Questionnaires

- Focus groups
- Websites and
- Existing networks (e.g., business networks, parish councils, community groups, etc).

- Obtaining views from the community is likely to require an extended debriefing programme (in terms of the time needed to issue questionnaires, collate responses, gather focus groups, etc), but the debrief still needs to be carried out in a timely fashion so issues are still fresh in people's minds. The use of an independent company or facilitator (possibly an Emergency Planning Officer from a different area) to take forward the public debrief programme should be considered to (1) demonstrate impartiality – particularly if the emergency has been contentious, and (2) because of the personnel resource such an exercise is likely to require.

- There is likely to be considerable pressure to release the recovery debrief report into the public domain, particularly if the community has been consulted. It is therefore recommended that a pro-active approach is taken to this issue, with an early statement being made about the consultation mechanisms, the fact that the Emergency Response and Recovery report will be published (with details of how, e.g., on a website, etc), and with an indicative publication date being provided.

- Documents produced during the debrief process should be held for a suggested five years, but then reviewed in light of possible inquiry or investigation timelines prior to disposal. Everyone should maintain their own documents in case of an inquiry.

4.3.4 Lessons Identified and Lessons Learned

It is essential that the industry assesses, builds knowledge capital, learns, and continually improves for better future outcomes. Learning should be developed through various activities, which may include a programme of simulations and operational exercises specifically focused on building preventative and predictive capacities. Peer involvement in such exercises can be a means of learning. Stress data should be used to create future projection models to allow effective scenario planning. Recovery should be viewed as an opportunity to transform, drive innovation, and change to build back stronger and better.

Source: RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance.

Under JESIP there now exists a capability to capture national learning via the Joint Organisational Learning (JOL) process (see Chapter 5). This is accessible via the Resilience Direct site, which is available to a multi-agency audience.

Debriefing allows individuals, departments and the wider organisation and industry to examine strengths and weaknesses and to refine planning and procedure processes. Personal reflection is one of the benefits of debriefing and an opportunity for individuals to examine their own behaviour and use the opportunity for reflective practice. Such a principle can become embedded into organisational thinking which in turn leads to a more effective workforce. It is widely accepted that the most effective way of learning as an adult is by following the stages of the experiential learning cycle shown in the diagram below (Figure 7).

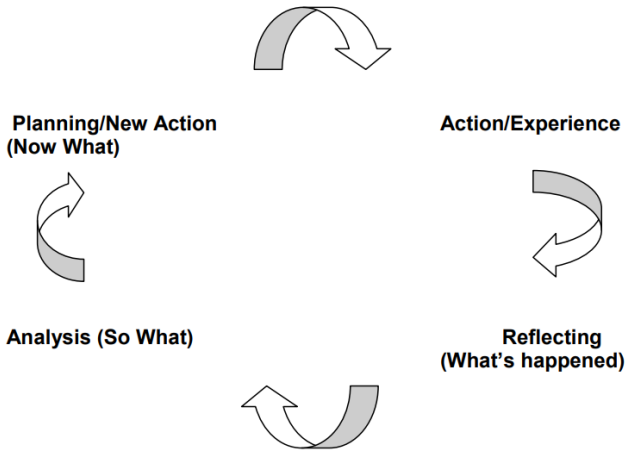

Figure 7 Experiential learning cycle

- The action stage is the activity that has been undertaken for which the process will revolve around

(response to an incident).

- The reflecting stage is the opportunity to examine the incident, reflect on the response and recall the details.
- The analysis stage is the opportunity to evaluate the actual events and identify what went well and what could be improved.
- The planning/new action stage is the process of delivering those improvements to ensure there is no repetition in the future.

The challenge of the above process is the implementation of the cycle to ensure organisational learning across the board. This may take a number of different mediums to achieve through direct learning, distance learning or delivery of specific training.

Further detail on managing actions and outcomes as part of this process can be found in Chapter 6.

National lessons identified can be fed via DCLG RED, (or devolved equivalents), or the LGD to the Civil Contingencies Secretariat in the Cabinet Office for collation and coordination of any subsequent actions by the relevant government departments.

Regional lessons identified can be fed into Regional Resilience Teams for consideration and action by Regional Resilience Forums. Local lessons identified can be collated for consideration and action by Local Resilience Forums.

Where lessons identified would be of interest to other LRFs or responders in other geographic areas, these can be flagged to the DCLG RED / Welsh Government who will arrange for them to be disseminated via their networks. Consideration should also be given to producing case studies (with links to the full debrief report) for inclusion in the National Recovery Guidance. Details of how to submit case studies, along with the case study template, can be found with the Guidance on the UK Resilience website: National Recovery Guidance - GOV.UK (www.gov.uk).

The outputs of this process will then feed into the planning processes, to account for changes in the baseline and improvements to existing plans. Implementation of these improvements and actions is how lessons identified are transitioned into lessons learned. Further detail on this can be found in *RDG-OPS-ACOP-010 Rail Emergency Management Code of Practice with Guidance - Preparation.*

5 Post Incident Reporting & Information Dissemination

5.1 Overview

Recommendation 81 of the Pitt Review stated there should be an 'agreed framework, including definitions and timescales for local-central recovery reporting'. The Government accepted this recommendation and have since been developing a standard mechanism for recovery reporting to ensure that there is a common understanding between Government departments, the Government Offices/devolved administrations, and local responders, about what will be expected in terms of reporting during the recovery phase.

To ensure these arrangements are consistent and straightforward, they all operate according to a set of Recovery reporting principles (see section 3.3.1). These principles have been agreed between the relevant government departments giving guidance as to how the reporting framework will be activated, and the processes in place to alert localities to its activation.

Since the agreed framework for recovery reporting, Joint Organisational Learning (JOL) Online was developed to ensure that lessons are identified and learnt by responder agencies in accordance with JESIP. Additionally, JOL ensures that responder agencies have the facility to record lessons identified across a range of national resilience capabilities.

To have a joint organisational learning strategy fully embedded nationally was one of the original objectives for JESIP and is still a key element of the JESIP Joint Doctrine: The Interoperability Framework. The lessons identified from debriefing activities are vital to improving the way we respond to incidents. Inquests and inquiries focus heavily on previous lessons and responder organisations must be able to prove they have identified and shared learning to try to prevent future similar issues.

Issues have frequently been identified, but not successfully acted upon, to improve effective joint working. It is essential that JOL is accepted as the standard for multi-agency learning and is adopted by all responder organisations to ensure interoperability is continually improved. JOL Online, supported by a robust process and governance, provides responder organisations with a consistent and accountable mechanism to ensure lessons identified are acted upon, to make the transition from lessons identified to lessons learned.
The Interoperability Board provides governance for the JOL arrangements. This ensures that any issues regarding interoperability are considered and acted upon by appropriate representatives from the emergency services, their respective government departments, and other key stakeholders.

Source: Joint Organisational Learning - JESIP Website

This stage of the recovery process forms a crucial part of the IEM process and will help to close the feedback loop by providing input back into Preparation activity, as detailed in *RDG-OPS-ACOP-010 Rail Emergency Management Code of Practice with Guidance - Preparation.*

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 8 References. The Provision Endnotes can be found in Section 8.1. A full provisions table is provided in the appendices of this document.

5.2 Provisions

5.2.1 Rail Entities ***SHOULD*** utilise the Joint Organisational Learning Online standard, tool and supporting processes from JESIP. [6]

5.2.2 Rail Entities ***SHOULD*** ensure staff trained on, responsible and accountable for the recovery phase of an incident are knowledgeable on the Cross-Government Principles on Recovery Reporting (5.3.1). [2]

5.2.3 Rail Entities ***SHOULD*** ensure once the debrief report is completed it is circulated with those who attended the debrief and within the wider industry if necessary. [2]

5.2.4 Capture of information for Organisational Learning is key and ***SHOULD*** be made available where appropriate to the wider rail industry. This ***SHOULD*** be achieved by the provision of an identified site

which can be accessed by the whole organisation. [6]

5.2.5 Where identified, lessons learnt ***SHOULD*** be used to inform the future training needs of Rail Entities and ***SHOULD*** be incorporated in exercising plans. [1]

5.3 Guidance Notes

5.3.1 Recovery Reporting

The need for accurate record keeping is of paramount importance. The responses to issues will be on public view; there will be a requirement to prepare reports; and there is also the potential for subsequent inquiries or litigation. There needs to be clear audit trails with comprehensive records of timings, notifications, decisions, actions, and expenditure. It would therefore be beneficial to use the same information management system used in the response phase for the recovery phase.

A reporting framework for recovery was introduced by Cabinet Office (recovery-reporting-framework-1.pdf (publishing.service.gov.uk)) to ensure that there is a common understanding between government departments, devolved administrations, and local responders, about what will be expected in terms of reporting during the recovery phase.

The recovery reporting framework will enable local authorities to undertake a degree of planning to ensure they have the resources at their disposal to collate the information required, during and after an incident. It will also ensure that central government has a recognised system by which it can collect recovery information from localities. This will help to inform decisions as to what central government support may be required. The recovery reporting framework is only intended to be activated in the event of a wide area emergency requiring central government co-ordination of the recovery phase.

The recovery reporting framework sets out the likely data requirements from local responders and provides guidance as to what the information is likely to be used for. Local responders may find the recovery reporting framework helpful in training and exercising for larger scale emergencies. Flexibility about what data needs to be reported is important. The type of information required will depend on the particular nature of the incident and the operational needs of those responsible for recovery, particularly at the local level.

Further guidance on the duties of Category 2 responders regarding public communications and data handling can be found in RDG-OPS-ACOP-011 IEM, Response.

In order to ensure that these arrangements are as consistent and as straightforward for local responders to use as possible, they all operate according to a set of recovery reporting principles (see Section 3.3.1). These principles have been commonly agreed with all relevant government departments and give guidance as to how the reporting framework will be activated, and the processes in place to alert localities to its activation. It includes the procedure by which the information will be requested, and the process by which it will be collected, by central government.

Cross-Government Principles on Recovery Reporting:

- The recovery reporting framework allows local responders to be aware of the potential requirements for reporting recovery and, in the event of an emergency, will provide a strategy to co-ordinate central government requests for recovery information.
- The information requirements in the framework should be sufficiently generic to be useable in any type of emergency recovery situation, be it flooding, pandemic flu or a terrorist attack. That said, the framework will have the flexibility to allow for additional information needs depending on the situation being dealt with.
- The framework should only be activated when there is central government recovery co-ordination, and a Lead Government Department role is initiated. Government will judge whether co-ordination is needed on a case-by-case basis.
- Government Departments will ask for information using the recovery reporting framework and using the principles set out. Only in exceptional circumstances should Government Departments ask for additional information not covered in the reporting framework.
- Information included in the framework should have a sound rationale for their inclusion and clear provenance of the data. Data requests should be kept at a minimum whilst still allowing Departments and Ministers sufficient information from affected areas to allow them to determine the scale of the recovery situation and make decisions about the type of support that may need to be offered.
- Information in the framework will also be used to monitor progress being made during the recovery

process.

- The framework will be integrated as far as possible with the collection of information for the Emergency Response SitReps to make the reporting requirements as seamless as possible for Regional Resilience Teams /Welsh Assembly Government and local responders.
- Most recovery work in Wales will fall to the Welsh Assembly Government and there may not always be a requirement to report up to CCS or to other government departments if the emergency falls within devolved competence or is not of a sufficient scale to require the UK Government involvement.
- Information included in the framework should include, as far as possible, information requests that would be needed in determining any additional funding from individual departments recovery funding schemes. However, it will not necessarily follow that activation of the recovery framework goes hand in hand with additional funding for local authorities.
- It is not possible to prescribe timescales for the duration for collection of this information but exit strategies should link to the completion of recovery objectives as set out in recovery plans. Timescales should, as far as possible, be consistent with those required by the funding streams so as to reduce the burden on local authorities collecting this information.
- All of the information required may not be available during the early stages of the recovery phase. There may be an incremental increase in the amount of information it is possible to gather.
- The information required will be collected as a function of the Recovery Co-ordinating Group. The information should be provided and disseminated as follows:

5.3.2 Recording Outcomes and Organisational Learning

The primary purpose of any debriefing is to identify areas from which lessons can be learnt, identifying good practice and to implement procedures for improvement. Such outcomes must be captured and reviewed in a structured and timely manner to ensure that all those affected can benefit from the learning. The outcomes from all debriefs will need to be recorded in written format. It may be prudent to have a minute taker present to record the information or to video or audio record the process to ensure accuracy. Once the written outcome (debrief report) is completed it should be circulated with those who attended the debrief and within the wider industry if necessary.

Recommendations should then be implemented from this process. Forms exist for capturing information to support the debriefing process. These should be available to appropriate senior managers to allow oversight and make recommendations where necessary.

Capture of information for Organisational Learning is key and should be made available where appropriate to the wider rail organisation (See Section 5.3.3 - JOL). This should be achieved by the provision of an identified site which can be accessed by the whole organisation. Increased use of Resilience Direct across the rail industry will help to support both a sharing culture in general and engagement with JOL.

Where identified, lessons learnt should be used to inform the future training needs of rail entities and should be incorporated in exercising plans.

5.3.3 Joint Organisational Learning

In-depth guidance on the use of JOL can be found at JOL Guidance - JESIP Website.

JOL aims to achieve a consistent and accountable mechanism to ensure lessons from incidents, training, exercising and other external sources are identified and acted upon to continually improve interoperability and national resilience capabilities.

Following a debrief and identification of lessons learned there are triggers for submission to JOL Online. For example, if the lesson identified:

- May have an impact on responder agencies interoperability measured against JESIP Principles for joint working.
- May have a national impact.
- May impact on your organisation’s national standards.
- May impact on effectiveness of your sectors current national operational guidance, approved professional practice or doctrine.
- May impact on effectiveness of current national resilience capabilities.
- Is low impact but high frequency (trend).
- You want to share your lessons identified with other emergency responder agencies to promote learning.

This is not a definitive or exhaustive list and if organisations feel that a lesson should be recorded on JOL, they should do so.

Lessons identified will be captured from responder agencies, then monitored and analysed by the JOL secretariat, shared with responder agencies, and where required, recommendations for action will be made to the Interoperability Board. The Interoperability Board may issue a JOL Action Note with a directive towards agencies affected to implement locally. The use of JOL Online by responder agencies will convert "lessons identified" into "lessons learnt" throughout the planning, response, and recovery phase of incidents. Effective JOL will provide assurance to Government departments, Chief Officers, Chief Executives and ultimately the general public, that responder agencies can demonstrate true progress in Joint Organisational Learning and show commitment to learn from incidents and continually improve the multi-agency response to future incidents and emergencies.

Managing the flow of information into, and out of, JOL to gain the maximum benefit will have an impact on resources. Rail entities should identify suitable roles with responsibility for providing that link between JOL and any pre-existing single agency tools. This will need to go hand in hand with appropriate governance arrangements for this process.

5.3.3.1 JOL Process

The steps shown in Figure 8 below comprise the JOL process. Behind each step are a number of activities to be completed by responder agencies or JOL Secretariat. The process is supported by JOL Online.

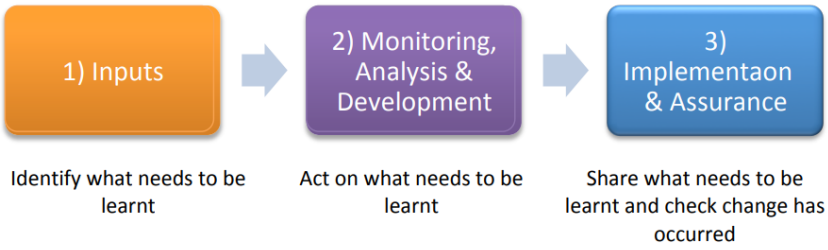

Figure 8 JOL Process.

Step 1. Inputs

Inputs are the Lessons Identified or Notable Practice which may come from responder agencies through their existing debrief processes. Lessons Identified may also come from other external sources such as national exercise debriefs, public enquiries, Prevention of Future Death reports or HSE recommendations. Inputs will be entered onto the JOL Online in a standardised and consistent format.

JESIP encourages responder agencies to use the multi-agency debrief template to capture and record interoperability Lessons Identified and notable practice as part of their local debrief procedures. It should be used to support all single service and multi-agency debriefs where responder agencies have attended an incident, exercise, or training event. It is designed to enhance and support existing local de-brief procedures / templates.
By using this template, responder agencies will find it much more efficient to transfer information relating to interoperability and national resilience capabilities, captured during debriefs, onto JOL Online.

Each responding organisation and each LRF can nominate a JOL Single Point of Contact (SPoC), who will be responsible for entering inputs onto JOL Online on behalf of their organisation or LRF. All lessons identified or notable practice from responder agencies should be agreed and authorised within their organisation (rail entity) and / or LRF before being inputted onto JOL Online. Emergency responder agencies should have a generic JOL mailbox to support effective communications between the JOL Secretariat and JOL SPoCs. Those taking the role of the JOL SPoC should:

- Be in a role within their organisation or LRF that has responsibility for capturing lessons from single service or multi-agency debriefs from incidents, exercises, and training.
- Have responsibility for managing their organisations generic JOL mailbox.
- Have an awareness and understanding of the Joint Doctrine: The Interoperability Framework and be able to identify relevant lessons or notable practice from debriefs that fall within the scope of JOL.
- Have appropriate delegated authority and influence to ensure that where JOL Action notes and other JOL information is communicated to organisations or LRFs then it can be effectively implemented.
- Have basic IT ability and confidence in using web-based applications.

- Input Lessons Identified and Notable Practice on behalf of their organisation.
- Have access to Resilience Direct.

Where any responder agency changes their JOL SPoC, they must inform the JOL Secretariat with their contact details. This will ensure the contact database remains current.

The concept of JOL is to learn lessons and improve practice. JOL Online provides responding organisations with the opportunity to publish information in a secure environment but that will facilitate the sharing of best practice and learning. The inputs provided from organisations are automatically protected as all data on the application will be marked as Official-Sensitive in line with the Governments Security Classifications 2014. JESIP are members of a number of organisational learning boards across the emergency services and government network and will share lessons identified / notable practice with these boards as part of stakeholder engagement and to ensure work is not duplicated.

JOL Online provides the facility for organisations to share lessons and notable practice from a variety of incident types. However, there may be concerns from organisations about the sharing of sensitive or commercial information with others. Information that is inputted onto JOL Online is managed in accordance with Official-Sensitive guidelines and the secretariat will after consultation with key stakeholders make an informed decision around how much information is shared with other organisations. Information which has gone through this process may then be shared with the JOL SPoC closed group or with wider ResilienceDirect users.

Before information is published through JOL Online the JOL Secretariat will redact any personal and may redact any sensitive data and will moderate any free text answers to ensure no comments are published inappropriately. This also applies to any files uploaded if they are likely to be published with an organisations input.

Once completed the secretariat will publish the following:

- Share lessons with all RD users - The information provided will be published and visible to other site users.
- Share lessons with JOL SPoCs - The information provided will be published and visible to other JOL SPoCs only.
- Share lessons with other approved closed groups –The information will be published and visible to approved closed groups only Where lessons or notable practice have been inputted that are believed to be sensitive (for example CT) JOL Online will automatically prevent this lesson from being published until further authorisation is received from key stakeholders.

Step 2. Monitoring, Analysis and Development

The JOL Secretariat monitor and analyse Lessons received to identify where issues raised fall within the scope of JOL Online. Whilst lessons identified and notable practice will be continually monitored and analysed, it is important that consideration at a national level does not replace local analysis and plans to implement lessons learned. Lessons Identified will be reviewed and an overall assessment rating applied. This rating determines the next steps. This methodology provides a clear rationale for determining which issues should be subject to consideration at the national level.

As part of the analysis, the JOL Secretariat team will adopt an impact-based assessment process in considering next steps. The results of this analysis may lead to one of two activities:

- Feeding back to the relevant organisation and confirming that the lessons identified will not at this stage be subject to further consideration at the national level.
- Escalation of lessons which may require commissioning further detailed analysis whereby actions and/or recommendations may be submitted to the Interoperability Board for consideration and approval.

Assessment Stage 1 – Initial Assessment

The JOL Secretariat will use an impact-based assessment process to each Lesson Identified. This will inform any further action.

Likelihood: The first assessment is the nature of the lesson identified and the likelihood of the issue occurring again. This assessment may involve discussion with relevant subject matter advisors and other stakeholders. As the number of inputs onto JOL Online grows, lessons identified will be indexed and links will be established to help us easily identify reoccurrences of issues. This will inform the likelihood assessment process.

Impact Grading: The second part of the assessment is the relative impact that an event had on responder agencies taking into account the varying nature of impacts.

Overall Assessment: From both the Likelihood and Impact, an overall assessment rating will be applied to the lesson identified. As part of the analysis, national trends may be identified, in these cases JOL will automatically trigger stage 2 of the analysis process.

Assessment Stage 2 - Further Analysis

If the rating is medium or above, the lesson will be escalated where a more thorough analysis of the Lesson(s) Identified will be carried out. The JOL Secretariat will:

- Facilitate additional discussions and outcomes from the initial assessment with respective SPoCs and other stakeholders where necessary; and / or,
- Clarify if work already exists locally or nationally to address the issue.

Outcomes from this further analysis may result in the JOL Secretariat liaising with the originators of the lesson identified to find an appropriate resolution. This may include sharing of information with other organisations or a degree of further engagement with originators to support/assist/guide them in finding an appropriate resolution.

If a successful course of action is agreed and implemented, information may then be shared with other responder agencies. Alternatively, the outcome of further analysis may dictate the commissioning of a task and finish group to further analyse the lesson identified and develop recommendations for action. It may be that wider scale change is identified which may lead to recommendations for action being proposed to the Interoperability Board for approval and then implementation. To help with this assessment the JOL secretariat will utilise the Single Loop learning process ‘what we do’ and Double Loop learning process ‘why we do what we do’ (Figure 9). By utilising this methodology, we can ensure we consider both the most efficient and effective process for developing action plans even if this may mean larger scale cultural/behavioural changes necessary to achieve lessons learned.

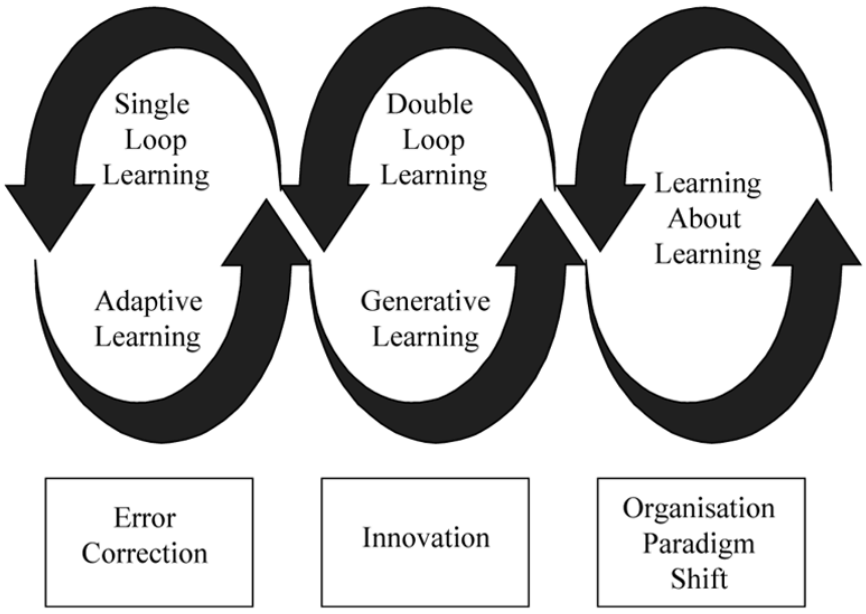

Figure 9 Single, Double and Triple Loop learning process.

Assessment Stage 3 - Development of Recommendations

Following Stage 2, if it is decided that a lesson identified requires action to be taken, the JOL Secretariat and SPoCs will formulate potential actions to address the issue raised. The recommendations developed may have both national and local impacts and may involve a number of activities such as doctrine review, multi-agency training, testing, and exercising or a combination of these.

Dependant on the nature of the lesson identified, work to develop actions will either by carried out by the JOL Secretariat and Organisational Points of Contact independently or with a Task and Finish group if one has

been established. Where recommendations are required the SPoCs will submit a JOL Action Note to the Interoperability Board for approval.

Step 3. Implementation and Assurance

It is envisaged that any lessons identified and subsequent recommendations for action are likely to fall into the following areas:

- Doctrine.
- Training.
- Testing & Exercising.
- National Resilience Capabilities.
- Safety of the public and emergency responder staff.

There is also likely to be the need for communication and engagement with those affected by the recommended changes who then become recommendation owners. Once a recommendation for action is approved by the Interoperability Board, the relevant representatives will be tasked with instigating the implementation process.

For the emergency services the Sector Interoperability Leads are those holding the national portfolio for interoperability for their sector (Sector Interoperability Leads are members of the Interoperability Board). Depending on the nature of the action to be taken, other organisations may be involved in implementing JOL recommendations. The other organisations which may be involved in implementation include but are not limited to:

- Civil Contingencies Secretariat
- DCLG RED Resilience Advisors
- Her Majesty's Coastguard (HMCG)
- Ministry of Defence (MOD)
- British Transport Police (BTP)
- Civil Nuclear Constabulary (CNC)
- Lead Government Department
- Environment Agency (EA)
- Department for Transport (DfT)

Local implementation of JOL recommendations will be the responsibility of the emergency services or the LRFs.

5.3.3.2 JOL Roles and Responsibilities

Service JESIP Strategic Lead

Each emergency service has a Service JESIP Strategic Lead. They are responsible for interoperability within their service or organisation. They are accountable for both their service inputs onto the JOL application and the implementation of any recommendations coming from JOL within their local service, force, or trust. Each emergency service JESIP Strategic Lead will be responsible for reporting their agencies activity in response to any JOL action notes that have been issued to their respective Organisational Point of Contact. This feedback will be regularly monitored to assess how recommendations are being implemented. Progress reports on implementation will be provided to the Interoperability Board.

Service JOL Single Point of Contact (JOL SPoC)

It is the responsibility of each emergency service JESIP Strategic Lead to nominate one or more Single Point of Contact(s) for JOL within their organisation. These people will have access to JOL Online, the generic JOL mailbox and be trained in its use and be responsible for inputting lessons identified or notable practice.

Local Resilience Forum (LRF)

Each of the 42 Local Resilience Forums in England and Wales should nominate a JOL SPoC(s) who will have access to JOL Online, be trained in its use and be responsible for inputting lessons identified or notable practice on behalf of their LRF. Should any recommendations or JOL action notes affect LRFs, the JOL Secretariat will share information about what action is required with LRFs through this network of JOL SPoCs. LRFs should direct any feedback in respect of implementation and embedding of recommendations through their respective LRF JOL SPoC who will update the JOL Secretariat. This feedback will be regularly monitored to assess how recommendations are being implemented. Progress reports on implementation will be provided to the Interoperability Board.

5.3.3.3 Tracking your inputs

JOL Online will provide the person submitting the lesson identified or notable practice with the ability to track their input. This will fall into a number of phases which tracks the complete lifecycle of the input:

- Received – The JOL Secretariat has received an input from an end user.
- Initial analysis complete – The input has been analysed and impact assessed.
  - An impact assessment may not be undertaken for notable practice but will be analysed.
- Escalated – The impact assessment indicates that the input is escalated to Stage 2 where:
  - A task and finish group may be established for further analysis.
  - Further stakeholder engagement is being undertaken.
- Published – The JOL Secretariat has published the end user's input.
  - This may be with JOL SPoCs or all RD users.
- Final Stage – The end user will be provided with information about what the outcome of their input is, which may be:
  - A referral to a Lead Government Department (identify which one).
  - Production of a JOL Action Note.
  - Referral to a professional Association – (NPCC, NFCC, AACE, HMCG).
  - No further action after escalation.
- Closed – The respective input has been completed and closed by the JOL Secretariat on behalf of the Organisational Point of Contact.

5.3.3.4 Progress Reporting on JOL

The JOL Secretariat will continually monitor inputs on JOL Online and will regularly review the status of recommendations and JOL Action Notes. It will work with organisations to ensure reporting information is current and activities are recorded. At the Interoperability Board the progress of recommendations or JOL Action Notes will be indicated by three status statements:

- Recommendation/Action Open - recommendations/actions are considered to still require action/implementation to move to completed. (regular updates will be required from recommendation owners)
- Recommendation/Action Closed - recommendations/actions have been completed and responder agencies reported back to the JOL secretariat.
- Awaiting Allocation – recommendation/action has been identified and allocation of owner not yet identified.

The JOL Secretariat will collate updates from responder agencies and submit a quarterly summary review of recommendations to the Interoperability Board. This summary will provide the Interoperability Board with information extracted from JOL Online with regards to the number of lessons identified, new recommendations proposed since the last quarter, current recommendations and their activity status and any recommendations proposed for closure. This information will provide key data to the Interoperability Board members to allow the assessment of how JOL is impacting organisations and benefiting joint working 'on the ground'.

A quarterly update of notable practice will be provided to Interoperability Board.

5.3.3.5 Communication with stakeholders

The JOL Secretariat will produce regular communication to the responder agencies about the progress with JOL, specifically where recommendations for action have been made. As with all JOL communications, the JOL Secretariat will seek to ensure a two-way flow of information from organisations, encouraging feedback so that responders can continually improve JOL Online and highlight areas to continually improve joint working.

6 Corrective and Preventative Actions (CAPA) Management

6.1 Overview

Corrective and Preventive Actions (CAPA) are processes for identifying, documenting, and addressing defects, deficiencies, and nonconformities. CAPA is the abbreviation for Corrective Action and Preventive Action. These two aspects have traditionally been connected but are ideally only distantly related:

- **Corrective Action:** "action to eliminate the cause of a nonconformity and to prevent recurrence" *(ISO 9000:2015 Quality management systems – fundamentals and vocabulary)*. It is the elimination of the cause or causes of an existing nonconformity or undesirable situation to prevent recurrence. There can be more than one cause for a nonconformity.
- **Preventive Action:** "action to eliminate the cause of a potential nonconformity or other potential undesirable situation" *(ISO 9000:2015 Quality management systems – fundamentals and vocabulary)*. It is the identification and elimination of the cause(s) of potential nonconformities in order to prevent occurrence.

That is to say that corrective action is taken to **prevent recurrence** whereas preventive action is taken to **prevent occurrence**.

The adoption of a quality management system is a strategic decision for an organisation that can help to improve its overall performance and provide a sound basis for sustainable development initiatives.
The potential benefits to an organisation of implementing a quality management system based on this International Standard are:

- The ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements.
- Facilitating opportunities to enhance customer satisfaction.
- Addressing risks and opportunities associated with its context and objectives.
- The ability to demonstrate conformity to specified quality management system requirements.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 8 References. The Provision Endnotes can be found in Section 8.1. A full provisions table is provided in the appendices of this document.

6.2 Provisions

6.2.1 Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve a quality management system. [7]

6.2.2 Top Management ***SHOULD*** demonstrate leadership and commitment with respect to the quality management system. [7]

6.2.3 Rail Entities ***SHOULD*** determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system. Rail Entities ***SHOULD*** monitor and review information about these external and internal issues. [7]

6.2.4 Due to the effect or potential effect of interested parties on a Rail Entity's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, Rail Entities ***SHOULD*** determine [7]:

- The interested parties that are relevant to the quality management system.
- The requirements of these interested parties that are relevant to the quality management system.

6.2.5 Rail Entities ***SHOULD*** monitor and review information about these interested parties and their relevant requirements. [7]

6.2.6 Rail Entities ***SHOULD*** determine the boundaries and applicability of the quality management system to establish its scope. [7]

6.2.7 The scope of the Rail Entity's quality management system ***SHOULD*** be available and be maintained as documented information. [7]

6.2.8 Rail Entities ***SHOULD*** determine and select opportunities for improvement and implement any necessary actions to meet customer requirements and enhance customer satisfaction. [7]

6.2.9 Corrective actions ***SHOULD*** be appropriate to the effects of the nonconformities encountered. [7]

6.2.10 Rail Entities ***SHOULD*** retain documented information as evidence of both the nature of the nonconformities (and any subsequent actions taken) and the results of any corrective action. [7]

6.3 Guidance Notes

6.3.1 ISO 9001:2015 Quality Management Systems - Requirements

ISO 9001:2015 Quality Management Systems – Requirements promotes the adoption of a process approach when developing, implementing, and improving the effectiveness of a quality management system, to enhance customer satisfaction by meeting customer requirements.

Understanding and managing interrelated processes as a system contributes to an organisation's effectiveness and efficiency in achieving its intended results. This approach enables the organisation to control the interrelationships and interdependencies among the processes of the system, so that the overall performance of the organisation can be enhanced.

The process approach involves the systematic definition and management of processes, and their interactions, so as to achieve the intended results in accordance with the quality policy and strategic direction of the organisation. Management of the processes and the system as a whole can be achieved using the Plan, Do, Check, Act (PDCA) cycle (Figure 10) with an overall focus on risk-based thinking aimed at taking advantage of opportunities and preventing undesirable results. The application of the process approach in a quality management system enables:

- Understanding and consistency in meeting requirements.
- The consideration of processes in terms of added value.
- The achievement of effective process performance
- Improvement of processes based on evaluation of data and information.

Figure 10 PDCA Cycle.

Figure 11 gives a schematic representation of any process and shows the interaction of its elements. The monitoring and measuring check points, which are necessary for control, are specific to each process and will vary depending on the related risks.

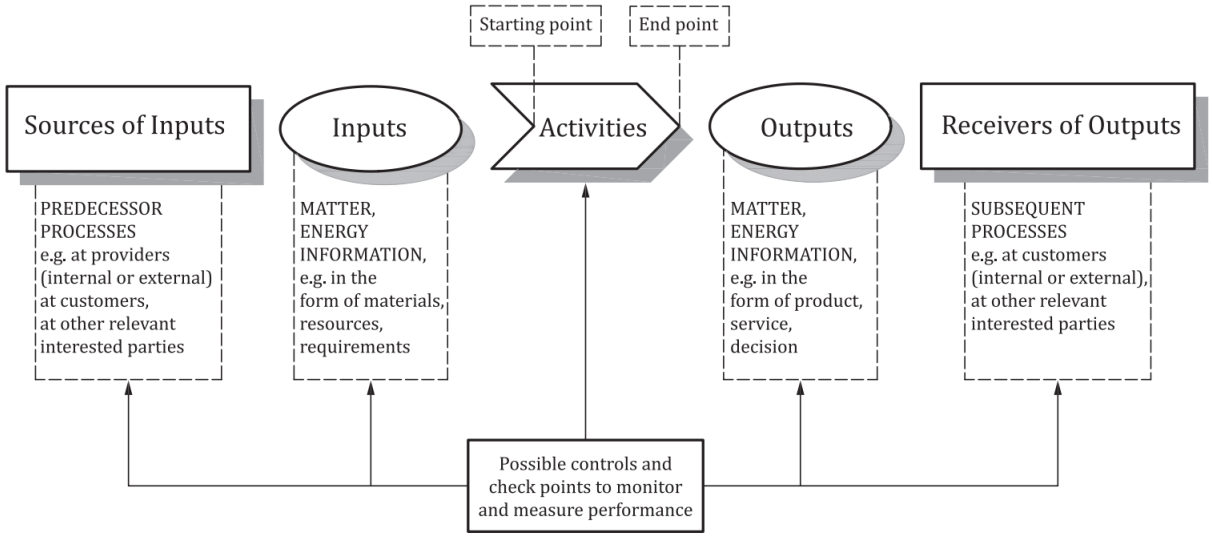

Figure 11 Schematic representation of the elements of a single process (Source: ISO 9001:2015 Quality Management Systems - Requirements).

The PDCA cycle can be applied to all processes and to the quality management system as a whole; it can be briefly described as follows:

- **Plan**: establish the objectives of the system and its processes, and the resources needed to deliver results in accordance with customers' requirements and the organisation's policies and identify and address risks and opportunities.
- **Do**: implement what was planned.
- **Check**: monitor and (where applicable) measure processes and the resulting products and services against policies, objectives, requirements, and planned activities, and report the results.
- **Act**: take actions to improve performance, as necessary.

Risk-based thinking is essential for achieving an effective quality management system. The concept of risk-based thinking has been implicit in previous editions of ISO 9001:2015 Quality Management Systems including, for example, carrying out preventive action to eliminate potential nonconformities, analysing any nonconformities that do occur, and taking action to prevent recurrence that is appropriate for the effects of the nonconformity. See Section 6.5.1 for further guidance on Risk-Based Prioritisation.

To conform to the best practice requirements for quality management systems, Rail Entities should plan and implement actions to address risks and opportunities (refer to the RDG-OPS-ACOP-009 Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention (AAP) for risk and opportunities management). Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the quality management system, achieving improved results, and preventing negative effects.

Opportunities can arise as a result of a situation favourable to achieving an intended result, for example, a set of circumstances that allow the organisation to attract customers, develop new products and services, reduce waste, or improve productivity. Actions to address opportunities can also include consideration of associated risks. Risk is the effect of uncertainty, and any such uncertainty can have positive or negative effects. A positive deviation arising from a risk can provide an opportunity, but not all positive effects of risk result in opportunities.

ISO 9001:2015 Quality Management Systems – Requirements specifies requirements for a quality management system when an organisation:

a) Needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and
b) Aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

In establishing, implementing, maintaining, and continually improving a quality management system, Rail Entities should instigate the following processes:

- Determine the inputs required and the outputs expected from these processes.

- Determine the sequence and interaction of these processes.
- Determine and apply the criteria and methods (including monitoring, measurements, and related performance indicators) needed to ensure the effective operation and control of these processes.
- Determine the resources needed for these processes and ensure their availability.
- Assign the responsibilities and authorities for these processes.
- Address the risks and opportunities.
- Evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results.
- Improve the processes and the quality management system.

Rail Entities should determine and select opportunities for improvement and implement any necessary actions to meet customer requirements and enhance customer satisfaction. These shall include:

- Improving products and services to meet requirements as well as to address future needs and expectations.
- Correcting, preventing, or reducing undesired effects.
- Improving the performance and effectiveness of the quality management system.

When a nonconformity occurs, including any arising from complaints, Rail Entities should:

- React to the nonconformity and, as applicable:
  1) Take action to control and correct it.
  2) Deal with the consequences.
- Evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:
  1) Reviewing and analysing the nonconformity.
  2) Determining the causes of the nonconformity.
  3) Determining if similar nonconformities exist, or could potentially occur
- Implement any action needed.
- Review the effectiveness of any corrective action taken.
- Update risks and opportunities determined during planning, if necessary
- Make changes to the quality management system, if necessary.

Source: ISO 9001:2015 Quality Management Systems – Requirements.

6.3.2 The 5 Whys

As previously stated, corrective action is reactive, whereas preventive action is proactive. Although these two actions use similar processes and some of the same analytical tools, they are not necessarily used together.

Corrective action involves the identification, documentation, and elimination of the root cause of a nonconformity to prevent the problem from recurring. Corrective actions are taken under more intense consideration than corrections (which address immediate issues); typically, they are enacted over a slightly longer time period to prevent recurrence.

Most corrective action procedures use a variation of 8D problem solving. 8D problem solving is a team-oriented approach to solving critical problems in the production process or business operations. The method consists of eight steps or disciplines that aim to find the root cause of a problem, implement corrective and preventive actions, and recognise team contributions. The 8D problem solving method is useful for improving customer satisfaction. The following are some examples of the types of steps taken during a corrective or problem-solving process:

- **Promptly identify and document the problem**. Use the 5 Why questioning (Figure 12) to acquire details and determine if this is an isolated event or if it is significant and has the potential to recur. Reporters may indicate that the problem is pervasive, but it may be limited. When documented, quality events should be reported to management.
- **Implement a correction or containment or temporary repair**. This may include removing a defective or redundant item / process.
- **Find the cause of the issue**. Use the 5 Whys to help pinpoint a problem statement. Use an Affinity or Ishikawa (fishbone) diagram to help determine the root cause.
- **Determine the solution that will prevent a recurrence**. Solutions can include new parts, process changes, and even system changes.
- **Implement the corrective action** and ensure that everything is documented.
- **Verify that the action continues to be effective and that the problem does not recur**. Document

the evidence of continued success or highlight as a residual risk.

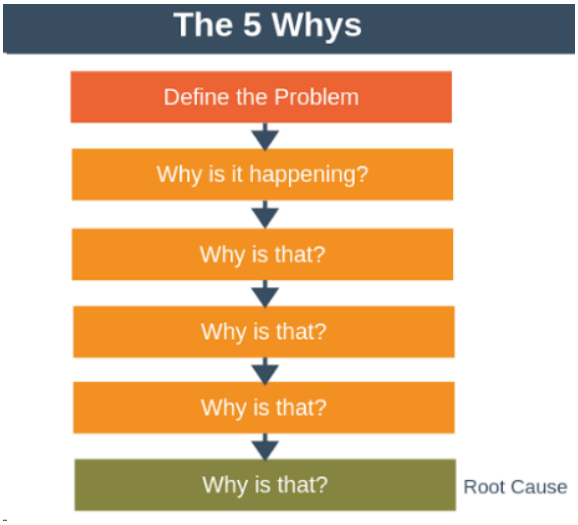

Figure 12 The Five Whys.

6.3.3 Risk-Based Prioritisation

Along with the defined corrective action procedures, a *predefined risk-based prioritisation* eliminates small nonconformities that teams can solve when they discover problems without initiating corrective procedures. Weight matrices help with these questions; the criteria often include frequency (frequently, occasionally, or rarely) and impact (negligible, critical, or even resulted in injury or death). Safety is typically a priority over frequency during action response.

ISO 9001:2015 Quality Management Systems – Requirements eliminates the requirement for predefined procedures for both corrective action and preventive action. Preventive action is now considered a part of good planning and risk management. It fully incorporates the notion that prevention comes first and eliminates problems and, thereby, the need for corrective action. As per 9001:2015, the requirement is to document what happened and how it has been fixed.

The following are tools for analysing risk or potential problems:

- **Hazard and Operability Study (HAZOP):** A HAZOP is a sequenced and methodical study of a process that is in development or in operation. The HAZOP seeks to identify problems that may represent risks to personnel or equipment.
- **Failure Modes and Effects Analysis (FMEA):** FMEA is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service. *Failure modes* means the ways (or modes) in which something might fail.
- **Fault Tree Analysis (FTA):** FTA is commonly used in safety and reliability engineering to break a system into subsystems to understand where problems may occur. FTA is often used in pharmaceutical development and manufacturing.

A *preventive action process*, in addition to including a specific preventive action plan to mitigate potential problems, also comprises the implementation of controls to ensure that any preventive measures continue to work. Preventive action means identifying not only potential problems, but also opportunities for improvement. With changes that are enacted through a preventive action process, controls should be included to prevent and check for possible nonconformities and to measure the overall effectiveness of the process and its evolution.

A *preventive control*, also known as an *internal control*, serves to reduce the chances of problems and nonconformities that occur.

Teams may find potential problems in internal or external data sources. Internal data sources may include process control data, trend analysis, the results of proficiency testing, or internal audits. External data includes customer complaints, service reports, and even data for similar products produced by other companies.

Preventive actions may also be sparked through the results of regularly assessing employees and then deciding if more or revised training is required. Risk analysis can help target costs, so the exercise doesn't appear to be a waste of money when problems don't occur.

Some examples of preventive actions:

- Creating emergency arrangements plans for hazards and unexpected situations throughout facilities.
- Implementing or updating safety and security policies.
- Creating checklists.
- Implementing lean practices to reduce waste that can contribute to problems and non-conformities.
- Implementing and following preventive maintenance plans to ensure that equipment performs efficiently, effectively, and safely.

Some experts still think that preventive actions follow the experience of corrective actions. This approach focuses on capturing the experience for the future, including tagging keywords from the action report in databases and updating documents, requirements documents, and procedures.

See RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance, 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.

6.3.4 CAPA Inspection

An inspection may seek to ensure that organisations have documented CAPA procedures and make sure that they contain certain elements. For example, records should show that organisations could find the root cause of problems and are tracking trends to ensure avoidance of future problems or reoccurrences of problems. Investigators also look for evidence that CAPA actions were tested to ensure effectiveness before being implemented. Inspections will want to verify that the data source and statistical process methods employed were sufficient for the task.

6.3.5 CAPA Reports

In all cases, assurance findings should be collated and recorded. Where corrective actions are identified, they should be incorporated into the organisation's standard process for tracking corrective actions. Likewise, where good practice or performance is identified this should be recorded and shared within the organisation and, where possible, with the wider industry.

A *CAPA report* provides a consistent vehicle for recording defects and issues as well as the method of their correction. Usual details include where the problem occurred, the customer's name and address, the details of the problem, whether there was a product breakdown, whether there was an injury, and so on. The report also states what immediate action or correction was taken. The report may walk through the process, suggest tools for the root cause analysis (such as 5 Whys and cause and effect analysis), and provide room to record analysis results. It may also provide guidance on how to route the report depending on the outcome of the analysis.

Source: RDG-OPS-ACOP-008 Rail Emergency Management Code of Practice with Guidance Part A – Governance.

7 Business Continuity Management (BCM)

7.1 Overview

Business continuity is the strategic and tactical capability of an organisation to plan for and respond to incidents and business disruptions to continue operations at an acceptable pre-defined level.

Business Continuity Management (BCM) follows a cyclical process of analysis to understand threats and requirements, determine and implement contingency strategies and validate planned response through testing and exercising.

ISO 22301:2019 is the international standard for Business Continuity Management Systems. The standard specifies the structure and requirements for implementing and maintaining BCM that develops business continuity appropriate to the amount and type of impact that the organisation may or may not accept following an emergency.

The outcomes of maintaining BCM will be shaped by a Rail Entity's legal, regulatory, organisational and industry requirements, products and services provided, processes employed, size and structure of the organisation, and the requirements of its interested parties.

There is a requirement under the Civil Contingencies Act 2004 for Category 1 Responders to implement, maintain, and make arrangements for business continuity.

BCM emphasises the importance of:

- Understanding the organisation's needs and the necessity for establishing business continuity policies and objectives.
- Operating and maintaining processes, capabilities, and response structures for ensuring the organisation will survive disruptions.
- Monitoring and reviewing the performance and effectiveness of BCM.
- Continual improvement based on qualitative and quantitative measures.

BCM comprises the following components:

a) A policy.
b) Competent people with defined responsibilities.
c) Management processes relating to:
    - Policy.
    - Planning.
    - Implementation and operation.
    - Performance assessment.
    - Management review.
    - Continual improvement.
d) Documented information supporting operational control and enabling performance evaluation.

Provisions and accompanying guidance

All references consulted for this Code of Practice are listed in Section 8 References. The Provision Endnotes can be found in Section 8.1. A full provisions table is provided in the appendices of this document.

7.2 Provisions

7.2.1 Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve BCM, including the processes and resources needed and their interactions, in accordance with the requirements of ISO 22301:2019. [8]

7.2.2 Rail Entities ***SHOULD*** determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of BCM. [8]

7.2.3 When establishing BCM, Rail Entities ***SHOULD*** determine the interested parties that are relevant to BCM and the relevant requirements of these interested parties. [8]

7.2.4 Rail Entities ***SHOULD*** implement and maintain a process to identify, have access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, activities, and resources. [8]

7.2.5 Rail Entities ***SHOULD*** ensure that the applicable legal, regulatory, and other requirements are taken into account in implementing and maintaining BCM. Rail Entities ***SHOULD*** document this information and keep it up to date. [8]

7.2.6 The scope of BCM ***SHOULD*** be available as documented information. Rail Entities ***SHOULD*** also determine the boundaries and applicability of BCM to establish its scope and ***SHOULD*** consider [8]:

- The external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of BCM.
- Both the requirements of interested parties and any legal and regulatory requirements.
- Its mission, goals, and internal and external obligations.

7.2.7 Rail Entities ***SHOULD*** establish the parts of their respective organisations, products, and services to be included in BCM, considering organisations location(s), size, nature, and complexity. [8]

7.2.8 Top management ***SHOULD*** provide leadership and commitment with respect to BCM. [8]

7.2.9 Top management ***SHOULD*** establish a business continuity policy. The policy ***SHOULD*** be available as documented information and communicated both within the organisation and to interested parties. [8]

7.2.10 Top management ***SHOULD*** ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organisation. Top management ***SHOULD*** assign the responsibility and authority for [8]:

- Ensuring that BCM conforms to the requirements of ISO 22301:2019.
- Reporting on the performance of BCM to top management.

7.2.11 When planning for BCM, Rail Entities ***SHOULD*** consider the issues referred to in Provision 7.2.6 and determine the risks and opportunities that need to be addressed to [8]:

- Give assurance that BCM can achieve its intended outcome(s).
- Prevent, or reduce, undesired effects.
- Achieve continual improvement.

7.2.12 Rail Entities ***SHOULD*** plan and evaluate the effectiveness of actions to address risks and opportunities and integrate and implement these actions into BCM processes. [8]

7.2.13 Rail Entities ***SHOULD*** establish business continuity objectives at relevant functions and levels. The objectives ***SHOULD*** [8]:

- Be consistent with the business continuity policy.
- Be measurable (if practicable).
- Take into account applicable requirements.
- Be monitored.
- Be communicated.
- Be updated as appropriate.
- Rail Entities ***SHOULD*** retain documented information on the business continuity objectives.
- Determine what will be done, what resources are required, who will be responsible, when it will be completed and how the results will be evaluated.

7.2.14 Rail Entities ***SHOULD*** carry out any changes to BCM in a planned manner, and ***SHOULD*** consider [8]:

- The purpose of the changes and their potential consequences.
- The integrity of BCM.
- The availability of resources.
- The allocation or reallocation of responsibilities and authorities.

7.2.15 Rail Entities ***SHOULD*** determine the necessary competence of person(s) doing work under its control that affects its business continuity performance and ensure that these persons are competent on the basis of appropriate education, training, or experience. [8]

7.2.16 Persons doing work under the Rail Entity's control ***SHOULD*** be aware of the BC policy and their contribution to the effectiveness of BCM, including the benefits of improved business continuity performance and the implications of not conforming with BCM requirements. [8]

7.2.17 Rail Entities ***SHOULD*** ensure their competent person(s) understand their own role and responsibilities before, during and after emergencies.[8]

7.2.18 Rail Entities ***SHOULD*** determine the internal and external communications relevant to BCM. [8]

7.2.19 Documented information required by BCM and by ISO 22301:2019 ***SHOULD*** be controlled to ensure [8]:

- It is available and suitable for use, where and when it is needed (including preservation of legibility and version control).
- It can be distributed, accessed, retrieved, and used.
- It is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).

7.2.20 Documented information of external origin determined by the Rail Entity to be necessary for the planning and operation of BCM ***SHOULD*** be identified, as appropriate, and controlled. [8]

7.2.21 Rail Entities ***SHOULD*** ensure that outsourced processes and the supply chain are controlled. [8]

7.2.22 Rail Entities ***SHOULD*** implement and maintain systematic processes for analysing the business impact and assessing the risks of disruption. [8]

7.2.23 Based on the outputs from the business impact analysis and risk assessment, Rail Entities ***SHOULD*** identify and select business continuity strategies that consider options for before, during and after disruption. The business continuity strategies ***SHOULD*** be comprised of one or more solutions. [8]

7.2.24 Rail Entities ***SHOULD*** determine, implement, and maintain the resource requirements for the selected business continuity solutions so they can be activated when needed. [8]

7.2.25 Rail Entities ***SHOULD*** identify, and document business continuity plans and procedures based on the output of the selected strategies and solutions. [8]

7.2.26 Rail Entities ***SHOULD*** implement and maintain a structure, identifying one or more teams responsible for responding to disruptions. [8]

7.2.27 The roles, responsibilities, competencies and authorities of each team and the relationships between the teams ***SHOULD*** be clearly stated. [8]

7.2.28 Rail Entities ***SHOULD*** alert interested parties potentially impacted by an actual or impending disruption and ***SHOULD*** ensure appropriate coordination and communication between multiple responding organisations. [8]

7.2.29 Rail Entities ***SHOULD*** exercise their warning and communication procedures as part of their exercise programme. [8]

7.2.30 Business continuity plans ***SHOULD*** meet the requirements set out in ISO 22301:2019. [8]

7.2.31 Rail Entities ***SHOULD*** have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption. [8]

7.2.32 Rail Entities ***SHOULD*** implement and maintain a programme of exercising and testing that meets the requirements set out in ISO 22301:2019 in order to validate over time the effectiveness of its business continuity strategies and solutions. [8]

7.2.33 BC evaluations ***SHOULD*** be conducted at planned intervals, after an incident or activation, and when significant changes occur. [8]

7.2.34 Rail Entities ***SHOULD*** determine the requirements for monitoring and measurements as set out in ISO 22301:2019. [8]

7.2.35 Rail Entities ***SHOULD*** conduct internal audits at planned intervals to provide information on whether

the BCMS conforms to both the organisation's own requirements for its BCM and the requirements of ISO 22301:2019 as well as audits to inform whether BCM is effectively implemented and maintained. [8]

7.2.36 Rail Entities ***SHOULD*** consider planning, establishing, implementing, and maintaining the management review processes outlined in Section 7.3.6.3 Review. [8]

7.2.37 Rail Entities ***SHOULD*** determine opportunities for improvement in the suitability, adequacy, and effectiveness of BCM and implement necessary actions to achieve the intended outcomes of its BCMS. [8]

7.2.38 When nonconformity occurs, Rail Entities ***SHOULD*** follow the requirements set out in ISO 22301:2019 and the guidance in Chapter 6 (Corrective and Preventative Actions). [8]

7.2.39 Rail Entities ***SHOULD*** consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities, relating to the business, or to BCM, that shall be addressed as part of continual improvement. [8]

7.3 Guidance Notes

7.3.1 CCA Category 1 Requirements

Whilst Rail Entities as Category 2 Responders are not under a duty to implement business continuity, the regulations provided for Category 1 Responders under the CCA provide the following requirements for the implementation and maintenance of business continuity management that could be followed:

- Have in place business continuity management arrangements.
- Maintain plans to ensure continuation of their function (business as usual and emergency functions).
- assess internal and external risks when developing Business Continuity Plans (BCPs).
- Have in place procedures for business continuity invocation.
- Include arrangements for training and exercising BCPs.
- Ensure plans are reviewed and updated.
- Publish aspects of the plans where required to support emergency response.

7.3.2 Establishing BCM

Useful guidance for the establishment of BCM can be found at the Business Continuity Institute in their Good Practice Guidelines 2023.

BCM will understand the Rail Entity's needs and necessity for establishing BC policies and objectives, together with the importance of operating and maintaining processes, capabilities, and response structures for ensuring the Rail Entity will survive disruptions / emergencies / crises.

To establish BCM in larger or more complex Rail Entities, coordination of activities is typically achieved through a programme comprised of related projected and BAU activities. In smaller Rail Entities, coordination of activities may be achieved through a single project. Once established, any major changes to BCM - for example due to a significant change in the Rail Entity's operating context - may be managed through a further programme. If the organisation has a project and programme management methodology this should be used to coordinate activities. If not, using a recognised project and programme management methodology will be beneficial.

Awareness and understanding of the external and internal operating context, including organisational strategy and risk appetite is essential when working to establish BCM. BCM supports organisational goals and strategies. Early engagement with stakeholders affected by BCM is essential to understand their needs and expectations, avoid duplication of effort, and avoid conflict downstream. Stakeholders might include people with responsibility for corporate governance, enterprise risk management, facilities, safety and security, and other core business functions. Taking an organisation wide view and collaborating cross functionally at an early stage will contribute to the effectiveness of BCM and therefore to the overall resilience of the Rail Entity and the wider rail network.

All the policies and programmes in the organisation that are relevant to business continuity should be identified and opportunities for collaboration considered and coordinated. For example, the people and culture department may have policies for internal communications, and the corporate communications department

may have predetermined agreements for external communication due to a regulatory or customer requirement.

Rail Entities should determine the documented information necessary for the effectiveness of BCM. As BCM is being developed, decisions and processes should be documented, and the documents controlled. When creating and updating documented information, Rail Entities should ensure appropriate:

- Identification and description (e.g., a title, date, author, or reference number).
- Format (e.g., language, software version, graphics) and media (e.g., paper, electronic).
- Review and approval for suitability and adequacy.

It is good practice to:

- Have a top management member as a sponsor for the programme.
- Establish a multi-disciplinary steering group of subject matter experts to oversee, advise, and make recommendations as BCM is developed.
- Establish communication channels for consulting stakeholders.

7.3.1.1 Defining the Scope

Defining the scope ensures clear understanding of which areas of the organisation are covered by BCM and which areas are not. A well-defined scope focuses BCM on organisational priorities and ensures BCM makes best use of available resources, such as funding and time. The scope is subject to change as BCM is developed.

The initial scope of BCM may be limited to specific areas of the organisation with high value, as identified with relevant stakeholders. This makes it easier to manage risk, complexity, and cost across the organisation.

There may be occasions when an organisation must build its initial implementation of BCM based on a regulatory requirement, a customer demand, certification against a standard, or an audit finding. In such an instance, the organisation will need to include all the activities associated with the relevant requirement in the BCM scope.

The BCM scope should be available as documented information. The scope of BCM is independent of the BC policy, so it may be defined before or after the policy is written.

7.3.1.2 Establishing the BC Policy

The BC policy is a statement from top management that:

- Explains the meaning and importance of BCM to the organisation.
- Demonstrates top management commitment to BCM and its continual improvement.
- Sets expectations for how BCM will be used by all workers.
- Defines the guiding principles for setting, reviewing, and meeting BCM requirements and objectives.
- Is written at a level that is independent of the scope of BCM and does not include any specific information such as BCM requirements, processes, or operational roles.
- Is available as documented information that is communicated and understood by the whole organisation.

The policy should be appropriate to the size, complexity and type of the Rail Entity and aligned with the organisational culture and operating environment.

It should be written by top management with support from BC professionals. The policy should be reviewed at agreed intervals or following significant changes to the operating context.

7.3.1.2 Establishing Governance

Establishing good governance early in the development of BCM provides the foundation for further development, effective operation, support, and continual improvement.

The early identification of clearly defined roles and associated responsibilities is a key element of governance, and it is essential for effective BCM. Having top management sponsor the programme to establish BCM is necessary to ensure commitment across all organisational levels and functions.

Top management should ensure that the support and resource is needed to establish and operate BCM or available including funding, time, technology, and competent people. Top management should also ensure that people with accountable roles in BCM are competent and receive any necessary education and training.

Assigning overall accountability for BCM and its effectiveness to a member of top management ensures that BCM is recognised as a key part of the organisation.

Senior accountability for BCM makes it visible across the organisation, which may encourage collaboration across the organisational boundaries.

BCM responsibility should be included in job descriptions and communicated to all interested parties.

7.3.2 Embracing Business Continuity

Embracing BC is a paradigm shift from mandating and enforcing compliance by embedding BC into the organisation. Embracing supports the requirements present in policies and audit requirements and it is an outcome of education, awareness, and a greater understanding of the reason why the organisation needs protection from operational disruptions and emergencies. Embracing also elaborates and provides clarity on those nuances and grey areas that are often missing from the compliance and statutory requirements. This level of pragmatism is specifically designed to help persuade all members of an organisation to adopt BCM. Time demands and overall commitment from personnel will only be met once the workforce accept that BC must be up-to-date and operational to protect the organisation and its interested parties. This results in improved BC culture that delivers fit for purpose capability and competency.

The most common drivers for BC derived from regulations, statutory demands, audits, compliance requirements, risks, client expectations, and shareholder pressure. In response, top management normally mandate BC viral policy to protect the organisation from disruptions.

The term “embedding” is used to describe a process that defines how to integrate BC practice into BAU activities and organisational culture. Embedding includes allocating roles and responsibilities across the organisation’s hierarchy, providing training, scheduling BCM-related activities over the calendar and confirming adherence to the policy.

7.3.2.1 Understanding Organisational Culture

Fit-for-purpose BC requires the development of a management system that is consistent with the culture of the Rail Entity, so that the organisation embraces the programme across all management levels.

According to ISO 22316:2017, organisational culture is a set of collective beliefs, values, attitudes, and behaviours of an organisation that contribute to the unique social and psychological environment in which it operates.

It is important to understand the cultural attributes that the Rail Entity exhibits. BCM may then be designed to leverage the potential opportunities that the organisation’s culture provides while being aware of, and managing, the potential pitfalls. Ultimately, understanding the organisation’s culture may also help identify whether the culture might need to be influenced to encourage personnel to better embrace BC.

7.3.2.2 Understanding, Improving and Measuring an Organisation’s BC Culture

Understanding the internal BC culture is an essential part of ensuring the prioritised activities become resilient in the event of an emergency. BC culture means that continuity forms part of the operational fabric of the Rail Entity. It requires a collaborative approach embraced by all and demonstrated by top management and other key figures.

BC culture means a shared understanding of why BC is a priority for the organisation. It should involve everyone in the Rail Entity, not only BC professionals.

The behaviour, attitudes, and beliefs of personnel are indicators of the level to which the organisation is embracing BC. A Rail Entity that embraces BC will operate more sustainable BCM.

Conversely, a lack of commitment, especially from top management, will ultimately result in poor execution, lack of corporate involvement, and ineffective BCM. In achieving full commitment from personnel, top management must demonstrate clear support towards BCM and its related activities.

Further guidance on measuring BC culture and the methods and techniques for improving such can be found in the Business Continuity Institute Good Practice Guidelines 2023.

Ultimately, embracing BC is about strengthening the relationship between the Rail Entity and its internal and external stakeholders. It is important that everyone understands the importance of staying operational in the

face of emergencies. This in itself is a powerful relationship that demands protection from disruption. When there is effective and balanced BCM, the outcomes will be:

- A programme that is bespoke for every Rail Entity, taking into account its organisational culture.
- A policy engaging emotional intelligence and empathy to not lose sight of the pragmatism required for holistic BCM.
- Complementary processes in place to embrace the scope and policies across the entire organisation, not because they are mandatory but because it is universally agreed to be the correct and proper course of action for the benefit of the Rail Entity.

7.3.3 Analysis

BCM uses two organisational analysis techniques, the Business Impact Analysis (BIA) and Risk Assessment (RA).

The BIA estimates the impacts of disruption over time to determine the Rail Entity's response, recovery priorities, and resource requirements, namely the BC requirements.

The RA identifies the disruption risks to the Rail Entity's prioritised activities and required resources. The BIA is the foundation for designing effective recovery strategies and plans.

The outcome of the BIA and the RA is an input to the Solutions Design stage of BCM. Therefore, the quality and results of the BIA and RA process and its outcomes are extremely important.

7.3.3.1 Business Impact Analysis (BIA)

The BIA is the technique used to define the impact of a disruption over time.

By performing the BIA, the BC professional determines the prioritised activities, and the recovery timeframes and resource requirements.

The BIA is not a one-time or single-stage activity. Initially, it can help clarify the scope of BCM, after which it becomes an integral part of ongoing BCM, typically reviewed periodically (for example, annually) or in the event of significant organisational changes in the operating context or environment.

The technical specification ISO TS 22317:2021 is considered best practice for further details on conducting the BIA.

Rail Entities should use the following process for analysing business impacts to determine business continuity priorities and requirements:

- Define the impact types and criteria relevant to the Rail Entity’s context.
- Identify the activities that support the provision of products and services.
- Use the impact types and criteria for assessing the impacts over time resulting from the disruption of these activities.
- Identify the time frame (maximum tolerable period of disruption (MTPD)) within which the impacts of not resuming activities would become unacceptable to the Rail Entity.
- Set prioritised time frames within the MTPD for resuming disrupted activities at a specified minimum acceptable capacity (recovery time objective (RTO)).
- Use this analysis to identify prioritised activities.
- Determine which resources are needed to support prioritised activities.
- Determine the dependencies, including partners and suppliers, and interdependencies of prioritised activities.

The aim of BC is to ensure that the organisation’s products and services are restored before the MTPD is reached. The BIA identifies and sets the RTO for prioritised products, services, activities, and resources so that the organisation can develop and implement BC strategies and solutions supported by plans, used by competent teams of people, that avoid reaching the MTPD. The RTO should always be less than the MTPD. Where activities and resources support multiple products and services, the shortest time requirement of these products and services is the RTO.

The development of BC requirements should consider more than just the RTO. The BIA should also determine a minimum capability level at defined points of time. One common term used to describe this capability is the MBCO. The MBCO should be achieved at specific time, either at or after the RTO. Setting several MBCOs for different times after a disruption and for each product group may be appropriate. Where MBCOs rely on

outsourced service providers, the objectives should consider service level agreements and any legal or regulatory requirements.

On completion of the BIAs, a final consolidation of all analysis is conducted to help with the identification and implementation of recovery strategies and solutions.

Rail Entities can choose the appropriate quantitative and qualitative analytical approach, which can be influenced by the type, size, or nature of the organisation, as well as resource and other dependency constraints. While the Rail Entity may be flexible on the methodology for the analysis, it is imperative that they challenge and ensure that the data collection is credible, complete, reasonable, sufficiently accurate, and justifiable.

The BIAs should be regularly reviewed at pre-defined intervals or following a significant change within the organisation or in the external environment in which it operates. The BIA process and methodology should also be reviewed to continually improve its quality and ensure it continues to meet the organisation's purpose.

7.3.3.5 Risk Assessments

In the Analysis stage, the BIA is often conducted before the RA so that the organisation can just focus on the prioritised activities. This can maximise the benefit of any investment in risk treatments.

The BC professional then uses RA techniques to identify unacceptable risk, single points of failure, and opportunities for continual improvement. Risks are collated by using a scoring system based on the likelihood and consequence of the risk occurring. A risk is defined as: "An effect of uncertainty on objectives,' (ISO 31000:2018).

RAs involve methods to identify, analyse, and evaluate a range of risks relevant to the organisation. They use a formula based on likelihood and consequence to calculate a risk score. RA is defined as the overall process of risk identification, risk analysis, and risk evaluation: and it should be conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiries as necessary (ISO 31000:2018).

The key steps when undertaking an RA as part of BCM are as follows:

- Listing risk sources
- Performing a risk source analysis
- Evaluating risk

Tables 6 and 7 are examples of a RA matrix and present a priority thresholds table to assist with developing a risk matrix. In most cases, the organisation's risk management framework already has the assessment matrix defined, which is also applicable for BC.

Impact of disruption	Duration	Financial	Reputation	Health & Safety
Note: the impact categories and examples should be specific and relevant to the Rail Entity.				
3 – Major	More than 5 days	Over £1m cost / lost revenue	National damage to reputation / customer or community support	Potential for irreversible injuries / fatalities
2 – Moderate	2 to 5 days	£100k to £1m cost / lost revenue	Regional damage to reputation / customer or community support	Potential for serious injuries (hospitalisation)
1 – Minor	Up to 1 day	Less than £100k cost / lost revenue	Local damage to reputation / customer or community	Potential for minor injuries (time-off work)

Table 5 An example of a RA matrix for impact of disruption.

Probability of disruption	3 – Likely	2 – Possible	1 – Unlikely
	Frequent occurrence / at least once in a 3-year period	Infrequent occurrence / once in a 10-year period	Exceptional occurrence / once in a 30-year period

Combining the probability and impact scores for each threat produces a risk score (high/medium/low)			
3 – Major	High	High	Medium
2 – Moderate	High	Medium	Low
1 – Minor	Medium	Low	Low

Table 6 An example of a RA matrix for probability of disruption.

The outcomes from the RA as part of BCM are:

- An awareness of the range of risks that could disrupt the Rail Entity's activities.
- A prioritised list of risks based on the risk rating.
- Identification of any unacceptable risks and single points of failure.

The RA process can be ongoing, depending on the size, complexity, and type of Rail Entity. However, the methods used should be regularly reviewed at pre-defined intervals or following significant change as defined within the BC policy.

7.3.4 Solutions Design

Solutions Design identifies strategies and solutions that enable an organisation to resume business operations within the approved continuity requirements and identifies capabilities to mitigate unacceptable risks and single points of failure. Strategies outline the high-level approach for meeting the organisation's BC requirements. Solutions detail how the strategy will be delivered. BC recovery solutions include approaches, arrangements, methods, procedures, treatments, and actions that can be put in place to implement business strategies with due consideration to the associated costs.

The identification of strategies and solutions should be based on the extent to which strategies and solutions:

- Meet the requirements to continue and recover prioritised activities within the identified time frames and agreed capacity.
- Protect the organisation’s prioritised activities.
- Reduce the likelihood of disruption.
- Shorten the period of disruption.
- Limit the impact of disruption on the organisation’s products and services.
- Provide for the availability of adequate resources.

7.3.4.1 Strategies to Resume Business Operations

The strategies to resume business operations are based on the outcomes of the Analysis stage, which identifies the following:

- Prioritised products and services.
- Prioritised activities.
- The MTPD, RTO, MBCO, and RPO.

Strategies and solutions describe how the organisation can resume business operations when disrupted. The identification of solutions must always include a series of considerations that are relevant to BCM and the organisation as a whole. Solutions must meet the BC requirements but at the same time they need to be considerate of costs and benefits. For instance, the cost of mitigating the impact of a disruption should not exceed the cost of the disruption itself or introduce a secondary risk that negatively affects the organisation.

Developing strategies and solutions for the resumption of business operations is a three-step process which includes:

1. A gap analysis which identifies whether resumption capabilities meet the BC requirements.
2. The identification of a strategy to close existing gaps.
3. The design and selection of solutions that deliver strategies.

7.3.4.2 Mitigating Unacceptable Risks and Single Points of Failure

Within the context of the RA, strategies and solutions are concerned with the mitigation of unacceptable risks and single points of failure. The identification of solutions is influenced by a variety of business relevant considerations, including:

- Regulatory obligations: these must not be breached.
- Initial and ongoing cost-benefit: these must not outweigh the cost of disruption.
- Intangible benefits: must not be ignored.

- Contractual requirements: must not be breached.
- BC requirements: must not be breached.
- Secondary risk: a solution must not introduce additional risk.

The BC professional must identify and collaborate with those across the organisation that have a deep understanding of items with unacceptable risk, or the single point dependency, to identify mitigation strategies.

7.3.5 Enabling Solutions

Enabling Solutions implements the agreed BC solutions, designs a response structure to mobilise resources and deploy during an incident, together with developing BC plans that detail the response activities and procedures that response teams need to follow. The resulting plans and processes are designed to be scalable and therefore able to be deployed in response to any incident type.

7.3.5.1 Implementing BC Solutions

The BC professional needs to ensure that the implementation of the solutions meet the agreed specifications. Therefore, the following steps should be carried out:

1. Gathering the solutions design specifications of the accepted solutions.
2. Determining who will develop under the solutions.
3. Allocating project activities and agreeing on the planning.
4. Developing / implementing the solutions.
5. Monitoring and reporting progress.
6. Addressing issues - especially if they affect the ability to meet the specifications.
7. Ensuring alignment with the response structure and plans.
8. Conducting training for users and support staff.
9. Ensuring ongoing support is provided and available when required.
10. Validating the solutions to meet the specifications.
11. Closing the project and identifying lessons learned.

The implementation should be managed as a project in compliance with the Rail Entity's project management procedures and practices. The implemented solutions should be regularly reviewed and validated through exercises.

7.3.5.2 Designing the Response Structure

The purpose of establishing a response structure is 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 and establishes command, control, and communication to help the organisation manage the emergency and minimise its impact.

Further guidance on Response Structures can be found in RDG-OPS-ACOP-011 IEM, Response.

7.3.5.3 Communications

When responding to incidents, both internal and external communications are critical elements of an effective response. How interested parties perceive the response to the incident is a key factor in determining how successfully it is being managed. Poor messaging, slow response, lack of empathy for those impacted, and failure to acknowledge the incident can worsen an already bad situation. The purpose of communications is to position the organisation as the central source of information, demonstrate its control of the situation, and reassure interested parties.

Both internal and external communications should be relevant to BCM and should include the following considerations:

- On what to communicate.
- When to communicate.
- With whom to communicate.
- How to communicate.
- Who will communicate.

Engaging with Media and Social Media

Communication procedures should address how the Rail Entity manages communications with the media and on the organisation's social media channels. The plan should ensure that only appropriately trained and authorised personnel liaise with the media and communicate using social media channels. They should also participate in exercises.

Communications with the media should be via written statements, information placed on the organisation's website, or through the provision of a spokesperson for live interviews.

When communicating using social media channels, communications should be two-way. This can provide insight into how interested parties react to the Rail Entity's response to the incident.

If social media is a key element in the Rail Entity's communications response strategy, then an appropriate preparation strategy is required. For example, build up followers and establish its social media channel(s) presence as the organisation's authentic voice before an incident occurs.

Warning Plans
As part of emergency response, there may be instructions on how to notify people of an actual or possible incident. This may be a separate warning plan or part of an emergency response plan. The instructions should enable the recipients to take action to protect themselves, carry out an action, or involve themselves in responding to an incident.

The BC professional should facilitate discussions to ensure that the organisation has procedures for receiving, documenting, and responding to external warnings, alerts, or communications, including those from national, regional, or global risk advisories.

Spokespersons
A spokesperson represents the organisation and positions it as the central source of truth, demonstrating its control of the situation.

Spokespersons should respond according to the communications strategy, which conveys information to interested parties. Part of the duties of a spokesperson will include attending press conferences, presenting the organisation's view of an incident, and offering apologies when appropriate.

Identification of Interested Parties
Within all plans there should be a comprehensive list of interested parties who might need to be contacted during an incident. The following information should be recorded for all interested parties:

- **WHO** is the interested party? For example, personnel, suppliers, customers, community, and the media.
- **HOW** should they be contacted? For example, by telephone, email, social media, text, or letter. This section should include a selection of several communication channels.
- **WHEN** should they be contacted? For example, immediately after becoming aware of the incident, the next working day, within the first week, etc. If there are regulatory timeframes for reporting incidents, these should be documented.
- **WHAT** are their identified information requirements during an incident? For example, facts of the incident, actions they should take, impact on service delivery, and timescales for restoration.

Logging Information and Decisions
All Rail Entities should have procedures for logging and securely storing actions, events, communications, and decisions. Following an incident there should be a review; types of reviews can vary from internal reviews or a debrief to an external review, investigation, or inquiry.

It is best practice to record decisions and actions. Further guidance on logging and the role of loggists can be found in RDG-OPS-ACOP-011 IEM, Response.

7.3.5.4 Developing and Managing Plans
A BC plan is defined as: "Documented information that guides an organisation to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives," (ISO 22301:2019). The term BC plan suggests a single document; however, it may comprise several documents for use by different teams. In addition, the plan or plans are likely to be structured according to the Rail Entity's size, complexity, type, infrastructure, products and services, and locations.

While BC plans focus on business recovery, plans must also be developed to address other responses to an incident. The response structure should determine the number and types of plans to be put in place.

The BC plan is not intended to cover every eventuality as all incidents are different. Also, it is not possible to envisage every impact. Therefore, the plans need to be flexible enough to adapt to the specific incident and

the opportunities that may arise. However, in some circumstances, scenario-specific plans are appropriate to address a particular threat or risk, for example, a pandemic plan.

Plans are intended to be used in high-pressure, time-limited situations. Therefore, a user-friendly plan should be concise and easy to read. Plans are guidance documents, not reports, and should not contain information that is not needed during a response.

Regardless of the type of plan being developed, it should not be carried out in isolation. It is essential to be mindful of the Rail Entity's overall BC requirements and involve users of the plans, including top management, in the development process to achieve a successful outcome.

7.3.5.5 Strategic Plan

A strategic plan defines how strategic issues (for example, those threatening the organisation, its integrity, and viability) resulting from an incident should be addressed and managed by the strategic team.

A strategic plan is often referred to as a crisis management plan and might be supported by other strategic plans such as a crisis communication plan. The BC professional is usually tasked with developing the strategic plan in consultation with a variety of other senior managers. Depending on the response structure, there may be more than one strategic plan.

Some incidents do not involve physical disruption to the organisation and may not require the activation of an operational or a tactical plan. Examples could include fraud, malpractice, or negative media exposure that threatens the organisation's reputation.

There may also be incidents that result in the mobilisation of one or more operational teams which do not require the mobilisation of the strategic team. However, it is good practice, especially where there is the potential for reputational damage, to make the strategic team aware of the situation in case it escalates.

The strategic plan should describe the process for handling all types of crises stemming from an incident (anticipated and unanticipated) that require a strategic response. It may also contain checklists, actions, decisions, and communications needed in response to specific scenarios appropriate to the organisation.

Crisis Communications Plan

There should be a separate crisis communications plan as the communications team will often work in parallel with the strategic team. However, some smaller organisations prefer to include the crisis communications plan as part of the strategic plan because response is being guided by the same top management. A crisis communications plan may also cover communications during an incident which has not been declared a crisis.

Tasks within the crisis communications plan should be allocated to one person or a team and should include:

- Appointing a member to serve on the strategic team to advise on the communications strategy.
- Developing internal and external messaging. Ensuring these messages are cascaded throughout the organisation and, when required, outside the organisation to ensure consistency.
- Monitoring, liaising, and facilitating interactions with the media.
- Social media monitoring and engagement.
- Updating the website with information on the crisis. This could include the latest updates, actions pertaining to the organisation and interested parties, and alternative ways of working.
- Receiving and logging incoming communications.
- Preparing and briefing the designated spokesperson(s).

7.3.5.6 Tactical Plan

Tactical plans facilitate the coordination of response activities when several operational teams are involved. The tactical plan should include consolidated resource requirements and time frames defined in the operational plans so that recovery can be monitored and reported. In addition, it should identify the possible options to coordinate the response effort and any resulting needs.

Tactical plans focus on coordinating the recovery of a group of interrelated activities defined in operational plans. They can be used to address the coordination of response activities in single or multiple locations.

The tactical plan should include consolidated resource requirements and timeframes defined in the operational plans so that recovery can be coordinated, monitored, and reported. The tactical plan may also contain details of services which could be deployed to support the operational plans.

7.3.5.7 People Welfare Aspects in Emergency Response Plans

Rail Entities have a duty of care to safeguard the health, safety, and welfare of their personnel, contractors, visitors, customers, and members of the public. In some countries and industry sectors, this is a legal requirement.

Further guidance on people aspects and humanitarian assistance following a major passenger rail incident can be found in RDG-OPS-ACOP-011 IEM, Response.

Further National Recovery Guidance on humanitarian issues can be found at the following address: National Recovery Guidance: humanitarian issues - GOV.UK (www.gov.uk)

7.3.5.8 Operational Plans

There are various types of operational plans with differing names, scopes, and owners. The BC professional is typically not responsible for producing all these plans. However, the BC professional will need to make sure these plans are consistent in structure (for example, via a template), are available, and work together.

Operational plans may also be designed to maintain the organisation's ability to function in specific situations (for example, unavailability of a critical system or key equipment failure, a localised natural hazard, or hazardous material spill).

7.3.5.9 Process for Returning to BAU

"The organisation shall have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption," (ISO 22301:2019). Producing detailed plans for returning to BAU is a challenge as the state of the primary resources during the incident cannot be predicted. The Rail Entity should consider its increased vulnerability when its primary resources are lost during an incident. Before any incident, a plan outlining possible options and processes for returning to BAU should be developed. However, the details can only be specified when the impact of the incident is clear.

7.3.6 Validation

Validation confirms that established BCM meets the objectives set out in the policy and enables the organisation to embrace BC through an effective and efficient awareness, exercising, maintenance, and review programme.

Validation ensures the findings of the analysis are proportionately and reasonably reflected within BC Solutions Design and that the implemented solutions, in combination with the response structure and BC plans, work according to the agreed specifications and are commensurate with the size, complexity, and type of the Rail Entity. Validation provides methodologies to measure the quality and effectiveness of BCM and BC capability, the competence of individuals, and team cohesiveness. A positive approach and attitude toward Validation will allow strengths to be acknowledged and areas for development to be seen as opportunities for continual improvement rather than criticism.

Validation is achieved through a combination of the following activities:

- **Exercising**: the process to train for, assess, practice, and improve organisational performance (ISO 22300:2021).
- **Maintenance**: the process to ensure organisational BC arrangements and plans remain relevant and operationally ready to respond.
- **Review**: the process for assessing the suitability, adequacy, and effectiveness of BCM and identifying opportunities for improvement.

7.3.6.1 Developing an Exercise Programme

A Rail Entity’s continuity capability cannot be considered reliable or effective until exercised.

Further guidance on developing and carrying out tests and exercises can be found in RDG-OPS-ACOP-010 IEM, Preparation.

7.3.6.2 Maintenance

Maintenance of BCM keeps the organisation's BC arrangements up to date. This ensures that the organisation remains ready to respond to and manage the impacts of incidents effectively, despite a periodic organisational change or a change in the organisation's context.

Maintenance activities should be embedded within the organisation's BAU processes to be effective, rather than being a separate activity that may be overlooked.

7.3.6.3 Review

The purpose of a review is to evaluate BCM for continuing suitability, adequacy, and effectiveness, as well as identifying opportunities for improvement.

Review activities should be embedded within the Rail Entity's BAU processes to be effective, rather than being a separate activity that may be overlooked. The review cycle of the Rail Entity's BCM should evaluate its continued alignment to the:

- Policy, governance structure and strategic objectives.
- Culture and operating environment.
- Technology systems (primarily ICT-specific business applications and operating systems).

Most pertinent to the Rail Industry is post-incident reporting. See Chapter 5 of this document for further guidance.

8 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:

8.1 Provisions References

Endnote Number	Source
1	Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004
2	National Recovery Guidance June 2013
3	RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident
4	UK Inquiries Act 2005
5	RM^3 PI & RCS Planning and implementing risk controls through co-ordinated management arrangements: RCS 5 Emergency planning
6	JESIP Joint Doctrine Edition 3 October 2021
7	ISO 9001:2015 Quality Management Systems - Requirements
8	ISO 22301:2019 Societal security - Business continuity management systems – Requirements

8.2 Legislation & Regulation

Name of the document	Reference number
Civil Contingencies Act 2004	N/A
Health and Safety at Work Act 1974	N/A
Management of Health and Safety at Work Regulations 1999 (MHSWR)	N/A
Railways and Other Guided Systems (Safety) Regulations 2006 (ROGS)	N/A
Merchant Shipping Act 1995	N/A
Railways Act 2005	N/A
National Health Service Act 2006	N/A
Inquiries Act 2005	N/A

8.3 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

Major Incidents – Preparation of Aide-Mémoires for Senior Managers	RDG-OPS-GN-014
RDG Guidance Note: Critical Incident Management, Issue 1 – January 2023	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

8.4 International / British Standards

Name of the document	Reference
Security and Resilience – Crisis Management – Guidelines	ISO 22361:2022
Security and Resilience – Community and Resilience – Principles and framework for urban resilience	ISO 22371:2022
Governance of Organisations – Guidance	ISO 37000:2021
Security and resilience – Vocabulary	ISO 22300:2021
Societal security - Business continuity management systems - Requirements	ISO 22301:2019
Risk management - Guidelines	ISO 31000:2018
Organisational Resilience	ISO 22316:2017
Quality Management Systems – Requirements	ISO 9001:2015

8.5 Guidelines

Name of the document	Date of Issue
National Risk Register	August 2023
UK Resilience Framework	December 2022
JESIP Joint Doctrine: The Interoperability Framework Edition Three	October 2021
UK Severe Space Weather Preparedness Strategy	September 2021
Fleet Management Good Practice Guide: 20. Business Continuity Management – Issue 15	July 2020
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
National Recovery Guidance	June 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
Home Office - Recovery: An Emergency Management Guide	January 2006

8.6 Good Practice Sources / Materials / Textbooks

Name of the document	Date of Issue
Cabinet Office ResilienceDirect™	2024
International Institute for Sustainable Development	2024
The Business Continuity Institute Good Practice Guidelines 2023	2023
Department for Business, Energy & Industrial Strategy: UK Severe Space Weather Preparedness Strategy, September 2021	2021
Norfolk Resilience Forum Recovery Guidance 2020	2020
Office of Rail and Road RM^3 The Risk Management Maturity Model	2019
The Recovery Myth: The Plans and Situated Realities of Post-Disaster Response	2018
Pitt Review: Learning lessons from the 2007 floods	2008

9 Appendices

9.1 Capability Maturity Model Integration (CMMI)

The maturity model below is referenced within this CoP 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).

9.2 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.

9.2.1 Case Study #1 – Example Impact Assessment to Assess Economic Losses

An example of an impact assessment approach to assess economic losses follows. The results can help selection of recovery options from consideration of hazards and vulnerabilities in the area, cost benefit analysis, and application of risk management. Each step does not necessarily need to be explicitly followed. The starting point should always be to identify the purpose of the assessment, but beyond that, progress will often be iterative, going back over the initial steps as more information emerges to modify what has already been assessed.

The steps are outlined as follows:

1. Identify the purpose of the assessment

Define what the assessment is intended to be used for, what problem(s) its results might address (immediate estimation (for response) or survey accurate for full recovery) and what level of accuracy it hopes to achieve (aggregation of jurisdictional areas or individuals/properties). There has to be a name and definition of the emergency in sufficient detail to define the area and time boundaries.

2. Organise consultation and information collection

No impact assessment can be successful unless a clear process has been set up beforehand to define and manage it. There must be:

- A centre for operations and collecting/processing data.
- A set work plan with milestones for consultation, assessment, feedback, and final reporting.
- A timeframe within which all this has to happen.

Impact assessment involves input from many people and organisations and from assembled bodies of knowledge. This generally needs a committee made up of stakeholders to advise on the project. The consultation process not only means talking to people, but also covers setting up and running surveys, collecting, and manipulating database information, and generally getting access to information in any form that would add value to the overall impact assessment.

3. Define the area and timeframe of the assessment

In any impact assessment there has to be a clear boundary within which the impact of the emergency of that area can be defined and evaluated. It is important to define the area being assessed, especially when estimating indirect losses and benefits in the form of insurance payouts and aid.

When defining the area of the assessment, make sure it represents the local economy affected by the emergency. There also has to be a timeframe set to define how long after the emergency the assessment will be considering losses associated with it. Clearly, any assessment needs start and finish dates. Consider using a timeframe which is consistent with that of the response to, and of the recovery from, the hazard event. A flood event may use a timeframe of at least one to two years to fully assess indirect and intangible losses – unless indirect and intangible losses are judged to be unimportant in the emergency in question. As impact assessments will have to be reported during and after the emergency, consideration should be given to estimates of the likely indirect losses.

4. Select the type of assessment to be made

There are three commonly used approaches in assessing impacts after an emergency. They are:

- A rapid assessment, based largely upon pre-existing data for losses from similar previous emergencies – this is estimation from historic data – if relevant data exists.
- A synthetic approach, based upon modelled estimations of losses to model natural, built, social, and economic environments (e.g., using average building types and contents, population distributions, and economic models). Impacts are based on assumptions for the time or timespan of the event.
- A survey approach, where surveys are used to establish actual losses of the event being assessed.

Some combination of approaches could be used. The survey approach is commonly required for the post-event impact assessment – to enable effective recovery management. In selecting appropriate assessment methods, take account of the advantages and disadvantages of each method.

Inspections and Needs Assessments (surveys):
Where possible, surveys should combine inspections (making judgements from visual checks, such as whether a house may be safely reoccupied) with needs assessments (which involve interviewing affected residents). To cover both in a single visit to inform recovery management requires careful management and co-ordination. Much of the critical information will have been collected during more rapid response activities. Registration (the process of recovering personal details of those affected by the emergency) will have identified many of the affected people and safety inspections will have produced a list of damaged properties.

Inspections and needs assessments require the adoption of clear and consistent criteria for reporting so that accurate comparisons can be prepared. For example, an agreed definition would need to be reached as to when a property is said to be affected by flooding – is it if habitable areas were flooded, or if the garage was flooded, or if just the garden was flooded, etc? When data is to be collated over more than one local authority area (e.g., during widespread flooding emergencies), it is even more important that clearly defined criteria are agreed and used by all – particularly if funding streams may flow from this.

Building inspectors, insurance assessors and environmental health officers are all likely to make inspections. The inspection process needs to be managed to ensure that priority tasks are completed first and that coverage is completed with efficient use of resources.

Allowance needs to be given to additional impacts that may follow the initial hazard event (e.g., further rainfall or another high tide following a major flood, or the failure of a lifeline, such as a road, that survived the hazard event but then fails when it has to carry increased loads as other roads are not now available).

Surveys can be used to assist short-term recovery by:

- Determining numbers, locations, circumstances, and ethnicity of displaced and/or injured people.
- Assessing the safety of buildings for occupation and continued use.
- Assessing the state of lifeline utilities.
- Assessing the need for temporary works, such as shoring and temporary securing of property.
- Protecting property from unnecessary demolition.

Inspections and needs assessments also contribute to longer-term recovery measures through:

- Defining personal and community needs.
- Determining the aid and resources required for permanent recovery.
- Estimating the total cost of damage.
- Acquiring engineering, scientific and insurance data to inform the mitigation process.

5. Obtain information about the hazard event

The aim of this part of an impact assessment is not to go into precise definition of the extent and characteristics of the hazard event but to focus on the key aspects in sufficient detail for the purposes of assessment. The starting point is generally a map, in whatever format best describes:

- The extent of the affected or assessed area.
- The route of a moving hazard, such as a flood inundation or airborne contamination.

A map(s) would be supported by a wide range of source data such as:

- Automated or manual field measurements during and after the emergency, such as flood depths and flow rates, projected rainfall.
- Photographs, television or private videotape records, eyewitness accounts.
- Reports on any other secondary impacts from the emergency, such as resulting contamination or building/infrastructure failures.

6. Obtain information about the people, assets, and activities at risk

Impact assessment is a measure of damage and disruption to assets and the effect this has on people and businesses in the affected and other areas. Environmental losses also may be important. Unfortunately, impact assessment sometimes has to measure the occurrence (where, who, how many) of death, injury and displacement resulting from the emergency.

A full list needs to be prepared in consultation with informed parties after an actual emergency. The outcome should be a database of everything likely to be affected by the hazard event.

7. Identify the types of impacts

In this step, the information derived in Steps 5 and 6 is used to separate impacts into categories, generally

described as direct or indirect losses, and tangible or intangible. This helps define where the major impact components are likely to arise and what measurement techniques will be needed. Measurement techniques will depend on the approach selected in Step 4. Intangibles are often ignored yet are frequently identified as the most significant losses by the people affected.

8. Measure the extent of losses from all sources

This is where the counting of losses starts. Step 4 outlines the ways of addressing impact measurement in the survey, synthetic and averaging approaches to impact assessment, when looking at direct, indirect, and intangible losses. Rather than grouping all losses by each category of loss (direct, indirect, and intangible), it may be more practical to collate them by 'loss sectors', and determine indirect, direct, and intangible losses for each sector at a time.

For example, in a typical flood emergency, loss sectors like these could be used to separate the items into study areas including residential, rural (including farming type, e.g., dairy, horticulture, etc), industrial, cultural heritage, vehicles/boats, commercial (including retail, tourism and hospitality), infrastructure, environmental, etc.

9. Decide whether to count 'actual' or 'potential' losses

The use of actual or potential losses raises a number of issues for recovery management. For recovery, actual losses result from survey or direct indicators (e.g., loss of retail activity); potential losses are forecasts – dependant on the degree of recovery achieved:

- Actual losses may discriminate against well-prepared communities if the loss assessment is used to decide on the worth of mitigation options.
- Actual losses may discriminate against poorer communities as they will typically have fewer assets and less economic activity to be damaged by a hazard.
- The difference between actual and potential losses will change considerably over time as people move and as other circumstances change.

10. Calculate Annual Average Damages (AAD) if needed

This step is generally useful for detailing the economic impact to a region and the required investment the recovery redevelopment and the disaster mitigation that can be economically justified (in terms of losses avoided on an average year, using an estimate of AAD. AAD is calculated by plotting loss estimates for a given hazard at a range of magnitudes, against the probability of occurrence of the hazard event.

11. Assess benefits to region of analysis

Economic assessment measures the net loss to the economy in the area of analysis. To obtain net loss, any benefits to the economy resulting from the emergency need to be subtracted from the assessed losses. Assessment of benefits is particularly important within a regional context because post-event aid and insurance payouts will partly offset the tangible losses suffered, as the area of analysis becomes smaller. This step is only relevant for economic loss assessment.

12. Collate and present the results of the loss assessment

Present the collated results of the impact assessment in a simple format, including maps and a table with assessments of different types of impact identified, together with any benefits from the emergency. A statement on the importance of intangibles should also be included to ensure they are not overlooked in recovery redevelopments and associated mitigation measures.

9.2.2 Case Study #2 – Buncefield Oil Storage Depot Disaster 2005, Recovery Structures and Processes

In the early hours of Sunday 11th December 2005, explosions at Buncefield Oil Storage Depot, Hemel Hempstead, Hertfordshire resulted in a large fire, which engulfed a high proportion of the site.

Over 40 people were injured; there were no fatalities. Significant damage occurred to both commercial and residential properties in the vicinity and 2,000 people were evacuated on emergency service advice.

The fire burned for several days, destroying most of the site and emitting large clouds of black smoke into the atmosphere. Over 16,000 employees within the adjacent Maylands Industrial Area were unable to access work and 92 businesses were displaced for more than one week. 17 were forced to permanently relocate.

Overall, the explosion cost local businesses more than £70 million in lost stock, lost revenue, and relocation expenses.

How the Topic was Handled
In the initial stages of the incident, recovery issues were effectively considered and co-ordinated as part of the emergency response. However, the decision was soon taken to establish a multi-agency Recovery Group to co-ordinate recovery issues in more detail. The first meeting of the group took place on 13 December, under the chairmanship of Hertfordshire County Council's Director of Environment. Whilst the group was ultimately responsible to Strategic (Gold) Command, there would inevitably be an overlap with operational recovery related issues being addressed by Tactical (Silver) Command. Therefore, ensuring effective communications and liaison was a key issue.

It was intended from the outset that, as well as looking at short term actions, the Recovery Group would also be looking to put in place a more formal structure to effectively manage the longer-term recovery process. As well as identifying a way forward for the Recovery Group, it was proposed that three sub-groups should be established to address short term physical issues (e.g., infrastructure, utilities, maintenance, etc.), business recovery and community infrastructure and welfare.

It was also agreed that any political, elected official or stakeholder input would be more appropriately addressed directly through the Recovery Group, along with the generic issues of communications, finance, and resources. In particular, communications formed a key part of the recovery structure. Although the Recovery Group co-ordinated the overall strategy, it was also important that there was effective liaison throughout the recovery structure and, after a period of time, communications staff from Dacorum Borough Council were directly involved in the work of the sub-groups.

It was also recognised that the handover from the emergency phase to the multi-agency recovery phase would be more effective if the recovery structure accommodated the outstanding strategic objectives from Strategic (Gold) Command. The formal recovery structure and terms of reference for the Recovery Group and three sub-groups were agreed on 19 December. It was also agreed that Hertfordshire County Council's Director of

Environment should continue to chair the Recovery Group in is strategic role. Chairs from Dacorum Borough Council and Hertfordshire Chamber of Commerce and Industry were appointed for the three subgroups and swiftly tasked with establishing appropriate membership, agreeing the frequency of meetings, and developing actions plans. In addition, outstanding Gold Command strategic objectives were assigned to the Recovery Group or appropriate sub-group.

With the longer-term recovery structure effectively now in place, Strategic (Gold) Command (i.e., Herts Constabulary by this time) were formally notified that the Recovery Group was ready for a full handover of responsibility from the emergency response phase to the longer-term multi-agency recovery phase.

Lessons Identified
A month after the incident, the Recovery Group undertook a structured debrief to identify any lessons arising from initial recovery efforts and the establishment of the formal multi-agency recovery structure. The following were identified:

- Disasters that affect businesses also have a huge community impact.
- The sheer scale of the recovery phase and the number of agencies that need to be involved.
- A co-ordinated multi-agency response is important and there needs to be good communication channels between those dealing with the wider recovery and those responding on the ground.
- There is a need to engage directly with all communities, providing clear information.
- Having a clear understanding of the command structure is useful.
- There is a need for communications and information to be coordinated in a structured and systematic manner.
- The division of police resources, so that the Deputy Area Commander was involved at Silver (Tactical) Command and the Area Commander was involved in the wider recovery, worked particularly well.
- Good contact with key professionals throughout the recovery process is essential.
- There is a need for the recovery response to be flexible since different emergencies will call for different skills.
- There is a need to be clear on responsibilities in order to best fit in with the emergency activity.
- The recovery structure should be established as early as possible, as part of the overall response structure.
- The importance of the Recovery Group holding early public meetings and communicating with the public through all sorts of media.
- Guidance on recovery structures and the issues to be addressed need to be built into emergency plans.

- The role and importance of 'recovery' in relation to emergency planning and its relationship with Gold, Silver, Bronze needs to be clarified.
- The importance of having the right agency/person providing leadership.
- Relationships should continue to be built so that the Recovery Group, when it is established, is clear about its own responsibilities and the role of the agencies and individuals around the table.

The debrief process leading to the publication of the Buncefield Multiagency Debrief Report and Recommendations also identified the following learning points:

- Guidance on recovery should be built into emergency plans and should outline clear roles and responsibilities in order to ensure a joined up and comprehensive response.
- The business community should be engaged early on in the incident to facilitate good communication with businesses and an open dialogue.
- Relationships with local communities and the business communities across Hertfordshire should continue to be developed and enhanced so that they can fully contribute to the recovery phase of an incident.
- The existence of Hertfordshire Resilience and previously HESMIC meant that there was a strong culture of working together in terms of emergencies. The existing network, training, and previous experience of dealing with incidents created an inbuilt resilience and also allowed the confidence to be flexible in terms of the recovery process.
- Had the incident resulted in the loss of life then the recovery, and in particular the community recovery, would have been more complicated and probably would have been undertaken in a different format.

9.2.3 Case Study #3 – Class 800 series trains withdrawn from service for safety checks on Great Western Railway

When cracks were found on the bodyshell (yaw damper bracket and anti-roll bar fixing points) of some trains, rigorous safety checks by Hitachi Rail and the train operators impacted were carried out, with oversight from ORR. Stringent mitigation measures were put in place to allow the trains to re-enter service without passenger safety being compromised, which have assured no safety failures and trains have performed as specified while in service. ORR's final safety review sets out the root cause of the cracking, provides detail on Hitachi Rail's plan for long term fleet recovery and management, and identifies several areas of improvement for the industry.

Lessons learned from Operators

- The majority of operators have concluded their lessons learnt exercises and most of them have considered that their management system arrangements were sufficient and effective in managing the impact from the train cracks and subsequent vehicle stand down.
- It should be noted that the vehicle standdown impact varied greatly between operators, which depended on their reliance of the AT200/300 stock to facilitate their passenger train service provision.
- Many operators continue to regularly engage with Hitachi to understand and manage the effect of the cracks on fleet and implement solutions.
- Where operators were part of the same overall owning group, this allowed greater collaboration between them and readily accessible access to a greater pool of technical engineering resource.
- Operators are continuing to engage with Hitachi on a frequent basis to continue checks and testing along with agreeing possible short-term solutions on the cracks.

Conclusions

- Targeted checks for unexpected cracks in the vehicle structure are not normal practice in the rail sector. Nonetheless, Hitachi's maintenance staff identified the cracks before they developed to a level that resulted in harm, and action was taken well before any significant risk had developed of a failure that could compromise the safe operation of the rolling stock.
- All operators were able to demonstrate that they had appropriate safety management systems in place to manage the fleet stand down, to liaise appropriately with Hitachi and to make suitable and sufficient risk assessments for returning trains with cracks meeting defined criteria back into passenger service.
- Operators were supported by high-level governance within their organisations, and from the two main owning groups, with board sign-off for key decisions being required. They resisted any early external pressures to get trains back into service before the correct internal procedures had been followed.
- Each operator implemented their own assurance measures to ensure that the information provided by Hitachi was correct, and the proposals to return trains to service subject to enhanced checks were based on sound evidence. Hitachi has fully cooperated with operators carrying out assurance activities on train checks.
- Interfaces between both AT200/300 users and Hitachi appear well-managed although some operators

would prefer more detailed information to be shared from Hitachi to satisfy their safety and assurance processes for fleet management.
- One of the successes was drawing on Class 387 from other operators to help boost the available fleet, as well as the push through operation of Class 387s to other routes all at short notice and all whilst maintaining the correct safety validation process. Furthermore, the cross-TOC assistance such as Cross Country running trains on Great Western's behalf enabled passengers to keep moving.

Next steps
- The industry should conduct further work to identify the reasons for the higher levels of fatigue loading experienced by rolling stock. Since the Hitachi design complied with the applicable industry standards, the industry as a whole should evaluate whether the applicable standards take into account the loads arising from operation on the rail network in the UK.
- This industry collaboration will require the involvement of those parties responsible for design, manufacture and maintenance of rolling stock including, but not limited to, Hitachi. RSSB is positioned to manage activities like this within the industry. It should also include input from Network Rail and other infrastructure managers, as the parties responsible for the track infrastructure.
- Hitachi should carry out a formal review of the effectiveness of their processes for welding when the component geometry is more challenging, which should include consideration of whether the existing approach adequately mitigates the risks of a weld with insufficient fusion being accepted.
- Designers of rolling stock should understand the risk posed by SCC and give it specific consideration when proposing the use of 7000 series aluminium components.
- The industry should consider whether a standard for mitigating SCC risk should be developed, as no dedicated standard currently exists.
- The industry should develop a process for responding to similar future cross-industry crisis events and appoint a strong, independent chair who can maintain pace, focus, and ensure all voices are heard.

9.2.4 Case Study #4 – Western Route of the Elizabeth Line incident on 7th December 2023

On December 7th, 2023, an incident took place on the western route of the Elizabeth Line in West London. Hundreds of passengers were stranded on trains due to damaged overhead electric cables. The disruption affected both the Elizabeth Line and the Great Western Railway.

The incident arose when a train struck an obstruction between Paddington and Acton mainline resulting in damage to overhead wires and causing significant delays as a result. Passengers were stuck onboard trains in challenging and uncomfortable circumstances, for hours with heating and lighting turned off. Most of the approximately 4000 passengers on the affected trains were evacuated onto the tracks and walked to safety. Network Rail halted all services while engineers worked to fix the issue and urged passengers to follow staff advice. Repair work was considered high risk and time-consuming. The disruption also impacted the Elizabeth line and the Heathrow Express to and from the airport.

Conclusions
- Putting the needs of people before assets must remain a priority for the rail industry.
- Staff in response or recovery roles should have appropriate training, experience, and competence to undertake that role effectively.
- Empowered and timely decision-making by representatives of responding agencies has a significant impact of the effectiveness of recovery efforts.

Lessons Learned
- Even when short-term recovery doesn't go to plan, that doesn't mean that long-term recovery can't positively contribute to future planning and help drive industry-wide improvement.
- Further clarity is required around who can declare a major incident and what actions should then be taken.
- A clearer and more straightforward categorisation of incidents improves communication and understanding within the rail industry and for responding partners.
- A joint-industry major incident response protocol can help ensure a cohesive response to major incidents by establishing a consistent approach.

As part of the response protocol, Network Rail (with MTREL and GWR) subsequently established the RAIDED acronym below, to give those managing the response a consistent way of assessing and addressing stranded trains:

- **Risk & Opportunities**
  - Aligned stranded trains board across the industry that is digitally available in multiple operational locations.
  - Hierarchy of opportunities guide, providing actions to de-strand trains.
  - Huddle plan for stranded trains between Rail Incident Commander (NR), Tactical Incident Commander (NR) and Stranded Train Champions (TOC).

- **Access**
  - Using technology to align the GPS coordinates of services to the nearest access point.
  - Welfare and onward travel plans for each access point, as a developed contingency plan.

- **Information**
  - Stranded Train Champions charged with gathering onboard information to feed into the joint risk assessment.
  - Automation of information gathering from onboard equipment to be developed.
  - Prioritisation matrix for stranded services to help determine priority trains.
  - First wave and second wave responder process developed to identify and then provide additional resources to stranded trains.

- **Dynamic Decisions**
  - Alignment across the industry in the use of G-FORCE.
  - Hierarchy of control for evacuations.

- **Evacuation**
  - Interface with CE plans and their delivery.
  - Introduction of TOLO Lite capability.
  - Review memorandum of understanding between Network Rail and Rail for London (Infrastructure) (RfLi) to support personnel responding to evacuations.
  - Review availability of onboard equipment such as PPE to support resource deployment for evacuations.

- **Decision Point**
  - Clearly defined decision points that are articulated and subsequently stuck to.
  - Measures of success developed and aligned across the business.

9.2.5 Case Study #5 – M25 DBFO, Connect Plus Services Freight Stakeholder Engagement, 2009 - ongoing

Relevance: The DBFO is responsible for operating and maintaining the M25 and the contract plays a key role in supporting National Highways' customer imperative, where Highway Operators are considered to be service providers and highway users are viewed as customers. Key freight stakeholders include the Road Haulage Association, Logistics UK, and Royal Mail.

Action Taken: Within CPS, they regularly engage with Royal Mail operational managers in the Southeast to share their project plans and understand the impact that these plans may have on their business.

Benefits: Through this engagement, they learnt that starting works in the Dartford Tunnel 15 mins later than planned has a big benefit to postal operations in Kent. That small delay to the start of planned works can avoid a major disruption to postal operations as a result of diverting vehicles – a clear example of "getting the basics right" for customer service, by integrating stakeholders needs into standard decision-making processes.

9.2.6 Case Study #6 – East Region Design Services Contract, National Highways, 2019 – ongoing

Relevance: The region includes a number of major traffic generators for freight and critical routes to support their safe and effective movement around the country, e.g., the A14 provides key access between the region's ports and the West Midlands to more than 85,000 drivers every day, including more than 21,000 hauliers transporting essential goods.

Action Taken: CPS have engaged with a range of freight customers, including independent SME operators, where they have successfully applied good practice from previous schemes to minimise any impact on the customer's operations.

CPS regularly engage face to face with freight customers in specific locations, such as a business park with logistic companies and high HGV traffic close to a planned network closure.

They have also worked closely with ports and have planned works around the timings of incoming and outgoing vessels, and developed communications material in multiple languages for the port to cascade to freight drivers.

Benefits: Intel and data from freight companies is more widely shared and can also include information provided by others via a community customer knowledge depository. The regional Customer Centric Action Plan then drives better coordination between activity on the network, and this focus will tune approaches to consider diversion route utilisation in areas which substantially impact freight movements.

9.3 Full Provision List

Provision Number	Provision Statement
Chapter 3. Recovering From Emergencies	
3.2.1	Rail Entities ***MUST*** cooperate with all requests in relation to Public Inquiries. [4]

3.2.2	Rail Entities ***SHOULD*** ensure tested structures and procedures are in place for the recovery phase following an emergency. [1, 2]
3.2.3	Rail Entities ***SHOULD*** ensure the recovery phase begins at the earliest opportunity following the onset of an emergency, running in tandem with the response to the emergency. [1, 2]
3.2.4	Rail Entities ***SHOULD*** follow national recovery guidance from Cabinet Office National Recovery Guidance - GOV.UK (www.gov.uk) in providing appropriate representation at the RCG, as well as communicating and sharing information with the RCG when necessary. [1, 2]
3.2.5	Rail Entities ***SHOULD*** follow and refer to the RDG-OPS-ACOP-001 Joint Industry Provision of Humanitarian Response Following A Major Passenger Rail Incident, to ensure survivors of Major Passenger Rail Incidents are dealt with safely, efficiently and compassionately during the recovery phase. [3]
3.2.6	Rail Entities ***SHOULD*** consider attendance and contribution to sub-groups of the RCG, including management of multiple requests for attendance at different geographical RCGs in Emergency Preparedness cross-industry arrangements. [1,2]
3.2.7	Rail Entities ***SHOULD*** ensure recovery planning and management arrangements are included in and supported by training programmes and multi-agency exercises. [1,2]
3.2.8	Rail Entities ***SHOULD*** ensure recovery planning and management arrangements are extensively covered and clarified in role specifications, responsibilities, and capabilities expectations for responder role-holders and senior managers who will be expected to attend RCGs and manage recovery at site. [1,2]
3.2.9	It is important to ensure that the time, resources, and effort spent on planning is effective and will make a significant difference should an event occur. Planning for recovery ***SHOULD*** be [1,2]: • Risk-based. • Proportionate. • Flexible, scalable, and non-prescriptive. • Open to lessons learned from previous events. • Inclusive. • Collaborative • Coordinated.
3.2.10	Rail Entities ***SHOULD*** identify in advance, data, and information requirements to support impact assessment and facilitate the development of recovery strategies. Rail Entities ***COULD*** focus on how to access the information rather than gathering and maintaining all the data. Identify the custodians of data and information and consider how you will develop, maintain, and share these resources. [1,2]
3.2.11	Rail Entities, as part of planning for recovery, ***SHOULD*** consider bringing together relevant partner organisations to start the thinking on issues that will need to be addressed, and agree the criteria, steps, process, or strategy to assist the decision making, should an event occur. [1,2]
3.2.12	Rail Entities ***SHOULD*** clarify and agree communication (and media) roles and responsibilities. For example, this may be between communications specialists working at local or national level or on issues that would be the focus for partnership working. [1,2]
3.2.13	Rail Entities ***SHOULD*** develop clear communications strategies and arrangements for recovery, that can be used across industry. [1,2]
3.2.14	Rail Entities recovery arrangements ***SHOULD*** follow a common set of underpinning principles, from National Recovery Guidance from Cabinet Office, and these ***SHOULD*** be applied at the local, subnational, and national levels. [1,2]
3.2.15	Rail Entities ***SHOULD*** utilise the reporting framework (recovery-reporting-framework-1.pdf (publishing.service.gov.uk) for recovery, introduced by Cabinet Office. [1,2]
3.2.16	Rail Entities ***SHOULD*** contribute to Impact Assessments carried out by local authorities and LRFs, via the RCG sub-groups. [1,2]
3.2.17	Rail Entities ***SHOULD*** develop a media handling strategy and arrangements for recovery that can be used across industry, ensuring it aligns to the wider multi-agency RCG strategies. [1,2]
3.2.18	Rail Entities ***COULD*** ensure senior representatives attend community engagement meetings where requested. Senior representatives should be members of the RCG, and be clear about the agreed multi-agency strategy, actions, and messages. [1,2]

3.2.19	Rail Entities ***SHOULD*** plan for planned and spontaneous memorial events and be aware of the symbolic importance and emotion that will be attached to the management of such tributes. [1,2]
Chapter 4. Emergency Response	
4.2.1	Emergency response and recovery arrangements ***SHOULD*** be flexible and tailored to reflect the circumstances. [1]
4.2.2	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]
4.2.3	Rail Entities ***SHOULD*** embed within their local debrief processes; the facility to capture lessons relating to interoperability, the application of JESIP Principles for joint working and models and national resilience capabilities. [6]
4.2.4	Debriefing ***SHOULD*** be honest and open, and its results disseminated widely. But should not compromise any ongoing investigation. [1]
4.2.5	Rail Entities ***SHOULD*** ensure a debrief following a Critical Incident follows a formal process with identified outcomes. It ***SHOULD*** be chaired or facilitated by an appropriately trained individual within the rail entity or multi-agency response organisation and supported by a structured debrief trained member of staff, or external debriefer if considered appropriate. [6]
4.2.6	Rail Entities ***SHOULD*** arrange for senior media representatives to meet with senior members of the emergency services and other organisations involved in the incident, some weeks later, to assist parties in looking at how information was provided and identifying improvements in the future. [2]
4.2.7	Rail Entities ***SHOULD*** ensure that a continuous evaluation of the recovery phase takes place, and that any issues identified are captured and actioned as necessary. Identifying issues from all partners involved in the recovery process. Consideration should also be given to obtaining views from the affected community (residents and businesses). [2]
4.2.8	Rail Entities ***SHOULD*** ensure the collation of lessons identified from the recovery phase of emergencies and exercises is the same as those used for the response phase. [1]
4.2.9	Rail Entities ***SHOULD*** ensure hot debriefs are facilitated by an appropriately trained representative (a number of members of staff within an organisation should be trained in formal debriefing techniques) and all comments from all responding organisations and roles ***SHOULD*** be captured and written down / recorded in whatever process is considered the most appropriate for the circumstances. [6]
4.2.10	Rail Entities ***SHOULD*** ensure appropriate attendance at multi-agency cold debriefs. A review of initial and further comments received should take place, along with an action plan with accountable owners for each action. Where applicable these actions ***SHOULD*** be accepted by Rail Entities and be cleared as soon as possible. [1]
4.2.11	Rail Entities ***SHOULD*** consider utilising the JESIP multi-agency debrief template for all multi-agency incidents. [6]
4.2.12	All critical incidents should be subject to ongoing review and monitoring. Rail Entities ***SHOULD*** ensure reviews have senior management oversight and are managed at an appropriate level of Command. [1]
4.2.13	Rail Entities ***SHOULD*** ensure the points captured at the hot debrief are recorded on the Command and Control log as well as the relevant debrief form. [1]
4.2.14	Rail Entities ***COULD*** consider utilising the debrief process considerations, structure and meeting model detailed at 4.3.2.2. [6]
4.2.15	Rail Entities ***SHOULD*** actively seek to find and share more effective ways of dealing with emergencies. [5]
4.2.16	Rail Entities ***SHOULD*** strive for continual improvement in response to all emergencies. [5]
Chapter 5. Post Incident Reporting & Information Dissemination	
5.2.1	Rail Entities ***SHOULD*** utilise the Joint Organisational Learning Online standard, tool and supporting processes from JESIP. [6]

5.2.2	Rail Entities ***SHOULD*** ensure staff trained on, responsible and accountable for the recovery phase of an incident are knowledgeable on the Cross-Government Principles on Recovery Reporting (5.3.1). [2]
5.2.3	Rail Entities ***SHOULD*** ensure once the debrief report is completed it is circulated with those who attended the debrief and within the wider industry if necessary. [2]
5.2.4	Capture of information for Organisational Learning is key and ***SHOULD*** be made available where appropriate to the wider rail industry. This ***SHOULD*** be achieved by the provision of an identified site which can be accessed by the whole organisation. [6]
5.2.5	Where identified, lessons learnt ***SHOULD*** be used to inform the future training needs of Rail Entities and ***SHOULD*** be incorporated in exercising plans. [1]
Chapter 6. Corrective and Preventative Actions (CAPA) Management	
6.2.1	Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve a quality management system. [7]
6.2.2	Top Management ***SHOULD*** demonstrate leadership and commitment with respect to the quality management system. [7]
6.2.3	Rail Entities ***SHOULD*** determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system. Rail Entities ***SHOULD*** monitor and review information about these external and internal issues. [7]
6.2.4	Due to the effect or potential effect of interested parties on a Rail Entity's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, Rail Entities ***SHOULD*** determine [7]: • The interested parties that are relevant to the quality management system. • The requirements of these interested parties that are relevant to the quality management system.
6.2.5	Rail Entities ***SHOULD*** monitor and review information about these interested parties and their relevant requirements. [7]
6.2.6	Rail Entities ***SHOULD*** determine the boundaries and applicability of the quality management system to establish its scope. [7]
6.2.7	The scope of the Rail Entity's quality management system ***SHOULD*** be available and be maintained as documented information. [7]
6.2.8	Rail Entities ***SHOULD*** determine and select opportunities for improvement and implement any necessary actions to meet customer requirements and enhance customer satisfaction. [7]
6.2.9	Corrective actions ***SHOULD*** be appropriate to the effects of the nonconformities encountered. [7]
6.2.10	Rail Entities ***SHOULD*** retain documented information as evidence of both the nature of the nonconformities (and any subsequent actions taken) and the results of any corrective action. [7]
Chapter 7. Business Continuity Management (BCM)	
7.2.1	Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve BCM, including the processes and resources needed and their interactions, in accordance with the requirements of ISO 22301:2019. [8]
7.2.2	Rail Entities ***SHOULD*** determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCM. [8]
7.2.3	When establishing BCM, Rail Entities ***SHOULD*** determine the interested parties that are relevant to BCM and the relevant requirements of these interested parties. [8]
7.2.4	Rail Entities ***SHOULD*** implement and maintain a process to identify, have access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, activities, and resources. [8]
7.2.5	Rail Entities ***SHOULD*** ensure that the applicable legal, regulatory, and other requirements are taken into account in implementing and maintaining its BCM. Rail Entities ***SHOULD*** document this information and keep it up to date. [8]

7.2.6	The scope of BCM ***SHOULD*** be available as documented information. Rail Entities ***SHOULD*** also determine the boundaries and applicability of BCM to establish its scope and ***SHOULD*** consider [8]: • The external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of BCM. • Both the requirements of interested parties and any legal and regulatory requirements. • Its mission, goals, and internal and external obligations.
7.2.7	Rail Entities ***SHOULD*** establish the parts of their respective organisations, products, and services to be included in BCM, taking into account organisations location(s), size, nature, and complexity. [8]
7.2.8	Top management ***SHOULD*** provide leadership and commitment with respect to BCM. [8]
7.2.9	Top management ***SHOULD*** establish a business continuity policy. The policy ***SHOULD*** be available as documented information and communicated both within the organisation and to interested parties. [8]
7.2.10	Top management ***SHOULD*** ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organisation. Top management ***SHOULD*** assign the responsibility and authority for 8: • Ensuring that BCM conforms to the requirements of ISO 22301. • Reporting on the performance of BCM to top management.
7.2.11	When planning for BCM, Rail Entities ***SHOULD*** consider the issues referred to in Provision 7.2.6 and determine the risks and opportunities that need to be addressed to [8]: • Give assurance that BCM can achieve its intended outcome(s). • Prevent, or reduce, undesired effects. • Achieve continual improvement.
7.2.12	Rail Entities ***SHOULD*** plan and evaluate the effectiveness of actions to address risks and opportunities and integrate and implement these actions into its BCM processes. [8]
7.2.13	Rail Entities ***SHOULD*** establish business continuity objectives at relevant functions and levels. The objectives ***SHOULD*** [8]: • Be consistent with the business continuity policy. • Be measurable (if practicable). • Take into account applicable requirements. • Be monitored. • Be communicated. • Be updated as appropriate. • Rail Entities ***SHOULD*** retain documented information on the business continuity objectives. • Determine what will be done, what resources are required, who will be responsible, when it will be completed and how the results will be evaluated.
7.2.14	Rail Entities ***SHOULD*** carry out any changes to BCM in a planned manner, and ***SHOULD*** consider [8]: • The purpose of the changes and their potential consequences. • The integrity of BCM. • The availability of resources. • The allocation or reallocation of responsibilities and authorities.
7.2.15	Rail Entities ***SHOULD*** determine the necessary competence of person(s) doing work under its control that affects its business continuity performance and ensure that these persons are competent on the basis of appropriate education, training, or experience. [8]
7.2.16	Persons doing work under the Rail Entity's control ***SHOULD*** be aware of the BC policy and their contribution to the effectiveness of BCM, including the benefits of improved business continuity performance and the implications of not conforming with the BCM requirements. [8]
7.2.17	Rail Entities ***SHOULD*** ensure their competent person(s) understand their own role and responsibilities before, during and after emergencies. [8]
7.2.18	Rail Entities ***SHOULD*** determine the internal and external communications relevant to BCM. [8]

7.2.19	Documented information required by BCM and by ISO 22301:2019 ***SHOULD*** be controlled to ensure [8]: • It is available and suitable for use, where and when it is needed (including preservation of legibility and version control). • It can be distributed, accessed, retrieved, and used. • It is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).
7.2.20	Documented information of external origin determined by the Rail Entity to be necessary for the planning and operation of BCM ***SHOULD*** be identified, as appropriate, and controlled. [8]
7.2.21	Rail Entities ***SHOULD*** ensure that outsourced processes and the supply chain are controlled. [8]
7.2.22	Rail Entities ***SHOULD*** implement and maintain systematic processes for analysing the business impact and assessing the risks of disruption. [8]
7.2.23	Based on the outputs from the business impact analysis and risk assessment, Rail Entities ***SHOULD*** identify and select business continuity strategies that consider options for before, during and after disruption. The business continuity strategies ***SHOULD*** be comprised of one or more solutions. [8]
7.2.24	Rail Entities ***SHOULD*** determine, implement, and maintain the resource requirements for the selected business continuity solutions so they can be activated when needed. [8]
7.2.25	Rail Entities ***SHOULD*** identify, and document business continuity plans and procedures based on the output of the selected strategies and solutions. [8]
7.2.26	Rail Entities ***SHOULD*** implement and maintain a structure, identifying one or more teams responsible for responding to disruptions. [8]
7.2.27	The roles, responsibilities, competencies and authorities of each team and the relationships between the teams ***SHOULD*** be clearly stated. [8]
7.2.28	Rail Entities ***SHOULD*** alert interested parties potentially impacted by an actual or impending disruption and ***SHOULD*** ensure appropriate coordination and communication between multiple responding organisations. [8]
7.2.29	Rail Entities ***SHOULD*** exercise their warning and communication procedures as part of their exercise programme. [8]
7.2.30	Business continuity plans ***SHOULD*** meet the requirements set out in ISO 22301:2019. [8]
7.2.31	Rail Entities ***SHOULD*** have documented processes to restore and return business activities from the temporary measures adopted during and after a disruption. [8]
7.2.32	Rail Entities ***SHOULD*** implement and maintain a programme of exercising and testing that meets the requirements set out in ISO 22301:2019 in order to validate over time the effectiveness of its business continuity strategies and solutions. [8]
7.2.33	BC evaluations ***SHOULD*** be conducted at planned intervals, after an incident or activation, and when significant changes occur. [8]
7.2.34	Rail Entities ***SHOULD*** determine the requirements for monitoring and measurements as set out in ISO 22301:2019. [8]
7.2.35	Rail Entities ***SHOULD*** conduct internal audits at planned intervals to provide information on whether BCM conforms to both the organisation's own requirements for its BCM and the requirements of ISO 22301:2019 as well as audits to inform whether BCM is effectively implemented and maintained. [8]
7.2.36	Rail Entities ***SHOULD*** consider planning, establishing, implementing, and maintaining the management review processes outlined in Section 7.3.6.3 Review. [8]
7.2.37	Rail Entities ***SHOULD*** determine opportunities for improvement in the suitability, adequacy, and effectiveness of BCM and implement necessary actions to achieve the intended outcomes of its BCM. [8]
7.2.38	When nonconformity occurs, Rail Entities ***SHOULD*** follow the requirements set out in ISO 22301:2019 and the guidance in Chapter 6 (Corrective and Preventative Actions). [8]
7.2.39	Rail Entities ***SHOULD*** consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities, relating to the business, or to BCM, that shall be addressed as part of continual improvement. [8]

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