Rail Delivery Group

National Rail

RDG Approved Code of Practice:
Rail Emergency Management - Preparation

RDG-OPS-ACOP-010
Issue 1.2 – 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 first ACOP in a series across the prepare-respond-recover model for IEM:

- **RDG-OPS-ACOP-010: 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 prepare for emergencies within the remits of IEM activities. The Code addresses the legal and regulatory provisions required when preparing for emergencies and reflects industry guidance and other best practice for preparedness. The Code outlines these requirements across key topics of organisational preparedness, planning requirements, training & awareness, testing & exercising and communication needs / multi-agency partnerships.

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, including railway undertakings or operators (including infrastructure maintainers and charter operators (passenger and freight)).

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	22/12/2023	First Draft
1.1	08/02/2024	Final Document Issue
1.2	13/06/2024	Final Document Issue aligned to CoP for Response and Recovery

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

Authorised by:
Rail Resilience Steering Group (RRPSG)

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

Contact: Andrew Wade

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

Contents

Abbreviations

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

Acronym	Full Form
AAP	Anticipate, Assess, Prevent
ACoP	Approved Code of Practice
ADDIE	Analysis, Design, Development, Implementation, Evaluation
ALBs	Arm's length bodies
BAU	Business-as-Usual
BoD	Board of Directors
BTP	British Transport Police
BC	Business Continuity
BCI	The Business Continuity Institute
BCM	Business Continuity Management
BCMS	Business Continuity Management System
CAPA	Correct and Preventative Action
CAPSS	Cyber Assurance of Physical Security Systems
CCA	Civil Contingencies Act 2004
CCS	Civil Contingencies Secretariat
CIPD	Chartered Institute of Personnel and Development
CMEP	Crisis Management Excellence Programme
CMS	Competence Management System
CMT	Crisis Management Team
CNI	Critical National Infrastructure
COBR	Cabinet Office Briefing Room
CoP	Code of Practice
CTC	Counter Terrorist Check
DFID	Department for International Development
DfT	Department for Transport
DLUHC RED	Department for Levelling Up, Housing and Communities Resilience and Emergencies Division
EA	Environment Agency
EM	Emergency Management
EPC	Emergency Planning College
FOC	Freight Operating Company
GBRTT	Great British Railways Transition Team
GCS	Government Communication Service
GN(s)	Guidance Note(s)
GPG	Good Practice Guidelines
GSM	Global System for Mobile Communications
IEM	Integrated Emergency Management
ISO	International Organisation for Standardisation
JDM	Joint Decision Model
JESIP	Joint Emergency Services Interoperability Programme

JOL	Joint Organisational Learning
KPI	Key Performance Indicators
LNA	Learning Needs Analysis
LoA	Lines of Assurance
LRF	Local Resilience Forum
LRP	Local Resilience Partnership
LUL	London Underground
MCA	Maritime and Coastguard Agency
MHSWR	Management of Health and Safety at Work Regulations 1999
MTPAS	Mobile Telecommunications Privileged Access Scheme
NHS	National Health Service
NPIA	National Policing Improvement Agency
NPSA	National Protective Security Authority
NRR	National Risk Register
NRSP	National Rail Security Programme
NSRA	National Security Risk Assessment
ORR	Office of Rail and Road
PRIMER	Plan, rehearse, implement, maintain, evaluate, recover
PRR	Prevent, Respond, Recover
PSTN	Public Switched Telephone Network
RACI	Responsible, Accountable, Consulted, Informed
RAIB	Rail Accident Investigation Branch
RAIRR	Rail (Accident Investigation and Reporting) Regulations 2005
RAM	Relevance, Alignment, Measurement
RDG	Rail Delivery Group
RM^3	Risk Management Maturity Model
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RRF	Regional Resilience Forum
RRP	Rail Resilience Project
RRPSG	Rail Resilience Project Steering Group
RRPWG	Rail Resilience Project Working Group
RRPs	Regional Resilience Partnerships
RSBB	Rail Safety and Standard Board
SAT	Systematic Approach to Training
SFO	Station Facility Owner
SIDOS	Security In the Design of Stations
SIM	Subscriber Identity Module
SIO	Station Incident Officer
SIRP	Station Incident Response Plan
SMS	Safety Management System
SOP	Standard Operating Procedure
SP	Station Plan
SRL	Security Response Level
SRO	Senior Responsible Officer
SSP	Station Security Plan

TfW	Transport for Wales
TIM	Traffic Incident Management
TOC	Train Operating Company
TOLO	Train Operator Liaison Officers
TSG	Telecommunications Sub Group
UKRA	UK Resilience Academy
VBS	Voice Broadcasting Service
VGCS	Voice Group Call Service
WECC	Western Electricity Coordinating Council
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
Assurance	Assurance provides certainty through evidence and brings confidence that systems are working. With assurance, triangulated evidence is provided to demonstrate that what needs to happen is happening. Evidence is seen in practice or reliable sources of information are received and reviewed. Organisations often have evidence of historic progress in the area in question and outcomes that confirm this. *Source: Governance 101: assurance and reassurance* Assurance and compliance activity related to IEM are addressed by the Three Line of Assurance (3LoA) model. The definition of this model can be found in RDG ACOP: Part A – Governance.
Business Continuity	Capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. *(ISO22301:2019 Security and resilience – Business continuity management systems – requirements).*
Business Continuity Management (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).*
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).*
Category 2 Emergency Responders (as relevant to railway operations)	The Civil Contingencies Act 2004 sets out: 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 organization is directed, overseen, and held accountable for achieving its defined purpose. *(ISO 37000:2021 Governance of Organisations – Guidance).*
Hazard	Hazards are non-malicious risks such as extreme weather events, accidents, or the natural outbreak of disease. *(UK Resilience Framework, December 2022).*
Incident	An event or situation that can be, or could lead to, a disruption, loss, emergency or crisis. *(ISO 22361:2022 Crisis Management)*
Integrated Emergency Management	Integrated Emergency Management (IEM) is the framework adopted by UK government and Devolved Administrations for anticipating, preparing for, responding to, and recovering from emergencies or disruptive events. The aim of IEM is to develop flexible and adaptable arrangements for dealing with emergencies, whether foreseen or unforeseen. It is based on a multi-agency approach and the effective co-ordination of those agencies. It involves Category 1 and Category 2 responders (as defined in the Civil Contingencies Act 2004) and also the voluntary sector, commerce, and a wide range of communities. *(Preparing Scotland – Scottish Guidance on Resilience Chapter 3).*
Interoperability	Interoperability in integrated emergency management is the extent to which organisations can work together coherently as a matter of routine. Interoperability allows emergency responders to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real-time, when needed, and when authorised. *(JESIP Joint Doctrine: jesip.org.uk).*
Issue	A change in environment, product, system, process, or control which presents new/change in exposures and requires action to forestall the cause or potential causes of one or more incidents.
Joint Decision Model (JDM)	The Joint Decision Model (JDM) is a common model used nationally to enable commanders to make effective decisions together in a multi-agency working environment. It is part of the Joint Emergency Services Interoperability Principles (JESIP), which aim to ensure the emergency responders are trained and exercised to work together as effectively as possible. The JDM centres around three primary considerations: Working together, saving lives, and reducing harm.

	The JDM guides commanders through the steps of an emergency situation and helps bring together available information, reconcile objectives, and make effective collaborative decisions. *(JESIP The Joint Decision Model (JDM)).*
Joint Emergency Services Interoperability Principles (JESIP)	JESIP (Joint Emergency Services Interoperability Principles) aims to improve and standardise the way the police, fire and rescue and ambulance services work together when responding to major multi-agency incidents. To achieve the overarching aim of 'working together, saving lives, reducing harm', JESIP models and principles have become the standard for interoperability across the responder agencies in the UK. JESIP is the thread that should run through all plans and subsequent incidents, and recovery from these. All incident phases need to consider multi-agency working, best served by following the JESIP principles. The JESIP *Joint Doctrine: the interoperability framework* sets out a standard approach to multi-agency working, along with training and awareness products for responding organisations to train their staff. Whilst the initial focus was on improving the response to major incidents, JESIP is scalable, so much so, the principles for joint working and models can be applied to any type of multi-agency incident.
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)*
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.
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).*

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.**
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).* **The DfT has identified six priority risk areas to the transport network (see Section 3.3.4.1)**
Risk Appetite	The amount of risk an individual, business, organisation or government is willing to tolerate. *(UK Resilience Framework: December 2022).*
Severe Space Weather	Space weather is a collective term used to describe variations in the Sun, solar wind, magnetosphere, ionosphere, and upper atmosphere that can influence the performance of a variety of technologies, and that can also endanger human health and safety. Day-to-day space weather, much like terrestrial weather, most often occurs with no tangible disruptive impacts. The UK Severe Space Weather Preparedness Strategy is focused on the rare events that could have a significant impact on infrastructure or vital services. The strategy directly supports the aims of the 2021 Integrated Review of Security, Defence, Development and Foreign Policy by seeking to build resilience to the risk of severe space weather, whilst also making science and technology integral to addressing this risk. *(Department for Business, Energy & Industrial Strategy: UK Severe Space Weather Preparedness Strategy, September 2021)*
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).*
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).*

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 ***preparedness*** in the context of IEM within the rail industry.

To support the provisions, accompanying guidance is provided to allow users a reference for best practice and/or examples for the associated preparedness elements for IEM. It is hoped that the GNs will enable 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 preparation 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 contribute to, or who are responsible for their Rail Entity's preparedness for 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:

- The Carmont derailment, August 2020.
- The mass self-evacuation outside Lewisham during darkness and poor weather conditions, March 2018.
- 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**:**

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

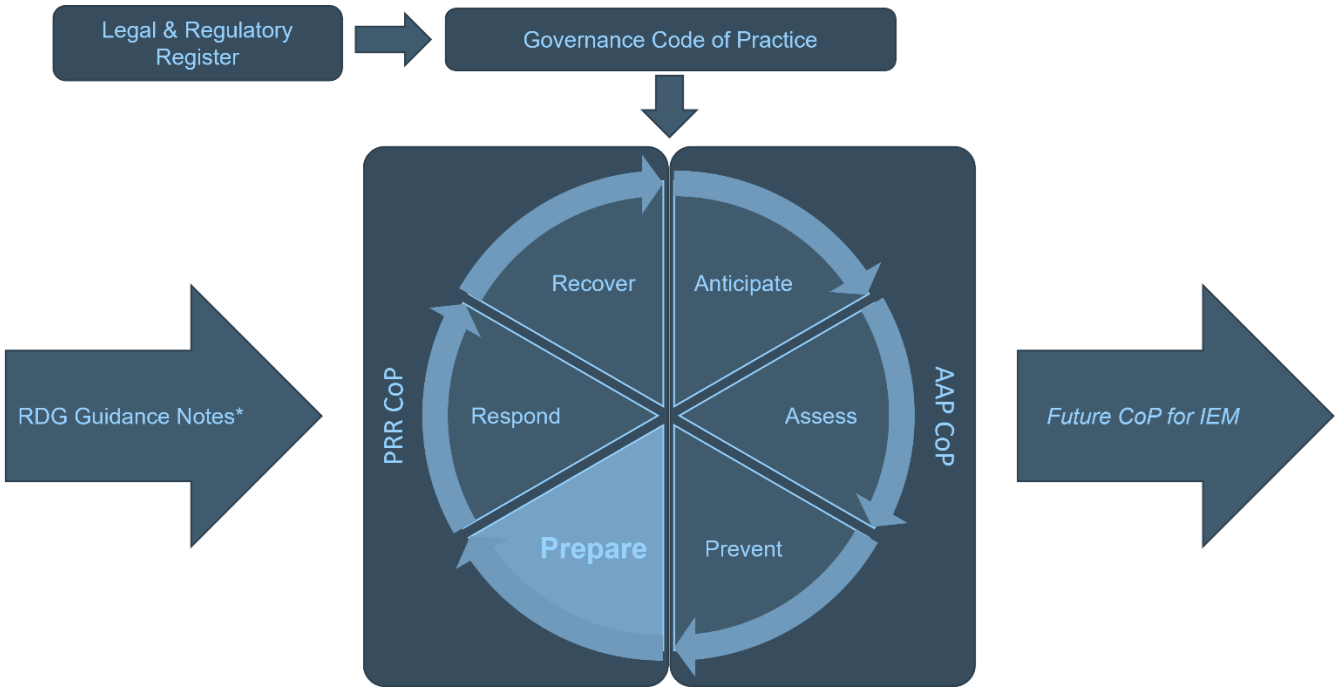

Figure 1 Document orientation

*** Other RDG Guidance Notes used to support IEM CoP are referenced in Section 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 – Preparation & Resilience
Chapter 4 – Planning for Emergencies
Chapter 5 – Training & Awareness │ Testing & Exercising
Chapter 6 – Communication │ Multi-Agency Partners
Chapter 7 – References
Chapter 8 – Appendices

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

Chapters 3-6 are structured as follows:

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

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

1.6 Reading the 'Provision' Statements

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

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

Term	Definition
Must	A **legal or regulatory requirement**, and what is typically meant by a provision statement. For example, preparedness '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 – Preparedness & Resilience Chapter 4 – Planning for Emergencies Chapter 5 – Training & Awareness | Testing & Exercising Chapter 6 – Communication | Multi-Agency Partners
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 – Preparedness & Resilience Chapter 4 – Planning for Emergencies Chapter 5 – Training & Awareness | Testing & Exercising Chapter 6 – Communication | Multi-Agency Partners
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 the RDG ACoP: Part A – Governance is also referenced within this CoP (see Appendix 8.1). There are ***COULD*** provision statements within the following chapters: Chapter 3 – Preparedness & Resilience Chapter 4 – Planning for Emergencies Chapter 5 – Training & Awareness | Testing & Exercising Chapter 6 – Communication | Multi-Agency Partners

Table 1 Definition of provision statements.

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

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 Preparedness.

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".
[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 emergencies through planning, training, and testing and exercising
5. **Response**: being able to deal with emergencies 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.

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 to improve and further refine it.

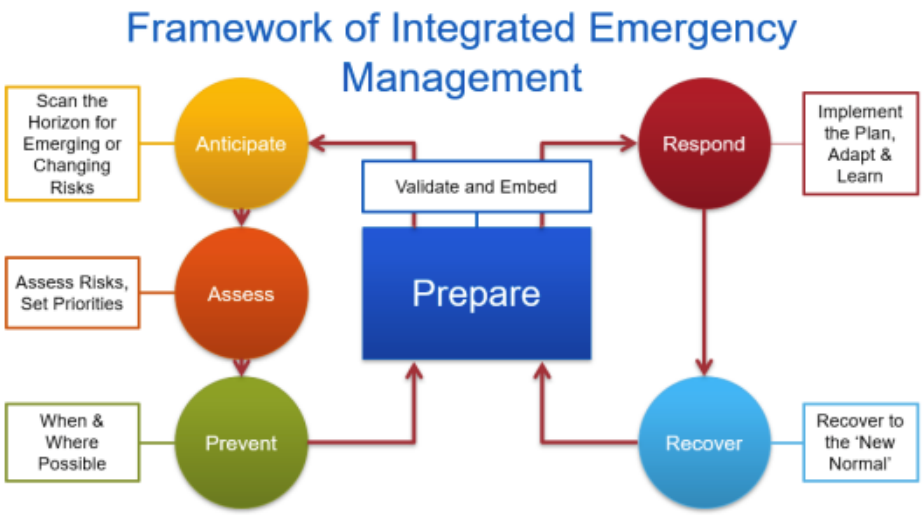

Figure 2 Framework of IEM, sourced from the Emergency Planning College.

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 the RDG ACOP: Part A – Governance and is applicable for this RDG CoP for Preparation.

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 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).
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 is important to help quantifying the benefit in resilience investments. Creating 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

Preparing for an incident encapsulates the resilience principles above. This is further detailed below in Chapter 3.

2.4 Risk Management in relation to Emergency Management

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

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).

2.5 Martyn's Law

It is important to reflect other elements within the resilience landscape whose change may impact IEM in rail. One such change is the imminent introduction of Martyn's Law (previously the Protect Duty) for the security and resilience industry. Whilst not yet approved in law, the below outlines the creation of Martyn's Law and the implications it may have on this CoP in the future for consideration amongst Rail Entities:

- On 2nd May 2023, the UK government published the Terrorism (Protection of Premises) Bill, creating what is otherwise known as Martyn's Law. The legislation will require public venues and organisations to implement varying security measures by reference to a tiered system, based upon capacity, to reduce the risk to the public from acts of terrorism.
- The Bill will impose obligations on those responsible for certain premises and events to consider the threat from terrorism and implement reasonably practical and proportionate measures to mitigate the risk. The Bill also establishes an associated inspection and enforcement regime, which will seek to educate, advise, and ensure compliance with the requirements of the Bill.
- It is understood that the legislation will primarily be applicable to locations that are not already subject to a transport security regime under S.119 Railways Act 1993 and this will therefore exclude large parts of the national rail network. Martyn's Law will be relevant for landowners with landlord responsibility for premises that do not comprise stations or depots, and for private/heritage network operators.

It is too soon to provide commentary on how Martyn's Law might impact the Rail Industry as there are many elements of the legislation that are yet to be decided. Nevertheless, it is understood that the standard duty requirements are designed to ensure there is a baseline level of protection and preparedness across the UK.

3 Preparedness & Resilience

3.1 Overview

It is imperative for Rail Entities to prepare for emergencies, from both a legal and regulatory perspective but also to protect their ability to continue to service rail operations across the country in the event of an emergency.

3.1.1 A Resilience Framework

Incorporating resilience within a Rail Entity can be achieved by following a resilience framework for preparing for emergencies. The new UK Resilience Framework 2022 stated:

"We live in an increasingly volatile world, defined by geopolitical and geoeconomic shifts, rapid technological change and a changing climate. This context means that crises will have far reaching consequences and are likely to be greater in frequency and scale in the next decade than we have been used to. We have a responsibility to prepare for this future."

Rt Hon. Oliver Dowden CBE MP **|** ***Chancellor of the Duchy of Lancaster***

Preparation is about identifying and then understanding the risks we face and being able to adequately address such risks in the future. The framework addresses the need for preparation and resilience by setting out action plans for the following:

- Improved risk assessment, including that within areas not traditionally assessed, to better identify what risks we face.
- Increased responsibility and accountability for risks.
- Improved partnerships to support cooperation for resilience activity.
- Empowering local communities to support resilience capability.
- Investing in resilience activities
- Upskilling resilience capability
- Reinvigorating national exercise programmes

Such principles can be developed within the Rail Industry to support the continued development of IEM and resilience across the network.

3.1.2 Resilience Capability & Capacity

An organisation capable of resilience is one that is prepared to respond effectively in uncertain times and that can manage and recover from the unexpected.

The characteristics of the organisation and how this is embedded into the overall organisational culture has a large impact on the resiliency of an organisation, as well as the resources allocated to a focus on resilience elements within day-to-day work. Resilience must be integrated from the initial design stage through to system resilience, ensuring resilient infrastructure and systems providing a baseline level of resilience, that with effective processes in place can be built upon and improved.

It is important to have the right roles in place within the organisation to support the preparation for an emergency, however, it is equally as important to ensure a general level of awareness in resilient principles across the entire organisation.

A workshop held by RDG in April 2021 shed light on the capacity for individuals responsible for emergency management within Rail Entities. Some organisations had several resources dedicated to resilience / emergency activities, however, others had limited resources dedicated to such. It is not clear if these were full time dedicated roles, or roles within the organisation that had an element of responsibility within other daily job activities. Additionally, the majority of respondents stated a desire for additional dedicated emergency management roles with the appropriate and necessary competencies, experience and qualifications to improve their capability and capacity as an organisation to prepare for major emergencies.

Rail Entities can assess their maturity for resilience by using a recognised and industry leading methodology, for example, the ORR Risk Management Maturity Model (RM^3) (see Appendix 8.1 for further details). It is accepted that the level of maturity, and the need for IEM roles and responsibilities across Rail Entities will

vary substantially.

It is also accepted that there is no one-size-fits-all model which can be used as a complete measure of resilience maturity for all organisations across all industries. RM[3] is used as an example here due to ORR's close involvement in rail resilience.

3.1.3 Embedding a Resilient Culture

Additionally, processes in place to support the preparedness for emergencies play a large part in building an organisation's capability to be resilient.

The RDG ACoP: Part A – Governance outlines the need to embed resilience within each organisation as being fundamental to enhancing the ability of the group to deal with emergencies. This CoP outlines this by integrating the following resilience disciplines *(based on Network Rail's descriptor headings):*

Figure 3 Embedding resilience across the organisation (Source: RDG ACoP: Part A – Governance / Network Rail).

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

The RDG ACoP: Part A – Governance stresses the importance of inclusive engagement across the resilience disciplines. It is essential to embed IEM / resilience objectives into overall business strategy and delivery. Cross-discipline engagement forms a key part of governance activities.

3.1.4 Achieving Infrastructure Resilience

The RDG CoP for AAP references infrastructure resilience as the ability of assets and networks to anticipate, absorb, adapt to, and recover from emergencies.

Ensuring the resilience of both rail infrastructure and its associated activities can be achieved by mainstreaming the following framework:

1. **Good Governance** involves defining roles and responsibilities so that rail entities' functions do not overlap and there is not competition for limited financial and human resources. This also includes public, accountability, transparency, and anti-corruption measures.
2. **Information Flows** between infrastructure system managers, staff, and users as well as across multiple agencies and infrastructure systems. Efficient information flows must also exist to transmit lessons learned following emergencies and crises.

3. **Flexibility** to be able to change and evolve in response to changing conditions.
4. **Resourcefulness** is the ability to mobilise assets and resources to meet priorities and goals. This includes financial, social, physical, technological, information, and environmental resources.
5. **Responsiveness and recovery** are the ability and motivation of rail entities to skilfully manage a shock as it unfolds and restore function and order rapidly after a failure. This includes identifying options, prioritising what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Response and recovery depend primarily on people, not on technology. Rapid recovery is the capacity to get things back to normal as quickly as possible after an emergency. Emergency management and business continuity plans and the means to get the right people and resources to the right places are crucial.
6. **Adaptability / Capacity to learn** is the means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis. Engineers, emergency planners, transport operators, owners, regulators etc. are able to learn from experience and past failures. Processes encourage reflexivity and learning from past failures and events.
7. **Reliability** is the capacity and capability of an asset/activity to maintain operations under a range of conditions. Reliability is built in during the design and build phases.
8. **Redundancy** describes the ability to keep operating through a substitute or redundant systems that can be brought to bear should something important break down or stop working. Redundancy involves increasing diversity of pathways and options so when one fails, others that serve a similar function can substitute and take their place.
9. **Safe Failure** involves designing infrastructure so that when one component fails it does this progressively with minimal disruption to other parts of the infrastructure and network.
10. **Robustness** is the ability of infrastructure assets and the network to withstand stresses and shocks to a level that is designated tolerable and cost effective (NB standards of tolerability and design standards change over time)

Source: Designing for Infrastructure Resilience (2016)

Provisions and Accompanying Guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document. The RDG ACoP: Part A – Governance also identifies a provision in relation to preparedness*.

3.2 Provisions

3.2.1 Rail Entities ***MUST*** ensure that recommendations of the Rail Accident Investigation Branch (RAIB) are considered and acted upon, where appropriate within emergency planning arrangements. [20]

3.2.2 Rail Entities ***SHOULD*** adhere to requirements of the Railway Group Modular Rule Book when accessing Network Rail infrastructure in an emergency. [17]

3.2.3 Rail Entities' Safety Management System (SMS) ***SHOULD*** include IEM activity throughout all its processes and provisions. [21]

3.2.4 The SMS ***COULD*** clearly demonstrate how the organisation is kept aware of good practice in the rail and other industries, so that continuous improvement can be maintained. [3]

3.2.5 The SMS ***COULD*** be adaptable and responsive to change, to accommodate emerging issues / risks and reasonably foreseeable developments in legislation, technology, social, environmental, and political influences, whilst maintaining assurance. [3]

3.2.6 The SMS ***COULD*** be an integral part of the organisation's overall management system. [3]

3.2.7 The monitoring arrangement ***COULD*** address proportionately and appropriately all the processes and systems within the SMS to ensure their implementation, adequacy, and effectiveness. [6]

3.2.8 Rail Entities ***SHOULD*** implement a Business Continuity Management System (BCMS) determined by the external and internal issues that are relevant to its purpose and that affect its ability to achieve its intended outcome(s). [2]

3.2.9 Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of ISO 22301. [2]

3.2.10 Rail Entities ***COULD*** proactively seek good practice examples in emergency management. [3]

3.2.11 Stakeholders ***COULD*** be consulted on and informed of best practice, to continually improve collaborative relationships and shared risk reduction.[3]

3.2.12 Risk assessment ***COULD*** be used to drive continual improvement in the risk profile of the organisation.[4]

3.2.13 Enterprise-level guidelines and standards ***COULD*** be in place with best practices incorporated from other industries.[5]

3.2.14 There ***COULD*** be clear evidence of searching for best practice in asset management and condition monitoring as part of the drive to continuous improvement.[5]

3.2.15 Rail Entities ***COULD*** be an early adopter of new standards relating to monitoring and recognised as an 'early complier' organisation. [6]

3.2.16 Appropriate risk assessment processes ***COULD*** be used to make strategic choices related to the totality of the rail infrastructure. [4]

3.2.17 Rail Entities ***COULD*** strive for continuous improvement in risk assessment processes looking at alternative techniques, which challenge the effectiveness of risk controls, by working with other organisations in their own and other industry sectors. [4]

3.2.18 Rail Entities ***COULD*** maintain an external view to identify effective risk controls from other organisations and other industry sectors. [4]

3.2.19 Rail Entities ***COULD*** be recognised as industry-leaders in risk management. [4]

3.2.20 Rail Entities ***COULD*** lead cross-industry risk reduction programmes. [4]

3.2.21 Active steps ***COULD*** be taken to identify, evaluate and utilise novel ways of monitoring to achieve continuous improvement in risk control. [6]

3.2.22 Managers ***COULD*** actively participate in industry-wide and cross-industry groups to improve risk control monitoring techniques e.g., remote condition monitoring. [6]

3.2.23 The organisation ***COULD*** have closely linked outcome and activity indicators which demonstrate risk controls are optimised. [6]

3.2.24 The organisation ***COULD*** be known for mature relationships with collaborators who strive to work again with the organisation as they are assured that risks will be controlled. [6]

3.2.25 Across the organisation monitoring activities ***COULD*** be recognised as vital in improving risk control.[6]

3.2.26 Rail Entities ***SHOULD*** understand the implications of incidents and incident response on corporate reputation. [19]

3.2.27 Emergency planners ***SHOULD*** have an understanding of risk management, train and station operation, command and control, and familiarity of IEM principles. [19]

3.2.28 Information on work history type and cost, condition and performance ***COULD*** be recorded at asset component level. [5]

3.2.29 Systematic and fully optimised data collection programme ***COULD*** be in place with supporting metadata. [5]

3.2.30 There ***COULD*** be evidence of an effective pro-active and predictive maintenance regime across the organisation. [5]

3.2.31 Preparedness for incidents ***SHOULD*** include gaining a level of understanding about the other organisations that may be involved at incidents. [12]

3.2.32 Rail Entity staff ***SHOULD*** be familiar with extreme weather plans and competent in their application. [16]

3.2.33 Rail Entities ***SHOULD*** increase the provision of response staff when weather related incidents are likely to occur. [16]

3.2.34 Additional staff ***SHOULD*** be co-located in strategic locations and in conjunction with emergency response agencies (BTP, for example). [16]

3.2.35 Rail Entities ***SHOULD*** not permit an employee to perform at the same time both the roles of TOLO and the RAIB Accredited Agent for a particular incident. [17]

3.2.36 Rail Entities ***SHOULD*** have a plan for the structure of Crisis Management Team (CMT) meetings. [19]

3.2.37 Rail Entities ***SHOULD*** have a plan to outline the relationship between the CMT and the strategic command.[19]

3.2.38 Rail Entities ***SHOULD*** determine knowledge and experience requirements and skills levels for personnel undertaking specific roles in emergency plans. [19]

3.2.39 Rail Entities ***SHOULD*** undertake a joint review into the response to, and management of the emergency.[19]

3.2.40 Rail Entities ***COULD*** produce a detailed report of the review including actions required and how and by whom they will be closed out. [19]

***The RDG ACoP: Part A - Governance identifies the following provision in relation to preparedness:**

Rail Entities ***COULD*** use a SMS to demonstrate how the organisation will identify opportunities to improve, not only against its own targets but against other organisations' targets which have been identified as being excellent. [3]

3.3 Guidance Notes

3.3.1 Building Resilience within an Organisation

There are a number of best practice items to highlight to guide the reader to achieve resilience within their organisation. As part of regulatory requirements, the following guidance as per the CCA provides a basis for preparation and resilience activity for Rail Entities.

The section is followed by non-regulatory requirements that will support the implementation of the provision statements detailed in this chapter.

3.3.2 Rail Entities Duty to Prepare

The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) provide the regulatory regime for rail safety, including the mainline railway, metros (including London Underground), tramways, light rail and heritage railways.

ROGS duty holders, as defined in those regulations, have a statutory duty to ensure that accidents, incidents, near misses and other dangerous occurrences are reported, investigated, and analysed and that necessary preventative measures are taken.

It is recommended that Rail Entities follow the ORR guidance to ROGS on the implementation of a Safety Management System (SMS) in order to comply with the provisions of the regulations.

The same regulations also require the production of plans for such events and for duty holders to co-operate as basic elements of their respective safety management systems.

Source: Incident Response Planning & Management. Railway Group Standard. GO/RT3118 October 2008, superseded by RIS-3118-TOM Issue 2 Incident Response Planning & Management.

3.3.3 Civil Contingencies Act (CCA)

The CCA, and accompanying non-legislative measures, delivers a single framework for civil protection in the UK. The Act is separated into two substantive parts: local arrangements for civil protection (Part 1); and emergency powers (Part 2).

3.3.3.1 CCA Part 1

Part 1 of the Act and supporting Regulations and statutory guidance 'Emergency preparedness' establish a clear set of roles and responsibilities for those involved in emergency preparation and response at the local level. The Act divides local responders into two categories, imposing a different set of duties on each.

Those in Category 1 are organisations at the core of the response to most emergencies (the emergency services, local authorities, NHS bodies). Category 1 responders are subject to the full set of civil protection duties (Figure 4). They will be required to:

- Assess the risk of emergencies occurring and use this to inform contingency planning.
- Put in place emergency plans.
- Put in place business continuity management arrangements.
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency.
- Share information with other local responders to enhance co-ordination.
- Co-operate with other local responders to enhance co-ordination and efficiency.
- Provide advice and assistance to businesses and voluntary organisations about business continuity management (local authorities only)

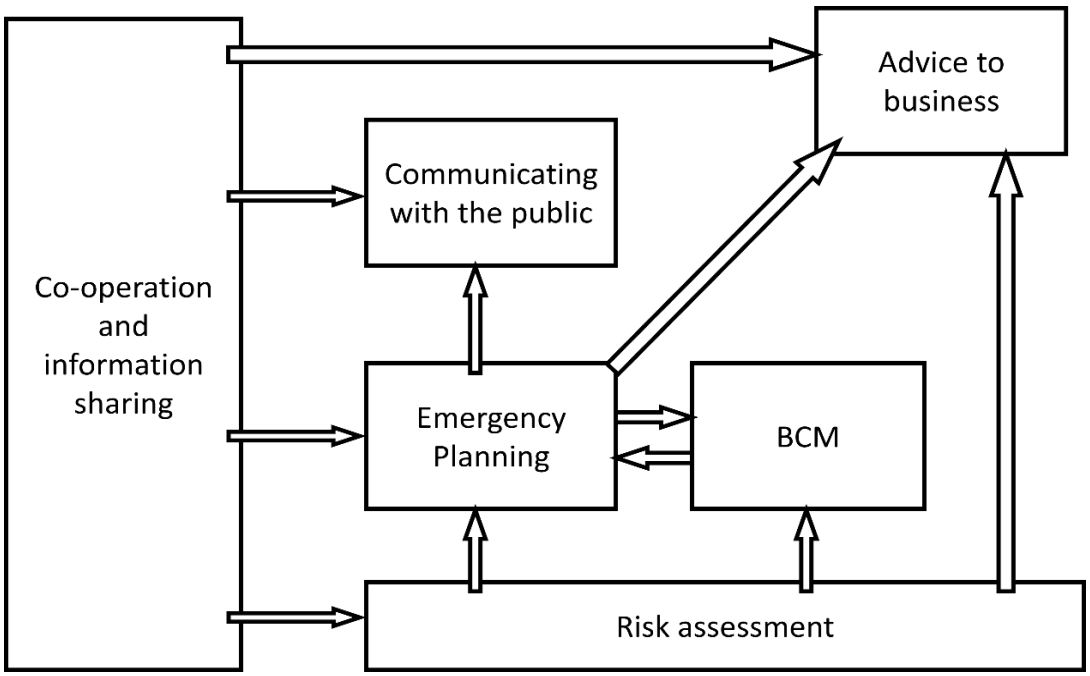

Figure 4 How the six civil protection duties under the Act and the Regulations fit together (Source: Civil Contingencies Act Emergency Preparedness Chapter 1 Introduction)

Category 2 organisations (the Health and Safety Executive, transport, and utility companies) are "co-operating bodies". They are less likely to be involved in the heart of planning work but will be heavily involved in the response to incidents that affect their own sector. Category 2 responders have a lesser set of duties; they lend their hand in co-operating and sharing relevant information with other Category 1 and 2 responders.

Category 1 and 2 organisations come together to form 'local resilience forums' (based on police areas) which help co-ordination and co-operation between responders at the local level. For more on what LRFs do and contact details for each, see the guide on 'Local resilience forums: contact details'.

Emergency Preparedness supports those individuals and organisations which have a statutory duty in the civil protection framework and those organisations subject to duties under the CCA. The CCA ultimately focuses on emergency preparedness, but its requirements should be seen within the wider context of integrated emergency management (IEM) and referral should be made to RDG ACoP: Part A – Governance.

Source: Preparation and planning for emergencies: responsibilities of responder agencies and others.

3.3.3.2 CCA Part 2

Part 2 of the Act was brought into force in December 2004; it updates the 1920 Emergency Powers Act to reflect the developments in the intervening years and the current and future risk profile. It allows for the making of temporary special legislation (emergency regulations) to help deal with the most serious of emergencies. The use of emergency powers is a last resort option and planning arrangements at the local level should not assume that emergency powers will be made available. Their use is subject to a robust set of safeguards - they can only be deployed in exceptional circumstances.

Source: Preparation and planning for emergencies: responsibilities of responder agencies and others.

3.3.4 Application of Risk in Resilience

For full detail of the risk management process, refer to RDG Guidance Note: Rail Emergency Management CoP Anticipation, Assessment and Prevention. This guidance provides supporting information on integration of risk into the Preparation phase of the IEM cycle.

3.3.4.1 National Risk Register

The National Risk Register (NRR) 2023 is the external version of the National Security Risk Assessment (NSRA); the Register details the UK government's assessment of the most serious risks facing the UK. The NRR assesses the likelihood and impact for each risk. The risks that meet the threshold for inclusion in the NRR would have a substantial impact on the UK's safety, security and/or critical systems at a national level. The NRR includes information about 89 risks, within 9 risk themes.

Risks can manifest in a variety of ways and with varying levels of severity. To ensure the UK is prepared for a broad range of scenarios, the NRR sets out a 'reasonable worst-case scenario' for each risk. These scenarios are not a prediction of what is most likely to happen but represent the worst plausible manifestation of that particular risk. This enables relevant bodies to undertake proportionate planning.

More specifically, the UK rail network faces a broad and diverse range of risks. The scale and exposed nature of the transport network makes it vulnerable to some significant risks, such as severe weather. However, multi-agency emergency planning, investment in engineering and technological solutions, and the interconnected nature of transport networks all lend resilience to the sector.

DfT has identified six focal risk areas which have the highest impact, or which have the biggest capability gaps. The Department's current priorities include:

- **Security** – including malicious rail incidents. The department engages with industry, cross-government colleagues, the intelligence community, and international partners to put in place effective and proportionate mitigation measures to protect the transport network. See the National Rail Security Programme (NRSP). [Land Transport Security and Security In the Design of Stations (SIDOS)] [Land Transport Security]
- **Incident response** – including rail accidents, collisions, major fires, and failure of the electricity network. The department works with the intelligence community (during terrorism-related events), other departments, local responders, and industry and has well-exercised internal response procedures.
- **Cyber incident**: The department has an active cyber security programme, working closely with industry as well as government and international partners to identify and mitigate cyber risks and vulnerabilities across all transport modes. [Rail Cyber Security Guidance to Industry]
- **Climate change and severe weather**: As part of the 2016 National Flood Resilience Review, the department is working to identify local road networks in England that are at risk of flooding to provide

an assessment of the impact of roads/bridges on communities if they are unavailable. Network Rail is developing route resilience plans to identify areas vulnerable to flooding. [Climate Change Adaptation]

- **Industrial action**: This can cause significant disruption to the travelling public across all the transport sub-sectors. The DfT is working with industry and lead government departments to understanding the risk and mitigate the impact on the public and wider industry. [A consultation on implementing minimum service levels for passenger rail]
- **Severe space weather**: The DfT is engaging with a number of government and industry stakeholders to build awareness and plan for the impacts of space weather on transport control, navigation and communication systems. As part of the resilience work, the DfT has a specific engagement programme with industry on severe space weather resilience; delivers targeted research programmes to provide evidence to support policy development; and maintains collaborative relationships with industry. [UK Severe Space Weather Preparedness Strategy]

It is therefore imperative that the UK rail network is prepared for emergencies such as these. This is reiterated in the UK Resilience Framework, 2022. The Framework is the first articulation of how the UK Government will strategically deliver on resilience; its core principles not only assert the need for a whole of society approach to resilience through transparency and empowerment, but that a developed and shared understanding of the civil contingencies risks we face will galvanise an approach to resilience that prioritises prevention over cure wherever possible. The Framework ultimately poses a greater emphasis on preparation and prevention.

Source: Public Summary of Sector Security and Resilience Plans 2018

3.4 Embedding a Resilience Framework

To embed resilience within the organisation, Rail Entities should consider implementing the ISO22316:2017 standard for organisational resilience. This standard is not specific to any sector but supports the development of several of the provisions set out within this chapter. It seeks to improve an organisation's ability to absorb and adapt in a changing environment, to ensure the organisation can continue to deliver on its objectives, and to survive and prosper. The standard provides guidance for the recognised attributes for organisational resilience and the importance of leadership commitment to enhancing resilience capability.

Further guidance on the implementation of resilience frameworks can be found in Appendix Section 8.2.1 Preparation & Resilience: Case Study #1 – Implementing a Resilience Framework.

3.4.1 Preparation, Resilience & Business Continuity

To prepare for emergencies, Rail Entities should implement a Business Continuity Management System (BCMS) in line with ISO 22301. The purpose of a BCMS is to prepare for, provide and maintain controls and capabilities for managing an organisation's overall ability to continue to operate during emergencies.

Business Continuity (BC) is a key management discipline that builds and improves organisational resilience. Embracing BC reconciles a paradigm shift from mandating and enforcing compliance by embedding BC into the organisation. Embracing and embedding BC is an outcome of preparing for operational disruptions. Embedding BC into business-as-usual (BAU) activities includes allocating roles and responsibilities across an organisation's hierarchy, providing training, scheduling BCM-related activities and confirming adherence to the BC policy.

The BC policy is the key document that sets out the purpose, context, scope, and governance of the BC programme. The BC programme is an ongoing cycle of activities that implements the policy. These activities are carried out by following the BCMS lifecycle:

Figure 5 The BCMS lifecycle (Source: Business Continuity Institute Good Practice Guidelines 2023)

A BCMS will understand the organisation'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 organisation will survive emergencies, while monitoring and reviewing performance and effectiveness of the BCMS, where continual improvement is based on qualitative and quantitative measures.

Further information on Business Continuity Management Systems can be found in RDG-OPS-ACOP-012 IEM, Recovery.

4 Planning for Emergencies

4.1 Overview

Whilst it is preferable to prevent incidents and emergencies entirely, as described in other CoPs comprising the IEM process, it is accepted that this is not always possible. Planning for emergencies is necessary for the rail industry to effectively reduce, control, and mitigate the effects of emergencies throughout the response and recovery phases. This will be covered in further detail within the RDG CoPs for responding to emergencies and recovering from emergencies. This section provides the overview of planning activity within the preparedness stage of activity.

Emergency planning is a cycle of activity, beginning with establishing a risk profile to help determine the priorities for plan development, and ending with review and revision before the whole cycle re-starts again to better prepare and plan for emergencies. Good emergency planning follows a systematic and ongoing process which evolves as lessons are learnt and circumstances change.

Emergency and Business Continuity plans set out an organised, pre-determined and coordinated course of action to be followed in case of several incidents including but not limited to a fire, explosion, flood, accident, or other incident that gives rise to a risk to human health or the environment that a Rail Entity has a duty to prepare for and respond to.

The need for emergency planning in relation to accidents and incidents, and the requirements for development and implementation of emergency plans, are detailed in this Chapter. They primarily arise from The CCA and the Railways (Accident Investigation and Reporting) Regulations (RAIRR), however there are parallel arrangements designed to achieve equivalent standards under legislation such as the Health and Safety at Work Act 1974, Management of Health and Safety at Work Regulations 1999 and the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009.

4.2 Types of plans

Often it is appropriate to have more than one emergency plan. The terminology for these plans is common across industries in the UK and may include:

4.2.1 Generic plans

A generic plan is the plan which will enable response to and recovery from a wide range of possible emergencies. It should include procedures which would be used in all instances for ensuring the safety and welfare of passengers, staff and the public, and protection of assets, property, and the environment. A generic plan can be developed for an area, Rail Entity or industry-wide, depending on how the plan will fit into the current BAU model for the specific Rail Entity.

4.2.2 Specific plans

Specific plans relate either to a particular emergency or kind of emergency, or to a specific site or location. Specific plans incorporate a detailed set of arrangements designed to go beyond the generic arrangements when they are likely to prove insufficient in a particular case. A specific plan usually builds upon a generic plan. Specific plans can also reference specific risks for the organisation that have been highlighted in a risk register. For example, certain Rail Entities will need to plan for high risks that many only apply to certain areas of their operations, e.g., coastal flooding. See section 4.4.1 in Guidance for more information.

Provisions and Accompanying Guidance

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

When reading these Provisions, Rail Entities should note that the CCA states that Category 2 responders are required to cooperate and share information and does ***not*** mandate that Category 1 responder duties apply to Category 2 responders.
However the CCA Enhancement Programme, Chapter 2[28] states that under the duty of cooperation Category 2 responders should look at how delivery of emergency duties can most easily match similar CCA duties of Category 1 responders.

4.3 Provisions

4.3.1 Rail Entities ***SHOULD*** have in place emergency plans which contain information on how they will reduce, control, or mitigate the effects of emergencies. [7, 29, 31]

4.3.2 As part of their emergency planning arrangements, Rail Entities ***COULD*** [10]**:**

- Implement a process of continual improvement.
- Update emergency plans to reflect best practice from within and outside the rail industry.
- Actively seek ways to improve emergency plans.
- Fully involve partner agencies in incident debriefs. [see Chapter 5]
- Update emergency plans to reflect lessons learnt from incidents and exercises. [see Chapter 5]

4.3.3 Rail Entities ***SHOULD*** ensure their emergency plans are updated to reflect risk assessments. [7]

4.3.4 Rail Entities ***COULD*** implement a documented and standardised process to cooperate with relevant Category 1 and other Category 2 responders. [7, 28, 31]

4.3.5 Rail Entities ***MUST*** ensure emergency plans include arrangements to assist the RAIB in their investigations. [30]

4.3.6 Rail Entities ***MUST*** ensure emergency plans include arrangements to provide permitted inspectors access to the incident site and instruction that no evidence shall be removed (except in very limited exceptions and having notified the RAIB). [8]

4.3.7 Rail Entities ***MUST*** ensure emergency plans include arrangements to preserve evidence at the scene. [1]

4.3.8 Rail Entities ***SHOULD*** prepare and update emergency plans which include [27]:

1. A Station Plan
2. A Station Security Plan
3. A Station Incident Response Plan (SIRP)
4. An Evacuation Plan
5. An Operational Continuity Plan (including business continuity plans)

4.3.9 Rail Entities ***COULD*** adopt the working ethos of the Joint Emergency Services Interoperability Principles (JESIP). [27]

4.3.10 The Station Plan ***SHOULD*** state its purpose and scope. [27]

4.3.11 Rail Entities ***MUST*** ensure that the requirements of the National Rail Security Programme are communicated to Station Managers to ensure they are carried out as required. [27]

4.3.12 The content of the SSP ***MUST*** be agreed with the DfT. [27]

4.3.13 The measures specified in the Security Response Level (SRL) tables in the NRSP ***MUST*** be applied to a relevant location in accordance with the current SRL, as notified to the Station Facility Owners (SFOs) or operator in writing by the Secretary of State. [27]

4.3.14 The SIRP ***SHOULD*** be implemented when there is any deviation from BAU. [27]

4.3.15 The SIRP ***SHOULD*** set out tasks and activities to be considered by those managing the incident. [27]

4.3.16 A process ***SHOULD*** be put in place to identify any deviation from the defined BAU baseline, e.g., failure of electricity supply, an unusual degree of overcrowding, emergency incident. This ***SHOULD*** include monitoring to ensure tolerable thresholds are not exceeded and recording where appropriate decisions to implement or not implement the SIRP. [27]

4.3.17 Rail Entities ***SHOULD*** consider funding essential training courses for those responsible for station plans to understand the principles of emergency planning, including plan writing, planning, exercising and validation. [27]

4.3.18 Rail Entities ***SHOULD*** ensure that those who are responsible for updating plans, particularly if new to the role and relatively inexperienced, are supported by, and the resulting plans reviewed, by those with greater skillsets. [27]

4.3.19 In order to facilitate an invacuation or lockdown, Rail Entities ***SHOULD*** seek to identify potential 'safe havens' within the station to which members of the public and/or staff can be directed. [27]

4.3.20 Rail Entities ***SHOULD*** consider whether some of their plans for dealing with specific threats may be restricted. [27]

4.3.21 In addition, Rail Entities ***SHOULD*** ensure their emergency plans include dangerous goods passing through stations. [21]

4.3.22 Rail Entities ***SHOULD*** proactively look outward when planning emergency response to identify and use good practice in a spirit of continuous improvement. [10]

4.3.23 Emergency response arrangements ***SHOULD*** be in place and reflect good practice from both within and outside the rail industry. [10]

4.3.24 Lessons from published reports ***SHOULD*** be included in procedure reviews and incorporated into revised emergency procedures. [10]

4.3.25 Rail Entities ***SHOULD*** actively seek to find and share more effective ways of dealing with emergencies. [10]

4.3.26 Roles and responsibilities ***SHOULD*** be reviewed to ensure they remain in-line with standards in recognised high performing organisations. [11]

4.3.27 Individuals from collaborating Rail Entities ***SHOULD*** recognise and undertake roles and responsibilities allocated during collaborative activities. [11]

4.3.28 Rail Entities ***SHOULD*** identify who within their organisations is authorised to declare a 'Major Incident'. [15]

4.3.29 Rail Entities ***SHOULD*** maintain, review, and regularly update extreme weather plans. [16]

4.3.30 Plans ***SHOULD*** be reviewed and updated regularly. [16,29]

4.3.31 Rail Entities ***SHOULD*** ensure that services & stations that may be affected by extreme weather are well stocked with emergency supplies of water and basic snacks. [16]

4.3.32 Rail Entities ***SHOULD*** ensure supply of vehicles to move emergency supplies to strategic locations as required. [16]

4.3.33 Rail Entities ***SHOULD*** reference RDG-OPS-GN-023 for the checklist for major incident response within the organisation. [18]

4.3.34 Emergency Plans ***SHOULD*** be exercised and reviewed on a regular basis. [29, 31]

4.3.35 Emergency Plans ***SHOULD*** be distributed and controlled for key stakeholders. [29, 31]

4.3.36 Rail Entities ***SHOULD*** organise a programme of exercises at all levels to validate emergency plan content and roles and responsibilities within the plan. [29. 31]

4.3.37 Rail Entities ***SHOULD*** have a crisis management plan. [19]

4.3.38 Rail Entities ***SHOULD*** have arrangements in place to provide humanitarian support to those involved in or affected by major incidents. [26]

4.3.39 The person responsible for emergency planning within a Rail Entity ***SHOULD*** have the ability to develop documented arrangements for all aspects of dealing with emergencies, including but not limited to[19]: -

- arrangements to ensure emergency plans are exercised and reviewed on a regular basis,
- the organisation of an exercise programme at all levels, to validate emergency plan content and specifically roles and responsibilities within the plan,
- arrangements to ensure emergency plans are distributed on a controlled basis to key stakeholders.[19]

4.4 Guidance Notes

Rail Entities should aim to maintain plans which cover the following three areas:

1. Plans for preventing an emergency.
   In some circumstances there will be a short period before an emergency occurs when it might be avoided by prompt or decisive action. These actions may be identified during the initial notification period or as part of dynamic risk assessments and should be considered during the stand-up, notification or activation sections of plans or procedures.

2. Plans for reducing, controlling, or mitigating the effects of an emergency.
   Planning should consider how to minimise the effects of an emergency. This should begin with the impact of the event (passengers, staff, survivors, the public, buildings/facilities, infrastructure, equipment) including the relevant alerting procedures and remedial actions that can be taken to reduce the effects. Recovery plans should also be developed to reduce the effects of the emergency and ensure long term recovery. The National Recovery Guidance provides more detail on recovery issues.

3. Plans for taking other action in connection with an emergency.
   Not all actions to be taken in preparing for an emergency are directly concerned with controlling, reducing, or mitigating its effects. Planning for emergencies should look beyond the immediate response and long-term recovery issues and look also at secondary impacts. For example, emergencies are likely to trigger media attention and public response and plans may need to consider how to handle this increased interest.

Emergency plans should include procedures for defining levels of emergency and determining triggers for when to activate a plan. This should include identifying an appropriately trained person or persons who will take the decision, in consultation with others, on when an emergency has occurred.

The maintenance of plans is also imperative and goes beyond their initial preparation. Once a plan has been written, it must be maintained systematically to ensure it remains up-to-date and fit for purpose.

It may be appropriate that multiple organisations or stakeholders within the rail industry cooperate in developing a joint emergency plan where the partners agree that, for a successful combined response, they need a formal set of procedures governing them all. A good example of this is the Incident Care Team initiative, a key principle of which is that there is full mutual support between Rail Entities, and which therefore requires common structures, procedures, training, documentation, etc.

4.4.1 Types of Plans, Specific Emergency Plans

Specific plans can reference specific risks for the organisation that have been highlighted in a risk register. For example, certain Rail Entities will need to plan for high risks that many only apply to certain areas of their operations, e.g., coastal flooding.

RDG-GN033 Station Incident Response Planning identifies five components which together make up a

comprehensive approach to Planning in the rail industry (Figure 6), they are:

- Station Plan
- Station Security Plan
- Station Incident Response Plan (SIRP)

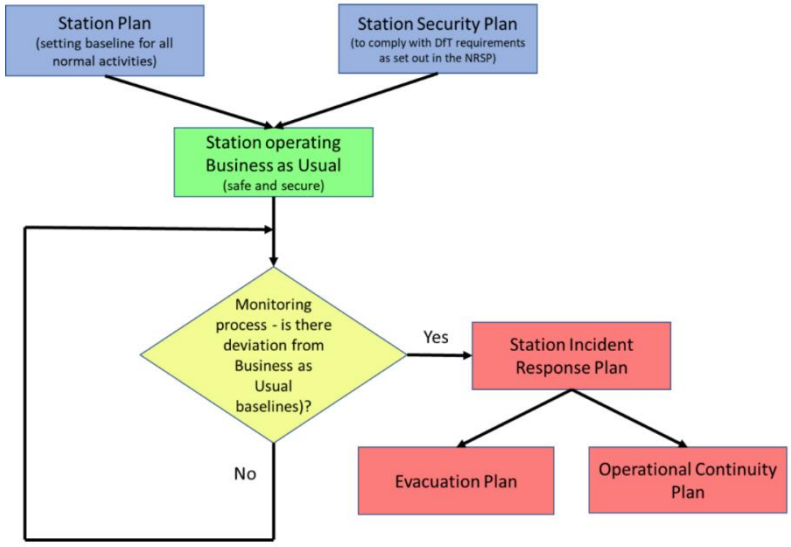

Figure 6 Recommended composition to Station Incident Response Planning (Source: RDG-GN033 Station Incident Response Planning).

There are a number of common processes which support all of the above, these are:

i) Communication [see Chapter 6 Communication │ Multi-Agency Partners].
ii) Training [see Chapter 5 Training & Awareness].
iii) Exercising [see Chapter 5 Testing & Exercising].
iv) Post incident review (see RDG-OPS-ACOP-GN035).

4.4.1.1 Station Plans

The Station Plan (SP) sets out what BAU looks like across all of the activities undertaken. This sets the baseline for the activities and enables the operator to identify any deviations from the state of normality. The range of business activities covered by the SP typically includes:

- Crowd management
- Automated announcements
- Catering outlets.
- Customer information screens / display boards.
- Data links.
- Electricity supply.
- Evacuation.
- Fire alarms and other alerting systems.
- Heating.
- Information points.
- Lighting.
- Phone lines.
- Public address systems announcements.
- Public information messages.
- Retail outlets.
- Security checks.
- Ticket gates.
- Ticket sales.
- Toilets and washing facilities (both public and staff).

- Train dispatch.
- Water supply.
- Others as identified.

The SP identifies the triggers which show that the activity has or is moving away from the state of normality. These triggers are used by the operator to consider whether any response or change in response is required.

4.4.1.2 Station Security Plans

A Station Security Plan (SSP) is required to be produced in order that Rail entities comply with the requirements set by the DfT under the auspices of the NRSP. The SSP is a classified document (Official Sensitive) which means that it cannot be made available to Rail entity staff who do not have Counter Terrorist Check (CTC) clearance. It is issued to:

- National Security Contacts (and deputies).
- Directors with Responsibility for Security.
- Cyber Security Contacts.

In most cases, Station Managers will not have direct access to the NRSP because they will not have the relevant security clearance. Rail Entities are inspected on a regular basis to ensure compliance. Advice as to the content of a SSP can be obtained from the DfT.

The measures outlined in the NRSP apply to Station Facility Owners (SFOs) of those stations in Categories A, B and C (but not D). The list of stations with their categorisation is set out in an Appendix to the NRSP.

Source: RDG-GN033 Station Incident Response Planning

4.4.1.3 Station Incident Response Plans

It is important that sound and cogent contingency plans exist across the rail industry to ensure that proactive action is taken to prevent incidents occurring wherever possible and that, if they do occur, a timely, effective, and professional response is provided.

The purpose of the Station Incident Response Plan (SIRP) is to set out the details of that response – what it is, how it is to be delivered and how and when it is to be activated.

Conceptually the SIRP comprises a number of different components. Guidance Note RDG-GN033 Station Incident Response Planning makes no recommendation as to whether these should be brought together in a single physical plan or maintained as separate documents. However, where two or more plans addressing these various components are in place, it is essential that they are fully aligned with each other and that there are no gaps in their collective coverage.

The SIRP can be used either in whole or in part dependent on the nature and scale of the incident. It is not intended to provide a prescriptive response but be a flexible and scalable plan from which the required elements can be drawn to provide an appropriate response.

The SIRP should be implemented when there is any deviation from BAU. The Plan should set out tasks and activities which might be considered by those managing the incident.

The SIRP is informed by:

i) Variations to the SP based on identifiable risks, e.g., loss of power, industrial action, flooding, overcrowding, terrorist attack, etc.
ii) Identification of the risks and mitigation measures e.g., partial or part closure of the station, bringing in additional staff/security, emergency evacuation, etc.
iii) The threats as set out in the NRSP.

The task of completing a SIRP should not be taken lightly; current practice shows that certain individuals are given the responsibility for completing station plans but few, if any, are qualified in plan writing, planning, exercising or validation. There are no training courses within Network Rail or the wider rail industry that are specifically designed to give those tasked with creating and developing station plans the necessary skills and competencies. Many have experience in completing plans but having a formal understanding of planning principles is considered an essential qualification.

It is suggested that the courses provided by the Emergency Planning College (EPC) be considered as a pre-

requisite to help those responsible for station plans to understand the principles of emergency planning. The EPC currently provides courses for civil protection, plan writing, exercising, and testing, and business continuity management. The Business Continuity Institute also offer similar training courses.

Source: RDG-GN033 Station Incident Response Planning

4.4.1.4 Evacuation, Invacuation and Lockdown Plans

Rail Entities should already have in place a plan to evacuate a station for an actual or suspected fire. The threat/risk assessments identify a range of new circumstances when a full or partial evacuation of the station is required. They should also determine the speed in which the evacuation should take place, i.e., immediate, controlled over a short time frame, controlled over a longer period.

A generic plan (Section 4.2.1) should be sufficient to cover the majority of eventualities identified in the threat/risk assessments. For some of the threats/risks an evacuation might not be necessary. Evacuation should only be used as a viable and appropriate response to a threat/risk.

There may be circumstances when either invacuation or lockdown may be a more appropriate response than evacuation, either for public, staff or both.

Invacuation involves members of the public and/or staff being made aware of an emergency and moved to the most sheltered/protected areas within the station (away from external windows and other exposed areas) Invacuation is typically employed if moving outside would increase the risk, e.g., bomb threat nearby, toxic fumes in the air, etc.

Lockdown involves the securing of external entry points and members of the public and/or staff being instructed to take immediate shelter in a secure location such as a storeroom or office until such time as the all-clear signal has been given. Lockdown is typically invoked in response to a security incident / threat.

Source: RDG-GN033 Station Incident Response Planning

4.4.1.5 Operational Continuity Plans

The time to return to BAU (or a revised BAU) will depend on the nature of the incident/event. For some eventualities the return to normality will be quick but for others it might be days, months and in a few cases even longer (in which case Rail entities should have in place business continuity plans (see Section 3.4.1) which show how services will continue if, for example, a station needs to be rebuilt following a building collapse).

Rail Entities are expected to demonstrate how the business operation (as shown in the SP) will continue after the emergency response and before return to normality. If the event has been significant then BAU might be very difficult to achieve for many days, weeks or even longer.

Examples of where an OCP might be required include the following (the list is not intended to be exhaustive):

- Long term loss of an external supply, e.g., water, electricity, or gas.
- Loss of an external service, e.g., refuse collection, cover by a security company, etc.
- Insufficient staff to continue a safe operation, e.g., following a critical incident in the vicinity of a station, a health emergency which has affected staff, strike, etc.
- Waiting for a response by the emergency services to be completed – this may be to allow for a forensic examination of a scene or check for a suspicious device or behaviour.
- A critical piece of station infrastructure has failed which cannot quickly be repaired or replaced.
- A structural failure has occurred which requires extended remedial work.
- Decontamination is required.

Source: RDG-GN033 Station Incident Response Planning

4.4.2 Plan Contents

To be most effective, Rail Entities should ensure that their emergency plans include information on:

1. The purpose of the plan
   Each plan should have a clear stated purpose, either as a generic plan to cover a range of scenarios, or as a specific plan. This should include how the plan links back to a risk assessment, which identified a need, gap, or required action.

2. How the plan works
   The plan should detail command and control arrangements, facilities, and equipment either available or required, processes for obtaining additional resources as required and how information will be recorded, managed, and disseminated. Clearly defining these procedures and processes will enable effective cooperation and integration with other Category 1 and 2 responders.

3. Roles and Responsibilities
   Key roles and responsibilities relevant to the plan should be identified and listed. Whilst these will vary across the rail industry, they should align with the Gold/Strategic, Silver/Tactical and Bronze/Operational arrangements and JESIP doctrine used by UK responders. [see Chapter 5 of the RDG ACoP: Part A - Governance and Chapter 5 of this document]

4. Plan activation
   Any emergency plan should include procedures for alerting, placing on standby and activating teams, individuals, and external partners (e.g., the emergency services) and other related procedures. This should include a procedure enabling decision-makers to identify what level of emergency has occurred, and to inform others of that decision as appropriate.

5. Checklists
   What needs to be done and by whom? The roles and responsibilities assigned should be matched to specific actions which are targeted towards specific aims. This may be via process diagrams, checklists (see RDG-OPS-GN-023: Checklist for Major Incident Response), or Aide Mémoires (see RDG-OPS-GN-014: Major Incidents – Preparation of Aide Mémoires for Senior Managers). This section should include details of how RAIB requirements will be integrated into the management of an emergency.

6. Communications
   The type of plan will define whether communications procedures, stakeholders and contact lists are included or held within a separate document. A generic plan may only contain generic details, whereas a specific plan may contain far more specific contact details, and therefore require more regular updates to remain relevant. [see Chapter 6]

7. Testing the plan
   To maximise the effectiveness of plans, they should be part of a regular cycle of training, exercising, assessment and feedback. In order to assess or measure a plan, staff must have been trained to use it, this ensures that updates and improvements are reflective of the plan itself and not due to lack of familiarity. [see Chapter 5].

4.4.3 Plan Update Process

Developing and improving emergency plans should be treated as a systematic and continuous process, learning, and implementing lessons from a wide and diverse array of sources including:

1. Incident Debriefing
   Rail Entities should ensure that incidents are thoroughly debriefed; internally, externally with other rail industry partners and also with partner agencies from the wider responder community. This will enable updates to reflect the widest possible range of perspectives and feedback. [see Chapter 5]

2. Exercise Debriefing
   A similar approach should be taken to capture lessons learned from exercises, which are likely to be more frequent than incidents, yet also more limited in scope.

Figure 7 Developing and implementing plans.

3. Use of Best Practice
   As part of actively seeking ways to improve emergency plans, lessons learnt, and examples of best practice should be sought from within the rail industry but also from outside. Examples from the highway sector, nuclear industry, and others with overlapping or aligning challenges have been included within these Codes of Practice. These case studies should be considered as the tip of the iceberg and used as a starting point for further engagement and study.

5 Training & Awareness | Testing & Exercising

5.1 Overview – Training & Awareness

This CoP aims to ensure Rail Entities are fully prepared for all types of emergencies, that they have the required IEM competencies in place and appropriate training and learning opportunities are provided.

Integral to that is the practising and testing of all elements of emergency management. Training staff who are involved in emergency management activities is fundamental to a Rail Entities ability to handle all types of emergencies.

Training is about raising the awareness of key staff regarding the types of emergencies are that they may face, and giving them confidence in their organisation's own procedures, rail industry standards, guidance / CoPs, and multi-agency guidance to carry out their emergency management activities successfully. It is about developing competencies and skill sets so that staff can fulfil key roles.

It is important that all those within an organisation who may be involved in emergency management activities should be appropriately prepared, requiring a clear understanding of roles and responsibilities and how they fit into the internal and external emergency management wider context. All staff will need to feel confident and competent in any role they may take.

Any staff who could be involved in emergency management activities should receive appropriate training. However, training should also extend beyond those employed by the organisation, to the wider rail industry and multi-agency partners also involved in preparedness activities and / or response.

Rail Entities need appropriately trained staff who are capable of conducting risk assessments (see the RDG Anticipate, Assess, Prevent CoP), BCM [Section 3] and emergency planning [Section 4]. These three processes underpin an organisation's preparedness for emergencies, and their ability to respond and recover effectively.

Staff trained in emergency management activities will need to provide leadership and a focus for emergency preparedness to ensure the ongoing processes of risk assessment, BCM and emergency planning are taken seriously at all levels of an organisation. As the central authors of an organisation's emergency arrangements, they will also be looked to for direction if an emergency occurs and plans must be carried out.

The CCA requires Category 1 responders to include provision for the carrying out of exercises and for the training of staff in emergency plans. The same or similar requirements for exercising and training apply to business continuity plans and arrangements to warn, inform, and advise the public. This means that relevant planning documents must contain a statement about the nature and frequency of the training and exercising to be provided. Whilst this requirement is asked of Category 1 responders only, such as the emergency services and local authorities, it is appropriate for Category 2 responders to follow suit, assimilating best practice and providing a seamless fit with regards to multi-agency training and exercising opportunities and requirements.

ResilienceDirect is the Platform generally used by emergency management professionals within the UK for sharing information and to deliver multi-agency training. For more information see Section 5.3.1.

5.1.1 Learning and Training Needs Analysis

A learning needs analysis (LNA) is a clear, systematic and ongoing identification of how learning and development needs relate to performance gaps and is key in ensuring effective learning across an organisation. A training needs analysis (TNA) is a process to identify any gaps between the actual and the desired / required knowledge, skills, and abilities in a role. More on LNA and TNA can be found in Section 5.7.2.

5.1.2 Programme / Awareness Requirements

A rolling training programme should be utilised by organisations and the wider rail industry to account for staff turn-over, and also to ensure all staff are regularly refreshed and practised in emergency management.
More on TNA can be found in Section 5.7.2.

5.1.3 Communications

Communications and the sharing of information are fundamental training components for emergency management activities. Internal processes, equipment, decision making, external processes and application of these within the wider rail industry must be tested individually and as part of a wider exercising programme on a regular basis.

5.2 Overview – Testing & Exercises

5.2.1 Emergency Exercises

The legal requirement for testing organisation's emergency arrangements and multi-agency plans is within the CCA regulations for Category 2 responders; under the requirement to cooperate with Category 1 responders, to provide and share information where relevant / necessary, and to attend / partake within reason, in exercise requests from Category 1 responders. The ORR also stresses the value of tabletop and practical exercises to test plans and communications between staff and responders under the Health and Safety at work Act 1974.

Planning for, attending, and taking part in multi-agency exercises should be undertaken proportionately, reflecting the size, complexity and profile of individual organisations. Coordination of organisations' input to exercises should be in a collaborative manner to meet the aims of all participating partners. There may be a difference in view of what is considered reasonable in varying circumstances and between separate LRFs/ Resilience Partnerships. Prioritisation of the degree of engagement with LRF partners and agencies is essential to maximise the benefits to both sides from participation in exercises.

LRFs and Resilience Partnerships will consider their own needs based on impacts within their own geographical area, however, wider area emergencies are often span a number of LRF areas and as such require an additional layer of coordination. These arrangements are also exercised, but on a far less frequent basis.

Planning for emergencies cannot be considered reliable until it is exercised and has proved to be workable, especially since false confidence may be placed in the integrity of a written plan. An exercise is a simulation of an emergency situation. Exercises are both a type of training, and a distinct type of emergency preparedness. Exercises have 3 main purposes: to validate plans; to develop staff competencies and give them practice in carrying out their roles in emergency plans (training); and to test well-established procedures.

It is important that people taking part in exercises have been appropriately trained beforehand. Participants should have an awareness of their roles and be reasonably comfortable with them, before they are subject to the stresses of an exercise. Exercising tests plans and procedures, not people. An important aim of an exercise should be to make people feel more comfortable in their roles and to build morale.

As an example, it is important that defined roles such as Loggists be trained beforehand. As a minimum, the purpose of the Loggist role is to record all decisions taken/not taken or deferred within the group charged with directing the incident response on behalf of the company. They should understand this responsibility before they can effectively contribute to an exercise in that role.

Further information on Logging and Loggists can be found in RDG-OPS-ACOP-011 IEM, Response.

The UK Government Cabinet Office Emergency Preparedness, Response and Recovery guidance states that there are four main types of exercise:

- Discussion-based
- Tabletop
- Control Post
- Live
- Notification

A fifth category combines elements of the others, referred to as a mixed method exercise. The choice of which one to adopt depends on what the purpose of the exercise is. It is also a question of lead-in time and available resources.

5.2.2 Discussion-based Exercises

Discussion-based exercises are the most cost effective to run and easiest to prepare. They can be used at the policy formulation stage as a 'talk-through' of how to finalise the plan. More often, they are based on a completed plan and are used to develop awareness about the plan through discussion. In this respect, they are often used for training purposes.

5.2.3 Tabletop Exercises

Tabletop exercises are based on simulation, not necessarily literally around a tabletop. Usually, they involve a realistic scenario and a timeline, which may be real time or may speed time up.

Usually, tabletops are run in a single room, or in a series of linked rooms which simulate the divisions between responders who need to communicate and be co-ordinated. The players are expected to know the plan and they are invited to test how the plan works as the scenario unfolds.

This type of exercise is particularly useful for validation purposes, particularly for exploring weaknesses in procedures. Table-top exercises are relatively cost effective, except in the use of staff time. They also require detailed preparation.

5.2.4 Control Post Exercises

In control post exercises team leaders and communications teams from partner organisations are positioned at their control posts (used during an actual incident). This tests communication arrangements and information flow between remotely positioned team leaders. By not involving front line staff these exercises are cost effective and efficient in testing plans, procedures, and key people.

5.2.5 Live Exercises

Live exercises are a live rehearsal for implementing a plan. Such exercises are particularly useful for testing logistics, communications decision making and physical capabilities.

They also make excellent training events from the point of view of experiential learning, helping participants develop confidence in their skills and providing experience of what it would be like to use the plan's procedures in a real event. Where the latter purposes are the main objective of the exercise, then it is essentially a training exercise or practice drill.

Live exercises are often costly and complex to set up and demand the most extensive preparation.

5.2.6 Exercise Programme, Development and Delivery

Section 5.6 covers approaches for testing emergency arrangements and plans, programming, planning, scope, conducting, assessing, debriefing, and reporting.

5.3 Multi-agency, JESIP requirements

JESIP models and principles have become the standard for interoperability in the UK. Amongst the UK emergency planning and response community JESIP is the thread which runs through all plans, response to 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 is on improving the response to major incidents, JESIP is scalable, the principles for joint working and models can be applied to any type of multi-agency incident.

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

Figure 8 The Joint Decision Model (Source: JESIP Joint Doctrine: the interoperability framework)

5.4 Command and Control

Across the rail industry and across multi-agency partners there is the need for command and control during incident management. Each plan or set of emergency arrangements needs to have; a role responsible for development and delivery of the plan and emergency arrangements, a role accountable for the enactment of emergency arrangements, and roles consulted and informed, as identified in the RDG ACoP: Part A - Governance provisions (Page 36).

Training and exercising of staff in their relevant command roles, whether at strategic, tactical, or operational level internally or in a multi-agency setting, is imperative to ensure a coordinated structured response. Section 5.7.5 provides guidance on the command-and-control structure from JESIP recognised across multi-agency responders in the UK.

5.5 Lessons Learned / Review Cycle

The lessons learned from debriefing activities following emergencies, training and exercises are vital to improving the response 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 may be frequently identified, but not successfully acted upon.

A post-incident review or debrief is an evaluation of incident response used to identify and correct gaps, errors, and deficiencies, as well as determine strengths. Immediately after an exercise or incident, it is critical to conduct multi-level post incident reviews or debriefs, gathering conclusions and identifying lessons learned. Emergency practitioners can then incorporate these lessons into emergency arrangements (emergency plans and business continuity plans), highlight any additional training measures, and inject new response measures into exercise scenarios. Actual recovery times for critical processes can be evaluated and mitigations put in place.

It is essential that Rail Entities adopt a robust process that provides a consistent and accountable mechanism to ensure lessons learned are acted upon, to make the transition from lessons identified to lessons learned. Section 5.7.6 provides more on guidance in relation to lessons learned embedment and the JESIP Joint Organisational Learning strategy, an objective for JESIP and key element of the interoperability framework. Further detail on Correct and Preventative Action (CAPA) will be provided in future RDG CoPs for recovery.

Provisions and Accompanying Guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document. The RDG ACoP: Part A - Governance also identifies a number of provisions and guidance notes in relation to roles, responsibilities and competencies**.

5.6 Provisions

5.6.1 Rail Entities ***MUST*** ensure that recommendations of the RAIB are considered and acted upon, where appropriate within emergency planning arrangements.
This requires a person (or organisational body) to whom recommendations made by the Branch are addressed to ensure that these are considered and, where appropriate, acted on. [20]

5.6.2 When designing exercises, relevant responder organisations ***MUST*** be included, and appropriate interoperability and single sector objectives ***SHOULD*** be built into the exercise design. [12]

5.6.3 Rail Entities ***SHOULD*** organise a programme of exercises at all levels to validate emergency plan content and roles and responsibilities within the plan. [19]

5.6.4 Rail Entities ***SHOULD*** include emergency response considerations during the design of enhancements and renewals. [21]

5.6.5 Rail Entities ***SHOULD*** test and exercise their emergency plans. [21]

5.6.6 Rail Entities ***SHOULD*** update emergency plans to reflect lesson learnt from published reports. Use lessons learnt to feed back into the cycle. [10]

5.6.7 Rail Entities ***SHOULD*** use lessons learnt from exercises to feed into a continuous improvement cycle. [10]

5.6.8 Rail Entities ***SHOULD*** use de-briefing sessions that are honest and open, with results disseminated widely. [10]

5.6.9 Rail Entities ***SHOULD*** partake in joint emergency response exercises. [10]

5.6.10 Rail Entities ***SHOULD*** deliver training courses, which are aligned to the JESIP learning outcomes framework and have multi-agency attendance in order to build and maintain an interoperable response. [12]

5.6.11 Rail Entities ***SHOULD*** ensure relevant responder organisations are included when designing Rail sector exercises, and appropriate interoperability and single sector objectives should be built into the exercise design. [12]

5.6.12 Rail Entities ***SHOULD*** where possible attend and contribute to LRF / LRP Training and Exercising working groups. [12]

5.6.13 Rail Entities ***SHOULD*** ensure their personnel, who are required to support the response to an incident, are appropriately prepared and aware of the JESIP models and principles, and how they are applied. To support this, everyone should receive a form of JESIP awareness training annually. In addition, individuals who are responsible for managing an incident at any level, should attend a multiagency JESIP training course, every three years as a minimum. [12]

5.6.14 Rail Entities ***SHOULD*** consider the inclusion of military participants in the planning and delivery of exercises where appropriate. [12]

5.6.15 Rail Entities ***COULD*** consider utilising Joint Organisational Learning (JOL) Online. Uploading all lessons identified from exercises, which affect a multi-agency response, and implementing lessons identified on JOL at the planning stage of the review cycle. Rail Entities ***SHOULD*** implement change at the local level, to reduce the risk of the lessons identified at exercises reoccurring during the response to an incident. [12]

5.6.16 Rail Entities ***SHOULD*** ensure the right people are always in the right place at the right time and there should be inbuilt resilience with some employees competent in both current and next roles. [13]

5.6.17 The organisation ***SHOULD*** use employee involvement to gather ideas for improvement and should put them into practice. [13]

5.6.18 The CMS ***SHOULD*** clearly consider operational competencies related to safety-critical work, referencing relevant legislation where necessary (e.g., ROGS). [13]

5.6.19 There ***SHOULD*** be a clear and well-defined link between the CMS and the need to maintain necessary organisational capability. [13]

5.6.20 Those who might be called on (as a Strategic Commander) to lead the response to Major Incidents on behalf of their organisations ***SHOULD*** be given appropriate training – both initial and on-going – for their role. [15]

5.6.21 Rail Entities Strategic Commanders ***SHOULD*** also be subject to periodic assessments of their continuing competence for the role, undertaken by an appropriate agency. [15]

5.6.22 Rail Entities ***SHOULD*** train, exercise, test and assess competency of Train Operator Liaison Officers (TOLOs) for recertification every 3 years. [17]

5.6.23 Rail Entities ***SHOULD*** maintain and enhance competency through participation in tabletop and live emergency exercises and maintain an exercise logbook. [17]

5.6.24 Rail Entities ***SHOULD*** determine who participates in exercises. [19]

5.6.25 Rail Entities ***SHOULD*** make arrangements for personnel to participate in exercises (internal and external). [19]

5.6.26 Rail Entities ***SHOULD*** capture issues arising from exercises. [19]

****The RDG ACoP: Part A - Governance identifies a number of provisions and guidance notes in relation to roles, responsibilities and competencies, that need to be considered in training plans, provisions include:**

Rail Entities individually ***SHOULD*** make clear statements of IEM roles, responsibilities, and communication both within their organisation and with external stakeholders. This should encompass those providing strategic direction to the organisation, full-time IEM professionals and those that have IEM responsibilities placed upon them as part of their BAU duties.

Rail Entities ***SHOULD*** have a clear, comprehensive, and robust competency framework aligned to, and supporting, the agreed roles and responsibilities assigned to its staff.

Rail Entities ***SHOULD*** have a clear process for managing this competency framework that integrates with organisational roles and responsibilities and enables individual performance management.

Rail Entities ***SHOULD*** adopt the Three Line of Assurance (3LoA) model for assurance and compliance activity related to IEM. This model provides increasingly independent scrutiny and assurance of (IEM) activities, from within the business unit right through to independent internal audit capability and assessment by a regulator or independent third-party assessor.

The relevant governing body, or responsible individuals, ***SHOULD*** provide effective oversight on the assurance model. This includes delegating authority to relevant individuals or governing bodies, responsible for conducting assurance at each level, and scrutinising the relevant reporting lines. Individuals tasked with assurance responsibilities should have the required competency, training, and resourcing to conduct such activities.

Where a Rail Entity conducts a regular, organisation-wide self-assessment/assurance process then IEM activity ***SHOULD*** be included in this. Any self-assessment assurance ***SHOULD*** adopt the following good practice:

- The role responsible for defining the organisation's IEM policy (hereafter Policy Owner) should be engaged to develop/set the wording of any self-assessment questions with guidance from the individual/team conducting the self-assessment process:
- When conducting self-assessment assurance, the IEM Policy Owner should be entitled to request that evidence be submitted to support any self-assessment by a part of the organisation.
- The overall process should allow sufficient time for those assessed to provide suitable and sufficient evidence and for the Policy Owner to evaluate any evidence provided.
- The assurance process should be collaborative with the Policy Owner engaging with those under assessment to enable the provision of best evidence to support accurate self-assessment.
- The Policy Owner should formally record their overall assessment and supporting reasoning/evidence, and this should be reported to the organisations strategic/senior leaders as part of the overall self-assurance activity.

Tactical leaders are responsible for determining how they should deliver senior leaders' strategy. They ***SHOULD*** develop the plans that set out the broad methods that will be employed to meet IEM objectives (e.g., a plan for a multi-year testing & exercising programme). The plans ***SHOULD*** enable operational leaders to manage the activities of frontline staff following their standard procedures/processes.

Rail Entities ***SHOULD*** collate roles and IEM activities into a clear matrix, or matrices. The matrix links together the different roles (whether full or part-time) with the IEM activities. Each activity should be assigned to one or more roles, and each role should be assigned one or more of:

- **Responsible**: Responsible designates the task as assigned directly to this person (or group of people). The responsible person/group is the one who does the work to complete the task. Every task should have at least one responsible person.
- **Accountable**: The accountable person in the RACI equation delegates and reviews the IEM activity involved. Their job is to make sure the responsible person/team knows the requirements for the activity and completes work on time. Every task should have only one accountable person and no more.
- **Consulted**: Consulted people provide input and feedback on the work being done as part of an IEM activity. They have a stake in the outcomes of an activity because it could affect their current or future work.
- **Informed**: Those listed as 'Informed' are individuals or groups that need to be aware of the progress of an IEM activity but not consulted or overwhelmed with the details of every task. They need to know what's going on because it could affect their work, but they're not decision makers in the process.
- Additionally, a '**Decider'** category may be added into the matrix (forms a DARCI matrix). The Decider is the individual or group that holds the ultimate approval or veto over an IEM activity.

A job role's IEM responsibilities ***SHOULD*** be supported by clear knowledge and experience requirements expected of the role holder. These ***SHOULD*** include experience of various elements of IEM activity or suitable qualifications that demonstrate expertise. Collectively this enables visibility and clarity of responsibilities and accountabilities, and suitable objective setting and individual performance management.

The Rail Industry IEM competency framework ***SHOULD*** describe how competency is managed, including:

- A process for assessing the competence (learning, expertise, experience) requirements for any given role.
- Identifying the initial training and continual professional development requirements pertinent to the role.
- Identifying the different levels of competency and how to progress through them.
- A process for assessment of IEM role competence.

The process should conform to the ORR Rail Safety Publication 1 2016 – Developing and maintaining staff competence.

5.7 Guidance Notes

5.7.1 Training

The following guidance relates to the provisions for Rail Entities to train staff in emergency management and meet appropriate competencies, ensuring the right people, at the right level, are in the right place at the right time, and that there is inbuilt resilience with employees competent in emergency management roles.

Regulation 13 of the Management of Health and Safety at Work Regulations 1999 (MHSWR) requires

consideration of people's capabilities as regards H&S when appointing them. Regulation 24 of The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) requires companies to have a system in place for ensuring that staff who carry out safety-critical work are competent and fit to do so.

RM[3] states that organisations should be capable of managing health and safety (H&S) effectively by having sufficient employees (including volunteers) with the appropriate competences at all levels. Therefore, an organisation needs to maintain an adequate organisational capability for H&S, including:

- Having the right number of people, in the right place, at the right time with the right competence.
- Ensuring recruitment, training and development systems are able to anticipate and cater for retirements and resignations, especially when there is an ageing workforce and / or a potential skills shortage, and;
- Understanding the minimum human resource needs to maintain safe operation and particularly to ensure effective risk control during times of organisational change.

A Competence Management System (CMS) should secure the competence of all those who have roles, responsibilities, authority, and accountabilities, within the organisation's health and safety management system (SMS), at all levels of the organisation. This includes directors, senior, middle, and junior managers, supervisors and front-line workers and volunteers.

5.7.2 Learning and Training Needs Analysis

5.7.2.1 Learning Needs Analysis

The need for organisational agility means learning and development professionals need to constantly align to their organisation's performance needs, the following provides methods that can be used to identify learning and development needs.

Identifying learning and development needs starts with knowing the organisation's current and future capability needs, and then assessing existing levels of skills, attitudes, and knowledge. This assessment can use formal and informal methods and will allow decisions about what learning is required at an individual, team, or organisational level. These gaps should be interpreted and prioritised within the wider organisational strategy.

Implementing an ongoing Learning Needs Analysis (LNA) is different to a TNA; a TNA is a one-off isolated event looking at the needs for a specific training activity. An LNA may be seen as a current or future health check on the skills, talent, and capabilities of the organisation (or part of the organisation) and is carried out with multiple stakeholders. It's based on the ongoing systematic gathering of data and insights about employees' capabilities and organisational demands for skills, alongside an analysis of the implications of new and changed roles for capability.

The LNA process needs to flow from business strategy. Its aim is to produce a plan to make sure there is sufficient capability to sustain current and future business performance. It's also vital to consider statutory and compliance requirements.

Preparing for an LNA includes engaging with a variety of stakeholders, including subject matter experts, operational managers, and the impacted employees. Analysis of learning and development needs can be undertaken for:

- The whole organisation
- A specific department, project or workstream
- Individuals

Any need analyses carried out at any of these three levels must be viewed holistically and not seen in isolation. If learning and development activities are aligned to the organisational strategy, then needs analysis will be an iterative process, with learning and development teams working regularly with stakeholders. This will allow for learning and development to gain deeper organisational insight in meeting the internal and external demands.

The 'RAM' approach
While it's critical that any assessment of learning needs is thorough, such a process also needs to be agile and responsive. The Chartered Institute of Personnel and Development (CIPD) developed an approach to learning known as RAM (Relevance, Alignment, Measurement). It covers the need for:

- **Relevance**: How existing or planned learning provision will meet new opportunities and challenges for

the business.
- **Alignment**: If the learning and development strategy takes an integrated blended approach, it's critical for learning and development practitioners to work with stakeholders about what their performance needs are and how to achieve them. Aligning with broader organisational strategy gives focus, purpose, and relevance to learning and development.
- **Measurement**: Learning and development effectively and consistently measure the impact, engagement, and transfer of learning as part of the evaluation process.

Capability analysis
Knowing the current performance standards, as well as those expected in future, is the first step when reviewing skills needs. In preparing for analysis, the following questions should be considered**:**
- Which capabilities will be required to carry out the roles (the person specification)?
- Which capabilities already exist in the workforce (a formal or informal skills analysis)?
- What are the gaps between existing capabilities and new/future requirements (the learning specification)?

Competency frameworks can provide more detailed structures for looking at job requirements.

Gathering data on learning needs
After planning the frequency, extent and nature of the analysis, the next stage is to decide how the information can be collected. Potential methods include:

- Organisational data and intelligence – 'mining' the existing data that's collated in the organisation is a great start point.
- Formal interviews and/or focus groups with stakeholders - these will often be primary sources of information on plans, work organisation and changes.
- Informal conversations with stakeholders – 'coffee chats' are a good source of finding out what is needed.
- Team meetings - attending team meetings across the organisation can give insights on performance needs.
- Observations – engaging with the learners' current 'real world'.
- Questionnaire-based or other surveys of managers, employees, and their representatives. However, it's vital that time is spent considering the questions that are asked, the likely response and what is done with the responses.
- Existing data - for example from management information systems or virtual learning environments/learning management systems. Information and analysis from competency frameworks.
- Performance management data.
- Documentation – for example organisation wide business plans, objectives and work standards, job descriptions and person specifications. This tends to be desk based and will support other methods.

A combination of these methods will give better results.

Much of the data will be sensitive, particularly where individuals' knowledge and skills gaps are exposed, as such confidentiality must be respected. There may also be times when major change is planned that senior management wish to uphold confidential. In these situations, learning and development professionals may need to build relationships and work with managers to demonstrate how learning and development can contribute to the success of an initiative.

Using the learning needs analysis results
Collating the information from the needs analysis will allow a number of outputs that can run concurrently:

- **A report of overall learning needs for the organisation or department** - to form the basis of a learning and development strategy or input to business planning processes.
- **Prioritising the identified performance gaps** - that is, where the gaps are most critical. Concentrating on results required for the learning outcomes is important.
- **Learning and development plans** - Once priorities and budgets are identified, the learning and development team will be able to set plans for learning solutions, prioritising appropriate ways to meet the needs identified. Line managers will also have a clear idea of where they need to coach or develop skills in their teams.
- **Personal development plans** - Aligned with the resources available.
- **Is a formal intervention needed?**

Source: The Chartered Institute of Personnel and Development (CIPD) Learning Needs Analysis 2023

5.7.2.2 Training Needs Analysis

The purpose of a TNA is not only to identify any gaps in knowledge and skills but to bridge those gaps in order to achieve optimal performance. TNA also uncovers the reasons for any gaps and helps determine the relevant approaches to removing them.

TNA helps to align training with business goals and, in the case of this CoP, with the IEM Preparedness elements, to ensure that Rail Entities are investing in the appropriate training. Identifying the short and long-term objectives for each Rail Entity and the skills needed to achieve these will help each Rail Entities' respective learning and development professional to identify the scope of their training programmes.

A TNA helps to uncover skills and performance gaps early on, allowing resolution before gaps become an issue, it will also help an organisation to determine prioritisation of training. Prioritisation needs to be carried out with respect to time and budget. By planning and targeting training, organisations can create training plans that target exactly the skills and knowledge identified as missing, so that resources are invested properly. A TNA facilitates customisation of a training programme based on employees' needs.

How to Conduct a Training Needs Analysis
Training needs analysis best practice:

1. **Start with the desired outcome**. Identify which activities lead to these organisational outcomes before identifying training activities. This outcome can be an organisational or departmental goal. Or it could be an individuals' particular skills or knowledge which needs improving.
2. **Manage expectations**. Training and training need analysis requires advanced stakeholder management. Stakeholders include employees, service users (or customers), educational providers who design and deliver the program, and internal sponsors who pay for the educational event. Ensuring that the training satisfies all groups is crucial for its success.
3. **Use an integrated approach**. Research shows that training programs that place new skills in a broader job or organisational perspective and integrate them with other organisational processes and activities are more successful. This does not mean that you cannot focus your training on something specific, but you must place what people learn into an organisational perspective.

5.7.2.3 Best Practice Training Models

Best practice models for training can be used, a Systematic Approach to Training (SAT) is based on recognised education and training management systems that integrate auditable and competency-based processes with wider learning. At the core of SAT is the cyclical process that supports the delivery of the right training, at the right time within a continuous improvement and evaluation process. A SAT training programme consists of management and administration and instructional design to ensure quality of instruction and the programme.

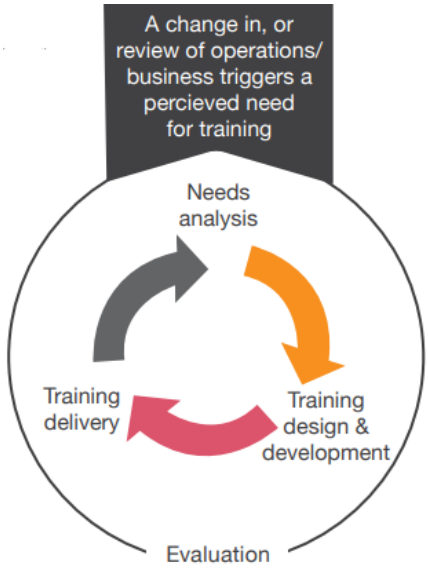

Figure 9 Systemic Approach to Training (SAT) Model

An ADDIE model comprises five phases and provides a structured, systematic approach to create a training program:

Analysis - the first phase of creating a training programme. Four questions need to be answered; Why, What needs to be trained, How do we measure it, and Who gets trained?

Design - the second phase of creating a training programme, this is the stage of planning where details start coming together that will be developed into training materials and a training programme. What format is tp be used and a methodology and strategy for training delivery are considered here.

Development - development of the course and materials is the third phase, this includes development of a participant guide, facilitator guide and job aids.

Implementation - this phase happens when training is delivered.

Evaluation - is the last phase in the creation of a training programme. By reviewing the metrics and adjusting the programme as appropriate based on the feedback and measurement of learning.

Source: Western Electricity Coordinating Council (WECC) Systematic Approach to Training

5.7.3 Training and Awareness Programme

A rolling training programme should be utilised by individual Rail Entities and the wider rail industry to account for staff turn-over, and to ensure all staff are regularly refreshed and practised in emergency management.

Training should include:

- The contents of the emergency and business continuity plans, as well as other emergency management arrangements. How are the plans invoked? What are the key decision-making processes? Who else needs to be involved?
- The individual's role in implementing the plan - what is expected of them? How do they fit into the wider picture?
- Key skills and knowledge required in crisis response.

Training and awareness programmes may include:

- User guides
- Reminder placards
- Conference participation
- Certification and examination preparation

- Skill-based training
- Strategy documentation
- Plan documentation
- First aid performance
- Call tree execution
- Drills / walkthroughs
- Crisis communication execution

Nationally there are a number of emergency management training pathways, implementation of the UK Resilience Framework (December 2022) provided updates to programmes and training platforms as follows:

- The UK Resilience Academy (UKRA) will be core to the 'whole of society' approach, ensuring that all those who work on resilience have the capability and knowledge they need to play their part. This includes government departments and arm's length bodies (ALBs), LRFs and partnerships, emergency responders, the voluntary and community sector, Critical National Infrastructure (CNI), businesses, as well as tools for households and individuals. In line with the Framework's commitment to establish the UKRA by 2025, the government is undertaking a stakeholder roadshow to test seven proposed pillars for the UKRA: emergency planning, crisis management, exercising, personal resilience, strategic prevention, organisational resilience, and citizen preparedness - with a wide range of groups across the country.
- The government launched its Crisis Management Excellence Programme (CMEP) in May 2023 to professionalise crisis management in government through a combination of formal training, informal knowledge sharing, exercising, and a cross-government community of like-minded professionals. This is a long-term programme of upskilling, challenging, collaborating, and growing across the community, to achieve world-leading crisis management and real culture change.
- A UK Resilience Learning Needs Analysis was launched in October 2023 to capture the resilience learning and leadership requirements from the resilience community, including government departments, devolved administrations, LRFs, the CNI sectors, and the voluntary and community sector.
- The Emergency Planning College is developing good practice guidance for exercising and managing lessons from incidents and exercises, to sit alongside the current learning offer and guidance.

5.7.4 Communications in Training

All staff utilising communications systems, or in receipt of communications during an incident must be trained appropriately on a regular basis. For example, Train Operating Companies (TOC) are responsible for running trains and leasing trains from a rolling stock, they operate most of the network's stations, leasing buildings and land from infrastructure managers and owners. Railway stations are owned by the network operator; however, most are leased to the TOC as the main user of that station. Owner and infrastructure management organisations (such as Network Rail), retain the operation of main passenger terminals and are responsible for managing the rail infrastructure. Therefore, the role of TOCs in an emergency may be to assist and support owner and infrastructure manager, who may have overall responsibility for managing the emergency. As such training, and particularly training in communications procedures, will have very different requirements depending on the Rail Entities involved, where the incident has occurred, who (organisation wise) has activated the emergency arrangements, and if the incident escalates to a multi-agency major incident. More information on communications can be found in Section 6.

5.7.5 Exercise Programme, Development and Delivery

The following guidance relates to the provisions whereby Rail Entities should test and exercise their emergency plans.

In planning for exercises, as with training, a rolling programme should be utilised by organisations and the wider rail industry, covering themes recommended by the regulator, based on the national risk profile, strategic objectives within Rail Entities and the wider rail industry, multi-agency forum objectives, and syncing with plan review cycles and system test requirements, as well as incorporating lessons learned from previous exercises.

Regional and local resilience forums such as RRP, LRP and LRFs are not legal entities and do not have powers to direct members, however the CCA and regulations provide that responders / partners through the forums have a collective responsibility to prepare in a multi-agency environment. Duties under the CCA rest with responders but can be exercised through LRFs and other forums. As such LRFs hold local and regional exercise programmes.

Rail Entities should ensure their own organisations' exercise programmes are shared with local / regional forums and endeavour to coordinate with local / regional forums exercise programmes, participating where requested and where beneficial. Local and regional multi-agency forums major incident exercises will test the functioning of Strategic Coordination Centres, Tactical Coordination Centres, Rendezvous Points, and Control rooms and in some cases national operations centres.

By ensuring coordination with external exercise programmes and participation in wider multi-agency exercises Rail Entities will provide training opportunities to internal decision makers and awareness of rail roles and rail emergency arrangements across multi-agency partners.

Plans covering emergency arrangements should be exercised following a programme based on plan review cycles. All constituent parts of a plan should be tested before the review cycle is up. However, time and resources may indicate whether a full exercise or modular approach is best. A full exercise is where all aspects of emergency arrangements are demonstrated in a single event, normally one day. Modular exercises are when elements of a full exercise are demonstrated over a period of time within the review cycle, taking account of other exercises. Considerations when deciding at planning stage whether a full or modular exercise should be undertaken include:

- Legal requirements
- Last use of control/ operations centres and /or specific equipment being tested,
- Requirements of local and national organisations
- Review of other exercises or live activation of arrangements that have been tested which would directly support the emergency/ business continuity plan.

Periodically the test should include implementation of emergency arrangements beyond the Rail Entities emergency planning area. Exercise dates should be agreed with all partners and take account of:

- Dates of previous exercises
- Availability of the Strategic Coordination Centres / Control Centres
- Availability of organisations that contribute to testing of the issued plan and
- Potential clashes with other local or national exercises.

In testing a Rail Entity's emergency arrangements, suitably qualified and experienced role holders should undertake planning of the exercise. Making provision for meetings with representatives who contribute to the plan and who wish to participate (forming the exercise planning group). If necessary, there may be the need for specialist sub-groups to assist in the development of relevant details of the exercises, for example a technical scenario, media briefing inputs and communications specific tests should be considered.

Exercise Directors (the role responsible for the emergency plan, which is being tested, or the role holder responsible for emergency preparedness) manage the formulation, implementation and execution of the arrangements and provide a focus for consultation with other parties. The Exercise Director chairs all planning group meetings to agree overall planning arrangements, objectives, scope, and format. Each function within the emergency arrangements being tested should be present or have input at exercise planning stage, to speak authoritatively on behalf of a function, system or role and put forward the intended contribution, objectives, and view on the format of the exercise. The exercise planning group will develop a scenario and master events list, setting out a list of events that will take place through live play and injects. Details of the exercise operational order or exercise plan should be provided to all participating parties at least a fortnight prior to the exercise date.

The objective of the exercise programme is to ensure all relevant parts of the plan are tested. However, this cannot always be achieved in one exercise. Exercise planners can use a matrix for an overall framework with a list of elements that will need to be tested in order to demonstrate effectiveness of the plan. The matrix should provide an overall framework to use when planning exercises and should not be considered as exhaustive. Additional requirements may arise due to operational changes, experience from exercises, real events, or regulatory issues. Organisations may wish to use the exercise matrix to provide an auditable and transparent process to confirm the relevant elements of their plan have been tested.

Exercises should attempt to demonstrate the following key activities:

- Notification
- Setting up of facilities
- Supply of information

- Interpretation of information
- Interfaces and exchanges/team-working
- Decision making
- Communications & public information
- Facilities and equipment
- Competence of participants

Ordinarily an Exercise Control is established, made up of subject matter experts responsible for inputting injects to replicate activities that would be part of a response to a real emergency. Umpires drive the exercise by providing input to the responders by painting a picture of what can be seen, or by providing information directly into the exercise to maintain the response. Some organisations combine the role of the Assessor and Umpire.

Exercise assessment should be agreed at the objective setting stage by the planning group. Assessors will provide key observations to the post exercise "hot debrief" and a more detailed response ahead of the "cold debrief" for inclusion in the exercise report. Key areas for assessors to consider include:

- Completeness, consistency and accuracy of the emergency plan and other documentation used by organisations responding to an emergency.
- Adequacy of the equipment and facilities and their operability, especially under emergency conditions.
- Competence of staff to carry out the duties identified for them in the emergency plan, and their use of the equipment and facilities.

A full exercise hot debrief should be held immediately after the exercise has finished, allowing participants attending to give their initial assessment of the exercise and identify any immediate issues that have arisen. A cold debrief, held after the exercise, reviews comments, actions and areas for improvement in a draft of the exercise report. The meeting should identify each issue as falling in to one of the categories:

- Issues for which local resolution is appropriate, and
- Issues of a generic nature for which resolution at a high level is appropriate.

These issues should be translated into actions and once accepted by the appropriate responsible person, should be cleared as soon as possible.

5.7.6 Multi-agency: JESIP requirements

A number of provisions state that Rail Entities should include, keep informed, cooperate and work together with multi-agency partners in preparation for emergencies. This section provides more guidance on multi-agency and JESIP requirements and working.

JESIP developed a number of training products to help responder organisations embed the interoperability principles, ensuring the Joint Doctrine continues to be delivered consistently. These include:

- JESIP Multi-agency Interoperability Training Course – a combined one-day facilitated course for Control Room staff and Commanders. The up-to-date materials for this course will be provided through ResilienceDirect™ (see Section 6.4.5) and will only be available to JESIP Trainers who have attended an approved *Train the Trainer Workshop*.
  - The Training and Trainer Specification provides guidance on how this course should be delivered and rolled out regionally/locally.
  - The Learning Outcomes Framework provides direction on the learning outcomes that the course should deliver for different roles.
  - There have been a number of nationally coordinated *Train the Trainer Workshops*. Those who have attended this are welcome to deliver their own *Train the Trainer Workshops* regionally/locally using the resources available on ResilienceDirect™ (see Section 5.7.6.1), to suitably experienced trainers, in accordance with the Training and Trainer Specification. *Train the Trainer Workshops* have been advertised via the JESIP Strategic and Training Leads.

- Awareness products – these can be used stand-alone or incorporated into wider JESIP training courses and/or as refresher material:
  - JESIP awareness presentation – a short presentation to enable awareness of JESIP to be delivered to all staff [coming soon]
  - E-learning – an e-learning package to improve awareness across all responder organisations.
  - Films – a number of animated films to highlight key elements of JESIP, specifically including

the use of M/ETHANE.
- Mobile application – an interactive aide memoire to ensure responders always have key JESIP information at their fingertips.

5.7.6.1 ResilienceDirect™

ResilienceDirect™ is an online private 'network' which enables civil protection practitioners to work together across geographical and organisational boundaries, during the preparation, response and recovery phases of an event or emergency.

The CCA requires that emergency responders cooperate and share information in order to efficiently and effectively prepare for and respond to emergencies and ensure that action is coordinated. ResilienceDirect™ helps organisations fulfil these duties by supporting the adoption of common working practices and ensuring that key information is readily and consistently available to users.

ResilienceDirect™ helps to facilitate multi-agency collaboration in many ways. Activities include:

i) Sharing emergency plans among LRF members and others such as national/sub-national partner organisations and neighbouring LRFs.
ii) Maintaining awareness of forthcoming exercises, events, and meetings, and accessing related documentation such as agendas and minutes.
iii) Sharing situation reports and briefings between local responders, to enable integrated management of events and consistent provision of information to the public.
iv) Communicating situation reports to lead government departments and/or the Cabinet Office Briefing Rooms (COBR), facilitating national coordination/action in response to an incident if necessary.
v) Gathering and reviewing comments on new policies or plans before publication and collating lessons learned following events.
vi) Managing contact information to ensure a single, up-to-date version of distribution lists.
vii) Issuing news and guidance from central government to local responders via the Resilience Gateway.

Those responsible for emergency planning should be aware of the existence and purpose of ResilienceDirect™ and consider subscribing to it.

Source: RDG Guidance Note: Emergency Planning - Knowledge, Understanding and Responsibilities (RDG-GN011)

5.7.7 Command and Control

Further guidance provided here relates to those provisions on competence of staff, and training and exercising of responder roles, including decision makers (strategic commanders).

Command, Control and Co-ordination are important concepts in the individual organisations and the multi-agency response to emergencies. There are single agency command and control structures (often termed Gold, Silver and Bronze) and the multi-agency co-ordination structures that may be convened at Strategic, Tactical and Operational levels (Figure 10).

Although Category 2 organisations are less likely to be involved in the heart of planning work, they will be heavily involved in incidents that effect their own sector. Therefore, JESIP multi-agency working advises Commanders should seek to include representatives from other responder agencies when planning for response. This includes multi-agency Strategic, Tactical and Operational training.

Training within organisations (and multi-agency training) can and should cover all three levels of Command and Control working together, decision makers at strategic, tactical, and operational levels. However other training is necessary that is specific to each level. For example, on the ground live training for operational staff, utilising equipment and communications systems, versus 'slow-time' talk through scenarios or media training for strategic staff.

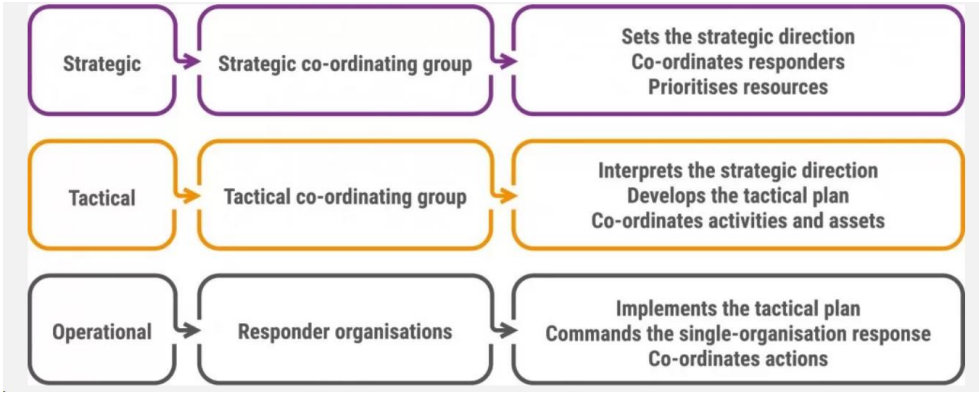

Figure 10 Command and control structure (Source: JESIP Joint Doctrine Edition Three)

5.7.8 Lessons Learned / Review Cycle

A number of provisions reiterate the requirement for Rail Entities to consider lessons learned from training events, exercises and emergencies to feed into a continuous improvement cycle.

Every event, whether a planned exercise or an actual emergency incident, has lessons that can be learned to improve the outcome of the next response. Emergency practitioners should not misrepresent failures or miscommunications but draw from the emergency response to improve preparedness.

Immediately after an exercise or incident, it is critical to conduct multi-level post incident reviews or debriefs, gathering conclusions and identifying lessons learned. Emergency managers can then incorporate these lessons into emergency arrangements, highlight any additional training measures, and inject new response measures into exercise scenarios. Actual recovery times for critical processes can be evaluated and mitigations put in place.

The post-incident debrief and review is an evaluation of incident response used to identify and correct gaps, errors, and deficiencies, as well as determine strengths. Timing is critical, an effective review requires that response and preparedness discussions take place while an incident or exercise is fresh in the minds of decision makers, responders, regulators, and the public. From this review, incident response lessons learned can be identified and preparedness improvement work can begin.

The post-incident review process is intended to identify which response procedures, equipment, and techniques were effective or ineffective, and the reasons why. Post-incident review checklists should include, at a minimum:

- Name and duties of personnel being debriefed
- Date, time, and location during incident
- Specific actions performed
- Responder’s view of the positive aspects of the response and areas for improvements
- Recovery time and possible mitigation measures for improvement
- Potential lessons learned
- Necessary programme and plan revisions
- Effectiveness of equipment used
- Overall post-incident perception and implications

Key areas of consideration that should be analysed by a review team can include, at a minimum:

- Mobilisation procedures for personnel and equipment
- Implementation plans and procedures
- Internal and external communications
- Management and coordination of emergency response
- Stakeholder reaction
- The short- and long-term consequences of the incident

Simplified, a template to facilitate the review process can be:

- What happened?

- Why did it happen?
- What worked well?
- What didn’t work well?
- What can we do to improve it?
- What can we do to confirm learning has been embedded?

Emergency response shortfalls can come from a variety of areas or functions. Applying incident response lessons learned to a crisis management or emergency response programme allows procedures to align with proven and realistic scenarios. Utilising this information provides those working in emergency preparedness the means of improving applicable programmes to better prepare for future situations.

Expanding lessons learned to cover Lessons identified, Lessons applied, Lessons learned and Lessons Embedded is addressed further in RDG-OPS-ACOP-012 IEM, Recovery. Within the UK Joint Organisational Learning (JOL) is the standard for multi-agency learning within JESIP and is adopted by all responder organisations to ensure interoperability is continually improved (Figure 11).

JOL Online is hosted on ResilienceDirect™, a Cabinet Office secure system at official-sensitive in line with government security classifications and is the national repository for interoperability, national resilience lessons and notable practice across the UK.

Access to JOL Online is accessible to all Category 1 and 2 responders as well as many additional sponsored responder organisations.

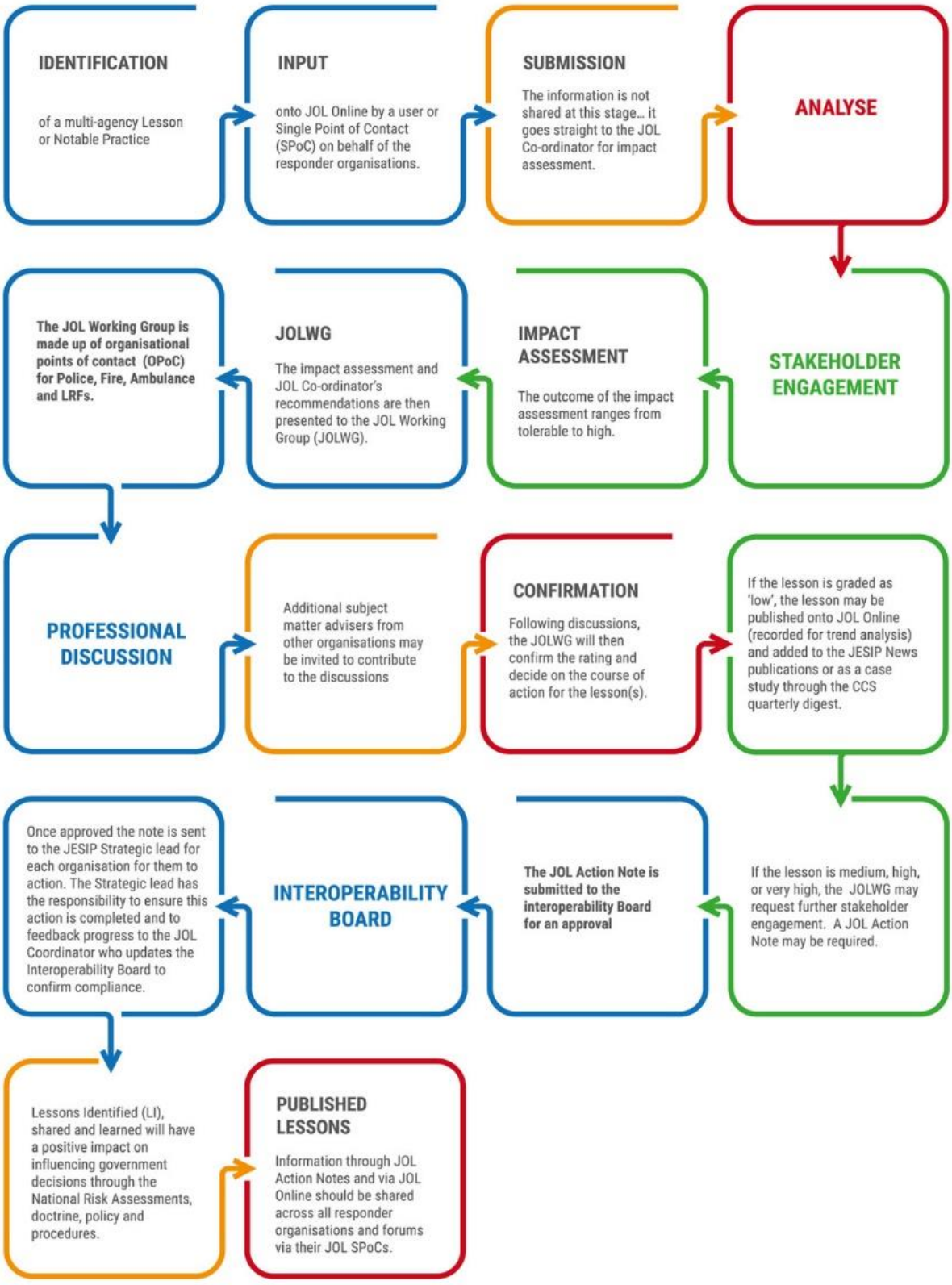

Figure 11 Joint Organisational Learning (Source: JESIP JOL Guidance October 2017)

6 Communication | Multi-Agency Partners

6.1 Overview - Communication

The ability to communicate effectively is a key part of the preparation for emergencies. The inability to communicate, and the requirements for restoring communications during an incident are important elements to prepare for.

Communications are a fundamental enabler underpinning the effective response to any emergency. Resilient communications are able to absorb or mitigate the effects of an emergency. Good communications are at the heart of an effective response to and recovery from an emergency.

There is no one simple solution to enhancing the resilience of communications. However, there are 5 guiding principles that, when appropriately applied, lead to enhanced resilience. These are:

- Identify and prioritise communication activities.
- Look beyond the technical solutions.
- Ensure diversity of your technical solutions.
- Adopt layered fall-back arrangements.
- Plan to share and exchange information.

The following types of communications should be considered by Rail Entities in the preparation for emergencies:

6.1.1 Internal Communications

Within the rail industry, communications channels with the regulator and rail partners for IEM preparation requirements and challenges should be incorporated into emergency management preparation communications.

6.1.2 Media Communications

Communication with the public is important to ensure information and advice is provided in the event of an incident occurring. This can be direct through social media channels, or via the traditional media. Rail Entities are also moving to communication via website and bespoke apps (for example, the Trainline, or National Rail apps) to provide real time information in the event of an emergency. It is important the same message is relayed across the various platforms to reduce any confusion in the event of an emergency.

6.1.3 Stakeholder Communications

It is important that emergency plans are made available and communicated effectively ahead of time to support incident response.

A pre-agreed method for warning and informing arrangements must be provided during the preparation stage to ensure that the correct information is provided to both emergency services and to other Rail Entities that may be involved in the incident. A full list of the required arrangements is provided in Provision 6.3.5.

6.1.4 Multi-Agency Partner Communications

Cooperation and therefore communication is a legal duty for Category 2 responders under the CCA. This duty is most effectively carried out via LRF structures. Telecommunications sub-groups (TSGs) within LRFs (LRPs and RRPs) act as a local focus for enhancing the resilience of responders' telecommunications arrangements. TSGs have been established in each LRF area as an integral part of the government's resilient telecommunications strategy.

In addition to use of public fixed telecommunications and public mobile telecommunications, the overall resilience of communications arrangements can be considerably enhanced through the use of schemes that are only available within the responder community. Technical solutions include but are not limited to:

- Satellite communications
- Airwave
- ResilienceDirect™

Under the CCA regulations, Category 1 responders must form a LRF as part of their obligation to co-operate with each other. Category 2 responders whose functions are exercisable within a local resilience area co-operate with other responders by attending meetings of the LRF or being represented at it. (In circumstances where all the Category 1 responders in a local resilience area agree, this requirement on a Category 2 may be varied). Often in practice, as permitted by the Act, several responder organisations in a particular industry or specialism will nominate a representative to attend on their behalf.

The LRF is the principal mechanism for multi-agency co-operation and co-ordination under the Act, based on each police force area. It is a process by which the duty-holders co-operate and formally communicate with each other to carry out duties under the CCA.

Organisations not specifically captured by the Schedule to the Act, such as the military and voluntary organisations, and the Department for Levelling Up, Housing and Communities Resilience and Emergencies Division (DLUHC RED) Team and Welsh Government will generally be invited to attend the LRF, contribute to its work and be involved in its working groups and sub-groups where relevant.

With regards to meetings and formal communications, the chief officer group of the LRF must make arrangements to meet at least once every six months. The aim should be to space these meetings evenly and to develop a regular cycle. Meetings can be held more frequently if LRF members agree that is necessary. The chief officer group should be supported by a general working group and subgroups. The frequency of these meetings is set by the LRF.

The LRF is not an operational body because it has no functional responsibilities to deliver during an emergency and no resources. However, generally, during an emergency, a particular set of those who make up the LRF are likely to come together as a multi-agency team to deliver their functional responsibilities. Having worked together via LRF exercises and at the request of single agency exercise development, responders are enabled to communicate and work together closely promoting interoperability via the functioning of the LRF.

6.1.5 Loss of Communications

In preparation for emergencies a priority consideration in planning and the exercising / testing of planning arrangements is the loss of communications and how this would be mitigated. Access, use and loss of telecommunications and electronic forms of communications are planned for and tested via multi-agency working groups, subgroups to LRFs and often by focus groups within individual organisations. Guiding principles from the Cabinet Office, Civil Contingencies Secretariat for loss of communications include:

- Avoiding reliance on a single technical solution.
- Technical interoperability
- Procedural interoperability
- Technical solutions solely for use contingency use.

Source: Cabinet Office Ensuring Resilient Communications

More information can be found in Guidance Notes section 6.4.14.

Provisions and Accompanying Guidance

All references consulted for this Code of Practice are listed in Section 7 References. The Provision Endnotes can be found in Section 7.1. A full provisions table is provided in the appendices of this document. The RDG ACoP: Part A - Governance also identifies a number of provisions and guidance notes in relation to communications***.

6.2 Provisions

6.2.1 Rail Entities ***MUST*** make their emergency plans available to aid cooperation and interoperability. [7, 28, 29]

6.2.2 Rail Entities ***MUST*** maintain arrangements to warn the public, and to provide information and advice to the public, if an emergency is likely to occur or has occurred. [7, 28, 29]

6.2.3 Rail Entities ***MUST*** collaborate with Local Resilience Forums (LRFs) and Local Resilience

Partnerships (LRPs) to enable information and expertise sharing, enhance understanding of best-practices and current horizon scanning, real-time monitoring and data gathering activities. [7, 28, 29]

6.2.4 Rail Entities ***MUST*** be effectively represented, or effectively represented by another responder, at meetings of the Chief Officers Group for the Local Resilience Area, where reasonably practicable and if invited to do so by the relevant Category 1 Responders; in the case of any other meetings of a LRF/LRP any groups or sub-groups, or, where the general Category 2 responder exercises functions in London, a borough resilience forum, must consider whether it is appropriate for it to attend the meeting or to be effectively represented at the meeting by another responder. [7, 28, 29]

6.2.5 Rail Entities ***MUST*** ensure their warning and informing arrangements include the ability to communicate an incident [22]:

a) Location
b) Access/egress routes
c) Date/time
d) Any rolling stock involved, plus its route
e) Incident timeline
f) Casualties/fatalities
g) No of passengers involved
h) Damage caused
i) Prevailing weather conditions
j) Dangerous goods on-board
k) Crew on-board
l) Railway property owner
m) Staff responsible for movement of the rolling stock
n) Number and type of vehicles involved
o) Emergency services in attendance
p) Incident Commander's contact details

6.2.6 Rail Entities ***MUST*** notify the Branch of its occurrence immediately as it learns of the occurrence and by the quickest means available. [22]

6.2.7 Rail Entities ***MUST*** ensure emergency plans include the capability to communicate with vehicles. [24]

6.2.8 Rail Entities ***SHOULD*** ensure their emergency plans include the roles and responsibilities of partner agencies and that this is effectively communicated to them, including [21]:

- BTP,
- RAIB,
- Network Rail,
- TOCs,
- LUL,
- Local Authorities; and
- Emergency Services.

6.2.9 Rail Entities ***SHOULD*** maintain plans for notification, communication, and response during an emergency. [23]

6.2.10 Rail Entities ***SHOULD*** have a formalised structure for internal information sharing. [19]

6.2.11 Rail Entities ***SHOULD*** agree emergency plans with partner agencies. [23]

6.2.12 Rail Entities ***SHOULD*** prepare for the loss of IT services & telecommunications. [2]

6.2.13 Rail Entities ***SHOULD*** have a crisis communications plan. This plan should be updated in accordance with PR and communications policies within the organisation. [19]

6.2.14 Rail Entities ***COULD*** have a media communications plan developed in the event of media interest in an incident. [19]

6.2.15 Rail Entities ***SHOULD*** communicate lessons learned that are honest and open, with relevant stakeholders. [19]

6.2.16 When sharing information or communicating with other agencies, plain language that is free of abbreviations and jargon ***SHOULD*** be used. This ensures that the information shared is clear and easily understood. [12]

6.2.17 Information sharing ***SHOULD*** be fully collaborative both with direct collaborating organisations and others with relevant information and / or experience. [10]

6.2.18 Employees ***SHOULD*** be able to communicate any concerns and issues or identify improvements to information, instructions, standards, and procedures. This should be acted upon by managers and feedback should be given promptly. [14]

6.2.19 The organisation ***SHOULD*** look at how other organisations communicate H&S information and implement best practice. [14]

6.2.20 There ***SHOULD*** be active pursuit of continuous improvement in communication within the organisation. [14]

6.2.21 There ***SHOULD*** be active attempts to continuously improve the two-way exchange of risk management information with collaborators. [14]

6.2.22 Effective risk management ***SHOULD*** be based on the provision of adequate information. [14]

6.2.23 The organisation ***SHOULD*** look to other sectors and countries to identify system-safety issues and controls. There ***SHOULD*** be evidence that this has led to continuous improvement. [14]

6.2.24 The procedures and standards ***SHOULD*** drive the organisation to strive for continuous improvement and ***SHOULD*** look for best practice from other industries in the UK and internationally. [14]

6.2.25 Best practice ***SHOULD*** be drawn from, implemented, and shared with other organisations in the UK and internationally. [14]

6.2.26 There ***SHOULD*** be arrangements for sharing information between organisations with shared H&S risks, in order to promote effective reviews and continual improvement. [14]

6.2.27 Rail Entities ***SHOULD*** communicate and disseminate extreme weather plans ahead of time. [16]

6.2.28 Rail Entity staff ***SHOULD*** be aware of changes to any extreme weather plans. [16]

6.2.29 Rail Entities ***SHOULD*** understand the implications of incidents and incident response on corporate reputation. [19]

6.2.30 Rail Entities ***SHOULD*** have a strategy to address corporate and reputation impact to include[19]:

- Contact with the media
- Social media usage
- R&R for CMT
- Stakeholder communications

***** The RDG ACoP: Part A - Governance identifies a number of provisions and guidance notes in relation to communications, including:**

Rail Entities ***MUST*** identify the relevant stakeholders from Category 1 and Category 2 responders and establish clear communication channels.

Rail Entities individually ***SHOULD*** make clear statements of IEM roles, responsibilities, and communication both within their organisation and with external stakeholders. This should encompass those providing strategic direction to the organisation, full-time IEM professionals and those that have IEM responsibilities placed upon them as part of their BAU duties.

Rail Entities ***SHOULD*** establish an effective process to engage regularly with its key regulators, including ORR, DfT, TfW and Transport Scotland – where relevant and applicable. This process should include senior-level engagement with the relevant regulator on IEM matters, establishing two-way communications to

influence relevant policy and regulatory requirements.

Rail Entities ***SHOULD*** develop, regularly conduct, and continuously improve, effective stakeholder engagement and communication strategy and plan. Rail Entities operate in a complex ecosystem, composed of internal and external, formal, and informal stakeholders – all of which have a role to play in enabling the resilience of each entity and the sector.

The IEM governance structure ***SHOULD*** support two-way communication providing individuals and leadership with voice on IEM and resilience.

6.3 Guidance Notes

6.3.1 Principles for Effective Communications

During an incident, communications must deliver information in a timely and effective manner, whilst also being cognisant of the fact that the situation can change rapidly. Different audiences will require different information and have different needs. Communicators should:

- Explain what is being done to control the situation.
- Use a consistent planning process that incorporates effective risk communication.
- Coordinate messages with other Rail Entities and, in some cases, external partners/stakeholders such as the BTP and DfT/devolved governments.
- Use a centralised communications channel / network.

Communications should be:

6.3.2 Communications Plans

Communications plans should include the following elements of best practice:

- Types of communications, utilisation, interoperability, and contingency only communications.
- Media response plan with pre-agreed templated responses approved by marketing / communications / CEO. Joint response statement with emergency response services discussed during preparation stages.
- Have a crisis spokesperson identified and trained for communication needs.
- Next of kin / emergency contact communications plan provided within training and exercising requirements.
- Arrangements for loss of communications.
  - Contingency arrangements for loss of, or loss of access to, electronic information, including emergency arrangements and redundancy.
- Review and testing cycle for communications systems and plans.

6.3.3 GSM-R, Global System for Mobile Communications – Railway

GSM-Railway is an international wireless communications standard for railway communication and applications. It is used for communication between train and railway regulation control centres.

GSM-R is a secure platform for voice and data communication between railway operational staff, including drivers, dispatchers, shunting team members, train engineers, and station controllers. It delivers features such as Voice Group Call Service (VGCS), Voice Broadcasting Service (VBS), location-based connections, and call pre-emption in case of an emergency. This supports applications such as cargo tracking, video surveillance in trains and at stations, and passenger information services.

6.3.4 Electronic Communications

Cyber-attacks are an ever-increasing threat to the UK's critical national infrastructure, whether it is to deny service or steal intellectual property. Cyber-attack poses a growing threat to the security and therefore the safety of infrastructure in Great Britain, including the railway networks. Electronic communications, including electronically stored emergency plans are therefore particularly vulnerable to cyber-attacks. It's essential that software and hardware security systems have the full set of threat mitigations at the core of their functionality and are utilised by a site for maximum effect. The National Protective Security Authority's Cyber Assurance of Physical Security Systems (CAPSS) is designed to assist security managers in focussing on key areas when it comes to protecting against cyber-attacks. Rail Entities are encouraged to consult both the National Protective Security Authority (NPSA) guidance and Rail Cyber Security Guidance to Industry.

Source: Cyber Assurance of Physical Security Systems (CAPSS)

6.3.5 ResilienceDirect™

ResilienceDirect™ is a unique digital online private 'network' which is a 24/7 365 live service with the UK and overseas territories. ResilienceDirect™ enables civil protection practitioners to work together – across geographical and organisational boundaries – during the preparation, response and recovery phases of an event or emergency.

ResilienceDirect™ provides emergency responders with situational awareness, clear communications and informed decision making. The platform enables organisations to fulfil these duties by supporting the adoption of multi-agency working practices and ensuring that key information is readily and consistently available to users.

ResilienceDirect™ helps to facilitate multi-agency collaboration in many ways, which include:

- Sharing emergency plans.
- Maintaining awareness of plans, exercising those plans and responding, followed by a recovery phase and lessons learnt.
- Real-time information sharing, supported by data visualisation.

ResilienceDirect™ is a web-based service built on a resilient and secure platform. It is accredited to hold electronic documents with protective markings. ResilienceDirect™ is available for use by all emergency management professionals. Organisations are required to sign an End User Agreement to ensure the continued integrity of the service.

Source: Resilient Communications Guidance

6.3.6 Resilient Satellite Network

The enhanced Resilience Satellite Network provides uninterrupted coverage when normal terrestrial or more consumer-based communications services may be congested, under threat or suffering from disruption. Two different satellites operating via two interconnecting and resilient teleports within the UK and each overing the same geographical area, meaning that if one should fail customers can be instantly moved onto the second network ensuring the connection is never compromised. The service is accredited with ISO:27001 certification, an internationally recognised standard for security compliance. The service is managed in real time from a network operations centre based in the UK.

Source: Excelerate Technology Enhanced Resilience Satellite Network

6.3.7 Privilege Access Schemes

Privilege access schemes are limited to those with a role to play in an emergency response. The schemes covered are:

- Privileged access to mobile telephone networks.

- Privileged access to the fixed-line telephone system.
- Access by those outside the emergency services to use Airwave.

Privilege access schemes will often form part of an organisation's arrangements to enhance the resilience of their telecommunications. However, some of the current schemes, notably access to mobile public telecommunications infrastructures, have acquired a level of importance that far exceeds their utility. Others, such as Airwave, are only really suitable as an everyday solution for those organisations with the need to be in contact with the emergency services and are familiar with the protocols applicable to using private mobile radios.

Source: Resilient Communications Guidance

6.3.8 Mobile Telecommunications Privileged Access Scheme (MTPAS)

MTPAS was launched by the Civil Contingencies Secretariat (CCS) in September 2009 and is intended to preserve access to mobile networks by those engaged in an emergency response when network capacity is under pressure.

Public cellular mobile telephony has played an important part in enabling communications during the response to recent emergencies, but mobile networks can become overwhelmed by a high concentration of calls that often occur immediately after a major incident.

Privileged access is achieved by the installation of a special SIM (Subscriber Identity Module) card in the telephone handset. These special SIMs are only available to entitled users within the responder community and not to members of the public. Privileged access SIMs are provided by the networks to their customers without additional cost.

Eligibility is restricted to organisations that have a part to play in responding to, or recovering from, an emergency as defined in the CCA. Primarily these are:

- Category 1 and 2 responder organisations
- Partners of Category 1 responders who have a requirement to be in communication with Category 1 responders when performing a front-line role in the response phase of an emergency, including the voluntary sector.
- Central government departments
- Devolved administrations in Scotland, Wales, and Northern Ireland

Within an eligible organisation, MTPAS will only be available to staff designated as having an operational role at the scene of a major incident or emergency or be required to directly support those with an operational role at the scene of an incident at a tactical or strategic level.

The majority of organisations are sponsored on MTPAS by Telecommunications Sub Groups (TSGs) which operate under the LRF structure. The TSGs fully co-ordinate the scheme for their local resilience areas. Some responder organisations work on a national rather than a local basis and these will be sponsored by central government departments. The devolved administrations assess eligibility and provide sponsorship for their responder's groups.

At the onset of an emergency response, when a SCG has been established, the Police Strategic Commander, who is likely to be in charge of the response, will use an agreed protocol to notify all mobile network operators that a major incident has been declared and request that call traffic levels are monitored. If networks become congested, the network operators are asked to consider invoking MTPAS to give emergency responders a much higher likelihood of being able to make a call than other customers.

Source: Resilient Communications Guidance

6.3.9 Airwave

Airwave is the secure and resilient mobile telecommunications system for the police, ambulance and fire and rescue services and other responder organisations. Network Rail and some TOCs are Airwave users. Under certain scenarios Airwave system access may be reduced to free up additional system capacity for the emergency services.

The radio spectrum used by Airwave is allocated for use by the emergency services and public safety users which largely embraces Category 1 and 2 responders as defined by the CCA. Consequently, Airwave is

restricted to a closed community of responders.

Access to Airwave is managed by Ofcom, the telecommunications regulator. Organisations wishing to join the Sharers' List must:

- Respond to emergencies.
- Be involved in emergency situations reasonably frequently.
- Be civilian or required to respond to civilian emergencies.
- Require interaction with those who respond to emergencies.

The Multi Agency Airwave User Group represents the non-blue light Airwave users and is open to all public safety organisations either using Airwave or interested in taking up the service.

Source: Resilient Communications Guidance

6.3.10 Interoperability

To ensure that the advantages of having a common radio platform for responders were fully realised, the CCS worked with the former Multi-Agency Interoperability Programme within the National Policing Improvement Agency (NPIA) to develop guidance for the use of the Airwave system. Since 2011, all LRFs have identified a multi-agency Airwave Senior Responsible Officer (SRO) to champion development of a Standard Operating Procedure (SOP) for local Airwave use across the responder community.

6.3.11 Information and Data Sharing - Emergency Preparedness

Sharing information is at the heart of emergency planning. It has a direct impact on members of the community, ensuring that they are put in touch with and contacted by the organisations and public bodies that can help them through traumatic events.

Events over recent years have raised awareness of information and data sharing amongst a variety of stakeholders and have prompted further thought and queries on wider issues outside the immediate emergency planning, response, and recovery phases.

The issues touch on a variety of types of sharing:

- Personal data
- Emergency plans
- Commercial or sensitive data, and all for a variety of planning, response, and recovery purposes

"Information sharing" generally refers to any information that is non-personal. This includes plans, schematics, commercial or business data amongst others. Appropriate information sharing lies at the heart of effective co-operation. Information sharing need not be formal and should happen as part of everyday co-operation.

"Data sharing" generally refers to information that can be used to identify a living individual, and usually comes under the remit of the Data Protection Act 2018.

Further information on Data Handling can be found in RDG-OPS-ACOP-011 IEM, Response.

6.3.12 Sharing Information under the CCA

Under the CCA, Category 1 and 2 responders have a duty to share relevant information with other Category 1 and 2 responders. This is fundamental to their ability to fulfil the range of other civil protection duties under the act, including emergency planning, risk assessment and business continuity management. The statutory guidance on the CCA also encourages information sharing between responders. In most instances, information will pass freely between Category 1 and 2 responders, as part of a more general process of dialogue and co-operation. But there are still some instances in which the supply of information will be more controlled, and hence a formal request for information may be appropriate. It should be noted that the Civil Contingencies Act 2004 does not contradict the Data Protection Act 2018.

6.3.13 Security Classified Information

Not all information can be shared, and the CCA allows exceptions from the supply of some sensitive information. There are broadly 4 kinds of sensitive information:

- Information prejudicial to national security

- Information prejudicial to public safety
- Commercially sensitive information
- Personal information

There are different degrees of sensitive information. The guidance to accompany the CCA, Emergency Preparedness, clearly states that some sensitive information may be suitable for some audiences but not others. The Act also offers safeguards that make clear that sensitive information can still be shared between Category 1 and 2 responders for emergency planning purposes – the organisation providing the information can specify that the information may only be used for the purpose for which it was requested.

For some incidents the multi-agency information sharing meetings may be required to happen in person within a secure location with agencies represented by a staff member with an appropriate level of security clearance.

6.3.14 Loss of Communications

One of the key issues identified in the aftermath of many emergencies, such as the 7th July London bombings, has been the vast increase in calls on the fixed and mobile telecommunications networks. Demand for use of the GSM network (mobile phone voice services and data services) greatly exceeded capacity and users experienced difficulty using telecoms for a time after the event. This exposed shortfalls for responders requiring resilient communications. Severe degradation or failure of telecommunications have been cited as a major concern underlying the response to many incidents.

In more recent years the increase of cyber-attacks has become more common place, with breaches of data and data leakages having serious implications. Often organisations will have key contact information, company plans and procedures and emergency arrangements in electronic format only, leaving them at risk of loss of vital information and communications should a cyber-attack occur.

There is no silver bullet to achieving resilient telecommunications and responders will achieve resilience via different means, but it should be driven by the need to communicate and not led by the availability of technical solutions.

Guiding principles from the Cabinet Office, Civil Contingencies Secretariat for loss of communications include:

- Avoiding reliance on a single technical solution.
    - Not relying on a single technical solution (such as GSM networks) and adopting a diverse, layered fall-back approach to communications can go a long way to enhancing resilience. A layered fall-back approach recognises that no means of communication is always likely to be available. In the event of failure or unacceptable degradation of the primary means of communicating, falling back to another option (possibly providing less ‘rich’ communications) helps absorb disruptive challenges or mitigate their effects. Fall-back options are likely to require a reconsideration of the interrelated issues identified above.

- Technical interoperability
    - Technical interoperability is often taken for granted with ‘gateways’ between different telecommunications platforms (such as GSM networks and the PSTN) that provide seamless communications. But this may not always the case, for instance gateways are not necessarily provided to the PSTN from private business radio systems.

- Procedural interoperability
    - Procedural interoperability becomes increasingly important with point-to-multipoint communications. Communication is greatly enhanced through agreed protocols; these can take the form of call-signs and radio discipline (particularly for mobile radio communications and agreed procedures for managing conference calls.

- Technical solutions solely for use contingency use.
    - The use of certain technical solutions solely for contingency use (for example, satellite systems or radio communications systems) can result in unanticipated consequences that could result in ineffective communications.

Diversity is a key enabler of resilient telecommunications. However, it can be difficult to assess how truly diverse technical solutions are because of the dependencies of one technical solution on another. Dependency arises in many forms. At a very fundamental level, all public land mobile networks are dependent on core communications networks: failure or degradation of core networks may affect mobile services. Pager systems

offer diverse means of initiating messages: through a voice call to a bureau, from a text message sent over a mobile phone or on-line via a website. Each of these means of initiation has its own dependencies, linked to the particular service providers selected as well as the availability of the underlying voice, message or IP network used as the bearer. Diversity issues can be very complex and should be explored with any prospective service provider to a depth that is appropriate for the requirement.

Communications systems will not be available 100% of the time. Availability is a consequence of the reliability of the system (associated with faults, including failure of power supplies) and its ability to cope with congestion (resulting from excessive demand). All communications systems are susceptible to congestion when demand exceeds the available capacity. The capacity is usually expressed in terms of bandwidth, number of concurrent calls, or a measure that is proprietary to the technology (such as ‘slots’ in GSM networks). Systems can be managed to increase the number of concurrent calls through more intensive use of bandwidth, although this is at the expense of reduce voice quality. Communications systems are managed to maintain the maximum number of conversations at an acceptable level of quality. If the traffic on a system were not to be managed the system would effectively become grid-locked and the total number of separate calls would start to decrease. All commercial systems are carefully sized to provide some headroom for periods of high demand. However, headroom comes at a cost and consequently substantial headroom is only available where the economics are favourable. The availability of a communications system should be explored with any prospective service provider.

7 References

For the purpose of developing this Code of Practice, we have consulted a variety of International Standards, guidelines, and good practice sources. This includes the following:

7.1 Provisions References

Endnote Number	Source
1	Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 8
2	ISO22301 Security and resilience – Business continuity management systems – Requirements
3	RM³ SP Health and safety policy, leadership, and board governance: SP 4 Written health and safety management system (SMS)
4	RM³ PI & RCS Planning and implementing risk controls through co-ordinated management arrangements: Pl 1 Risk assessment and management.
5	RM³ PI & RCS Planning and implementing risk controls through co-ordinated management arrangements: RSC 2 Management of Assets
6	RM³ MRA Monitoring, audit and review: MRA 1 Proactive monitoring arrangements
7	Civil Continencies Act 2004, Part 1.2.1
8	Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 7
9	Railway and Other Guided Transport Systems (Safety) Regulations (ROGS) 2006: Regulation 10
10	RM³ PI & RCS Planning and implementing risk controls through co-ordinated management arrangements: RCS 5 Emergency planning
11	RM³ OC Organising for control and communication: OC 1 Allocation of responsibilities
12	JESIP Joint Doctrine: The Interoperability Framework Edition Three, October 2021
13	RM³ OP Securing co-operation, competence and development of employees at all levels: OP 2 Competence Management System (CMS)
14	RM³ OC Organising for control and communication: OC 4 Internal communication arrangements
15	RDG Guidance Note: Major Incidents – Preparation of Aide Mémoires for Senior Managers RDG-OPS-GN-014 Issue 4 – April 2022
16	RDG Guidance Note: Extreme Weather Arrangements RDG-OPS-GN-015 Issue 4 – June 2023
17	RDG Guidance Note: Competence of Train Operator Liaison Officers (TOLOs) RDG-OPS-GN-016 Issue 4 – February 2021
18	RDG Guidance Note: Checklist for Major Incident Response RDG-OPS-GN-023 Issue 3 – July 2022
19	RDG Guidance Note: Emergency Planning – Knowledge, Understanding & Responsibilities RDG-GN011 Issue 4 – February 2023
20	Railways (Accident Investigation Reporting) Regulations (RAIRR) 2005: Regulation 12
21	ORR Strategy for regulation of health and safety risks - chapter 5: Interface system safety. December 2017
22	The Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 4.

23	Railways and Other Guided Transport Systems (Safety) Regulations (ROGS): Schedule 1.
24	Railways and Other Guided Transport Systems (Safety) Regulations (ROGS): Regulation 4
25	Railways and Other Guided Transport Systems (Safety) Regulations (ROGS): Regulation 6
26	RDG Approved Code of Practice: Joint Industry Provision of Humanitarian Assistance Following a Major Passenger Rail Incident. RDG-OPS-ACOP-001 Issue 17 – June 2021
27	RDG Guidance Note: Station Incident Response Planning RDG-GN033 Issue 2 – November 2019
28	Civil Contingencies Act Enhancement Programme - Chapter 2 Cooperation
29	Emergency Preparedness Guidance on Part 1 of the CCA 2004, its associated regulations and non-statutory arrangements, January 2006.
30	Railways (Accident Investigation and Reporting) Regulations (RAIRR) 2005: Regulation 6
31	Civil Contingencies Act Enhancement Programme - Chapter 5 (Emergency Planning) Revision to *Emergency Preparedness*

7.2 Legislation & Regulation

Name of the document	Reference number
Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009	N/A
Railways and Other Guided Systems (Safety) Regulations 2006 (ROGS)	N/A
Civil Contingencies Act 2004	N/A
Management of Health and Safety at Work Regulations 1999 (MHSWR)	N/A
Data Protection Act 2018	N/A
Health and Safety at Work Act 1974	N/A
Terrorism (Protection of Premises) Draft Bill 2023	N/A

7.3 RDG Documentation – ACoP / GN

Name of the document	Reference number
RDG/NR Guidance Note: Contingency Planning Arrangements for a Flu Pandemic	RDG NR-GN FLU01*
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 Approved Code of Practice: Incident Response Duties of Primary Support Operators	RDG-ACOP-016
RDG Approved Code of Practice with Guidance IEM, Response.	RDG-OPS-ACOP-011
RDG Approved Code of Practice with Guidance IEM, Recovery.	RDG-OPS-ACOP-012
RDG Guidance Note: The Training of On Train Staff in On Train Emergency Procedures	RDG-OPS-GN-003

RDG Guidance Note: Emergency Planning - Knowledge, Understanding and Responsibilities	RDG-GN011
RDG Guidance Note: Major Incidents – Preparation of Aide Mémoires for Senior Managers	RDG-OPS-GN-014
RDG Guidance Note: Extreme Weather Arrangements, including Failure or Non-Availability of On-Train Environment Control Systems	RDG-OPS-GN-015
RDG Guidance Note: Competence of Train Operator Liaison Officers (TOLOs)	RDG-OPS-GN-016
RDG Guidance Note: Competence of Station Incident Officers (SIOs)	RDG-OPS-GN-017
RDG Guidance Note: Checklist for Major Incident Response	RDG-OPS-GN-023
RDG Guidance Note: Post Incident Management of Personal Property	RDG-OPS-GN-025
RDG Guidance Note: Station Incident Response Planning	RDG-GN033**
RDG and Network Rail Guidance Note: Meeting the Needs of Passengers Stranded on Trains	RDG-OPS-GN-049
RDG Guidance Note: Emergency Management Legal & Regulatory Register	RDG-OPS-GN-064
RDG Guidance Note: Rail Emergency Management Code of Practice, Anticipation, Assessment and Prevention	TBC
Rail Resilience Project (RRP) Emergency Management Review: Findings & Recommendations Report. Version 1.3, September 2021.	N/A
* Issued jointly with Network Rail ** At the time of writing this Code of Practice, these Guidance Notes are undergoing review.	

7.4 International / British Standards

Name of the document	Reference
Security and Resilience – Crisis Management – Guidelines	ISO22361:2022
Security and Resilience – Community and Resilience – Principles and framework for urban resilience	ISO22371:2022
Governance of Organisations – Guidance	ISO37000:2021
Societal security - Business continuity management systems - Requirements	ISO22301:2019
Risk management - Guidelines	ISO31000:2018
Organisational Resilience	ISO22316:2017

7.5 Guidelines

Name of the document	Date of Issue
National Risk Register	August 2023
UK Resilience Framework	December 2022
Government Communication Service: Emergency Planning Framework	October 2022
JESIP Learning Outcomes Framework Version 2	April 2022
JESIP Training and Trainer Specification	April 2022

JESIP Roles & Responsibilities in Services	March 2022
JESIP Joint Doctrine: The Interoperability Framework Edition Three	October 2021
UK Severe Space Weather Preparedness Strategy	September 2021
Land Transport Security and Security In the Design of Stations (SIDOS)	July 2018
Preparing Scotland: Scottish Guidance On Resilience: Philosophy, Principles, Structures And Regulatory Duties	June 2016
DfT Rail Cyber Security Guidance to Industry	February 2016
National Recovery Guidance	June 2013
Emergency responder interoperability: Lexicon of UK Civil Protection Terminology Version 2.1.1	February 2013
Preparation and planning for emergencies: responsibilities of responder agencies and others	February 2013
Civil Contingencies Act: Emergency Preparedness Chapter 1 Introduction	March 2012
Cabinet Office: Civil Contingencies Secretariat: Ensuring Resilient Telecommunications: A Survey Of Some Technical Solutions	2006
Emergency Preparedness, Response and Recovery Guidance on Part 1 of the CCA 2004, its associated regulations and non-statutory arrangements.	January 2006

7.6 Good Practice Sources / Materials / Websites

Name of the document	Date of Issue
Cabinet Office ResilienceDirect™	2024
JESIP All Staff E-earning	2024
JESIP App	2024
JESIP Videos	2024
Network Rail Climate Change Adaptation	2024
Ofcom	2024
A consultation on implementing minimum service levels for passenger rail	2023
National Protective Security Authority Cyber Assurance of Physical Security Systems (CAPPS)	2023
The Business Continuity Institute Good Practice Guidelines 2023	2023
The Chartered Institute of Personnel and Development (CIPD) Learning Needs Analysis	2023
Governance 101: assurance and reassurance	2021
Department for Business, Energy & Industrial Strategy: UK Severe Space Weather Preparedness Strategy, September 2021	2021
Office of Rail and Road RM^3 The Risk Management Maturity Model	2019
Public Summary of Sector Security and Resilience Plans	2018
Designing for Infrastructure Resilience. Gallego-Lopez, C.; Essex, J. (with input from DFID) Evidence on Demand, UK (2016) 22pp	2016
Western Electricity Coordinating Council (WECC) Systematic Approach to Training	2015

8 Appendices

8.1 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	• There is no organised identification of possible emergencies and how to respond if they arise. • The organisation relies on the emergency services to deal with all aspects of an emergency. • The organisation does not consider the risks or the consequences of possible emergencies on the business or its workforce. • The organisation does not apply standards to support emergency planning or arrangements. • There is no consideration of the need for co-ordinated responses with other organisations in the event of major incidents requiring joint responses.	• The organisation realises that emergency responses are an important part of a risk control system. • Major emergencies that could arise are identified and there are some plans in place to deal with them. • Emergency responses are the responsibility of departments or divisions of the organisation. • The organisation applies basic requirements to the plans for major emergencies that could arise. • Emergency procedures requiring multi agency response are recognised, but there is no structured planning of responses required.	• Potential emergencies arising from tasks are identified as part of risk assessments. • Control measures, including training and resources, are in place to deal with emergencies. • The organisation determines and provides the resources needed to support the emergency planning arrangements. • The organisation recognises that emergency planning is a critical part of the business and is applying the appropriate standards. • Joint emergency response exercises take place with other organisations involved in a task. Roles in emergency response are clear and understood.	• Emergency responses are developed and reviewed in response to developing risks and emergency scenarios. • Feedback from exercise 'wash-ups' is taken into account when procedures are reviewed to make sure emergency responses remain up to date and effective. • 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. • Changes to the emergency response procedures are based on evidence from experience and demonstrably lead to improvements. • Collaborative organisations are fully involved in wash-up sessions including reviews of procedures.	• The organisation proactively looks outward when planning emergency response to identify and use good practice in a spirit of continuous improvement. • Emergency response arrangements are in place and reflect good practice from both within and outside the rail industry. • Lessons from published reports are included in procedure reviews and incorporated into revised emergency procedures. • The organisation actively seeks to find and share more effective ways of dealing with emergencies. • Information sharing is fully collaborative both with direct collaborating organisations and others with relevant information and / or experience.

People	• Strategic leadership of IEM is not in evidence. • People are unaware of their IEM governance responsibilities. • People are assigned to IEM governance roles on an ad hoc or inconsistent basis without training. • There is no wider culture of resilience across the Rail Entity (or industry)	• There is some strategic leadership for IEM. • People have been made aware of their IEM governance responsibilities. • Some people involved in IEM governance activities are suitably trained. • People are aware that the Rail Entity has a role to play in industry IEM	• Strategic leadership of IEM is often evidenced. • People have been made aware and generally understand their IEM responsibilities. • People fulfilling roles within the governance framework are suitably trained on how to deliver their obligations. • People understand the role that their Rail Entity plays in industry IEM.	• There is evidence of routine and consistent strategic leadership of IEM. • IEM governance responsibilities are documented within role profiles/ job descriptions. • People involved in IEM governance are trained and competent (including continuing professional development) to deliver their obligations. • People understand the role that their Rail Entity plays in UK IEM.	• There is evidence that strategic leadership of IEM is embedded in the organisation. • Everyone in the organisation recognises they have role to play in IEM and wider resilience and feel empowered to do so. • People are aware how their entity's IEM governance interfaces with that of colleagues in stakeholder organisations. • A culture of resilience has been embedded across the Rail Entity.
Processes	• There are no documented processes to enable IEM governance meetings across the Rail Entity. • There is no documented process for managing IEM skills and competency. • There is no documented process to support in developing situational awareness. • There are no documented processes to support the provision of IEM management information. • The is no process for assessing the maturity of a Rail Entity's IEM capability. • There is no process to manage the Rail Entity's engagement with other IEM stakeholders.	• Some processes to enable IEM governance meetings are documented. • Some elements of an IEM skills/competence system are documented but most are ad hoc. • The need for situational awareness is documented but supporting processes are ad hoc. • The need for IEM management information is documented but processes remain inconsistent. • IEM maturity is partially considered in other assessment processes. • Process to manage IEM stakeholder engagement are partially documented / inconsistent.	• Most processes to enable IEM governance meetings are documented. • Most elements of an IEM skills/competence system are documented. • Document processes exist for developing situational awareness. • There are documented processes for producing IEM management information. • There is a documented process for assessing IEM maturity. • Process to manage IEM stakeholder engagement are fully documented.	• Processes to enable IEM governance meetings are documented predictably applied. • An IEM skills/competence system is documented and applied consistently. • Document processes exist for developing situational awareness and are consistently applied. • There are documented processes for producing IEM management information with predictable outputs. • There is a documented process for assessing IEM maturity that is consistently applied. • Process to manage IEM stakeholder engagement are fully documented and consistently applied.	• There is an established (12+months) process for managing IEM governance meetings. • There is an established (12+months) IEM skills/competence system. • Document processes exist for developing situational awareness and are continuously improved. • Processes for producing IEM management information are embedded (12+months). • There is a documented process for assessing IEM maturity that is continuously improving. • IEM stakeholder engagement is fully embedded.

Technology	• The only technology support for IEM governance activities are standard office applications (email, word processing etc) • There are no specialist technology tools to enable provision and analysis of information for IEM governance. • No use is made of technology for real-time monitoring of information supporting IEM governance activity e.g. Remote-condition monitoring.	• Basic technology support is available for IEM governance activities e.g., simple spreadsheets to a capture ad analyse financial data. • Occasional use is made of specialist tools/systems for producing/analysing IEM data. • There is occasional or ad hoc use of real-time monitoring systems.	• Standard office applications are well-utilised to document, analyse, share/present and retain information supporting IEM governance. • Some specialist technologies are used routinely to gather and analyse IEM related information e.g., operational performance data. • Some standardised use is made of real time data, but this is mainly for individual projects.	• Standard office applications are used to their full capability (integrated data storage, remote meetings) to support IEM governance. • Specialist tools/systems are integrated to support IEM governance e.g., enterprise risk management software includes IEM-related risks. • Real time data is consistently used to support IEM governance where applicable.	• Standard office applications are used to their full capability (integrated data storage, remote meetings) to support IEM governance. • There is established (12+months) integration of specialist systems to support IEM governance and drive improvements. • The use of real time data to support IEM is well embedded (12+months) and routinely improved.
Locations	• Places, facilities, or premises are not relevant to the IEM governance provisions.	• Places, facilities, or premises are not relevant to the IEM governance provisions.	• Places, facilities, or premises are not relevant to the IEM governance provisions.	• Places, facilities, or premises are not relevant to the IEM governance provisions.	• Places, facilities, or premises are not relevant to the IEM governance provisions.
Suppliers	• The impact of suppliers' activities on IEM is not considered in IEM governance activities. • No data on supplier's activities is included in IEM governance information. • Suppliers do not contribute to IEM governance activities.	• The impact of suppliers' activities on IEM is rarely considered in IEM governance activities. • Data on or from suppliers to support IEM governance is considered on an ad hoc basis. • Suppliers contribute to IEM governance on an informal basis.	• The impact of supplier's activities on IEM is regularly considered in IEM governance activities. • Data on or from suppliers to support IEM governance is considered on a regular basis. • Suppliers contribute to IEM governance on an formal, but infrequent, basis.	• The impact of suppliers' activities on IEM is routinely and consistently considered in IEM governance activities. • Data on or from suppliers is integrated to support IEM governance activities. • Suppliers contribute to IEM governance on a formal and frequent basis.	• The impact of suppliers' activities on IEM is routinely and consistently (12+months) considered in IEM governance activities. • Data on or from suppliers is integrated to support IEM governance activities. • Suppliers' contribution to IEM governance is formal and embedded (12+months).

8.2 Case Studies

The following case studies showcase real world examples of best practice from various industries when preparing for emergencies. The case studies have been themed per chapter; they include examples across the 'prepare' arena.

To protect individuals and organisations, case studies have been kept anonymous.

8.2.1 Preparation & Resilience: Case Study #1 – Implementing a Resilience Framework

Utilising the ISO22301 framework, a development company implemented resilience at the outset of planning activity for the organisation by embedding resilience within the heart of the corporate organisation.

Organisationally, resilience sat within the governance, risk and compliance division. This ensured the enterprise risk management framework that was developed for the organisation and endorsed at Board of Directors (BoD) level was influenced and complimented the resilience framework. Preparation activity was focused on mitigation of, response to, or recovery from the risks identified across the business from an operational level through to strategic risk management needs.

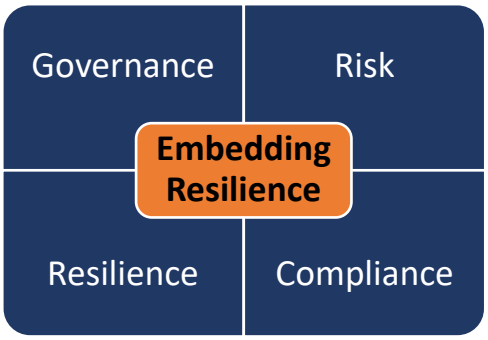

Figure 12 Embedding Resilience

The framework was endorsed via the Resilience Policy from the BoD, and the principles of resilience and the organisations preparedness for emergencies was cascaded across a pre-defined governance model (as demonstrated in the governance responsibilities within the RDG ACoP: Part A – Governance). This was supported by a compliance function to ensure legal and regulatory compliance requirements were also considered for resilience activity.

The implementation of the framework within this setting changed the way the organisation thought about both risk and resilience. It ensured a strategic, tactical, and operational mechanism was in place, but it also supported organisational wide training and awareness for resilience, as well as inter-disciplinary testing and exercising programmes that focused on pre-identified risks.

This framework enabled preparedness for resilience, with the following best practice examples highlighted:

- Quarterly knowledge shares were used to share information and best practice with the tactical and operational teams across the organisation, promoting better preparedness across the business and breaking down siloed communications.
- Industry / risk-based taskforces were implemented following COVID-19 to prepare for specific high-risk events that span both the organisational response capability but also external stakeholders.
- The framework endorsed at BoD level ensured that liaison with government entities to plan for high risks eventualities was better implemented.
- KPI's integrated for resilience and reliability across personal KPI's within the organisation was used to both measure performance linked to resilience, and to embed resilience within the performance metric for the organisation.

8.2.2 Planning for Emergencies: Case Study #2 – Bringing the plan to life

Following an emergency, and poor implementation of current emergency planning documents, a manufacturing company was struggling to ensure that plans were fit for purpose, well embedded within response teams and useful in the event of a major incident. The organisation focused on improvements to strategic planning requirements, ensuring that plans were articulating activity that was of most importance to the industry in the event of an emergency, but was also useful for those on the ground enacting the planning material when needed.

Examples of how the organisation brought their plan to life include:

- Plan page turns: plans were regularly 'page turned' within the committees that had been created to ensure content is understood, is fit for purpose, and doesn't need updating. This was implemented for emergency planning, crisis management planning and business continuity planning.
- An administration requirement section for the plans was added, outlining in plain English what was needed from an administration perspective to enact the plan.
- Where a risk was identified from the planning activity (lack of competency, plan elements missed, etc) this was captured on the enterprise risk management system as a specific resilience risk.
- Plans were taken 'off the shelf' and made simple. Key plan elements were printed on laminate one-page documents for ease of access and reading for operational teams.
- Plans were stored in various locations, to address the inability of plans to be implemented when required in some instances due inaccessibility.

8.2.3 Preparation & Resilience / Planning for Emergencies: Case Study #3 – Beyond Design Basis Planning

Following the March 2011 earthquake and tsunami in Japan and consequent major incident at Fukushima Daiichi nuclear plant, the Office for Nuclear Regulation reviewed all UK nuclear facilities. One nuclear operator also commissioned an internal review to support the regulators conclusions and to push resilience planning to consider events beyond a design basis accident scenario.

A company-wide programme brought together engineering, project management and resilience skills to produce enhanced emergency arrangements; documentation, training, and exercising programmes and new back up equipment and maintenance programmes. These enhanced arrangements were designed to account for those risks where the likelihood is ordinarily deemed too infrequent to include in regular anticipated / expected emergency arrangements.

Credible "beyond design basis" or extreme scenarios and emergency arrangements "enhancements" to meet these risks were developed whilst still ensuring integration with business as usual / previous emergency arrangements.

Specialist equipment, sites and resources that were flexible, transportable and with a timely emergency response capability, were established. As was the development and delivery of logistics support and sustainment arrangements. All new "extreme" event or beyond design basis equipment, logistical support, resources and support models were tested via large scale national exercises and incorporated into the company's existing training and exercising programmes, gaining buy in and approval from the regulator.

8.2.4 Training & Awareness, Testing & Exercising: Case Study #4 – Training Programme for Regional Emergency Planning Teams

A strategic highways organisation created new regional emergency planning teams (resilience specialists), to develop and embed emergency arrangements, and carry out the requirements of Category 2 responders under the CCA. As teams were regional, staff skill sets, and experience differed across the country. A strategic network resilience team managed the development of the regional teams and coordinated the following activities:

- Policy reviews and benchmarking studies to set criteria for staff.
- Coordination, facilitation and support of bi-monthly resilience forums and subsequent working groups with key stakeholders.
- Provision of specialist advice and support on civil protection issues and major events planning.
- Advising on national work priorities for resilience.
- Design and delivery of emergency exercises.

- Development of strategic resilience policies.
- Development of specific and generic national and regional emergency plans.

The national occupational standards for civil protection, and from there the core competency framework for civil protection (developed by the Emergency Planning Society and Emergency Planning College) were used to define the roles and responsibilities of emergency planning managers and emergency planning officers in each team.

A training needs analysis was carried out to identify any gaps in civil protection knowledge and capabilities for each staff member and a training package was then developed to align with the national standards in civil protection. The training package was mapped across to JESIP and multi-agency civil protection training delivered by the Emergency Planning College, providing a route to close out gaps and ensure consistency in delivery and capability across regional teams.

8.2.5 Training & Awareness, Testing & Exercising: Case Study #5 – Regulated Modular Exercise Programmes

Nuclear emergency arrangements in the UK cover many regions and therefore many LRFs and LRF exercise programmes. A generating nuclear company with many operating facilities also has new build and decommissioning facilities, therefore many aspects to plan for in relation to exercise development.

Nuclear exercises are regulated and as such must occur within the exercise and review period. Level 1 exercises are required every year by each site, and they are delivered on-site. The majority of a Level 1 exercise is Live, they include communications with the company's central emergency support centre and mutual aid arrangements from sister sites.

Level 1 exercises test staff response capabilities: training and awareness, equipment processes and procedures, control room operations and decision making within the command-and-control structure, ultimately testing the power stations on site emergency plan and arrangements for which the nuclear operator is responsible. Level 1 exercises are generally added to the power stations local LRF or RRP's exercise programme due to the on-site participation and support required by the emergency services.

Level 2 exercises are off-site exercises, each power station and local authority (owner of the off-site plan) is expected to complete a Level 2 exercise every 3 years. These are regional multi-agency exercises testing the LRF multi-agency nuclear power stations off site plan. Level 2 exercises test the control rooms on site and centrally for the nuclear company, the multi-agency control rooms (met office, food standards agency, environment agency / Scottish environment protection agency, local authority, NHS, and UK Health Security Agency control rooms etc) and the tactical coordination centre, strategic coordination centre (usually managed by the police), a simulated version of COBR and rendezvous points at scene etc.

Level 3 exercises are national, with all aspects of Level 2s and national government control centres also stood up.

As the regulator sets themes for nuclear operators to focus on in their upcoming exercises, based on learning from recent events or from previous exercises, these are incorporated into the exercise programme, the LRF will usually have themes or areas to focus on too – areas of concern in the review of the off-site plan for example. Due to the extent and vast number of stakeholders and agencies involved in the exercise development and delivery stages, it is often more efficient and resourceful for regions to adopt a modular exercise approach. However, a modular approach requires extensive planning and resource in the initial stages and in development of the exercise programme.

The nuclear operator's off-site emergency planner will work with LRFs and the power station's on-site emergency planner to populate a matrix of themes and areas that must be exercised – as determined by the regulator, which exercise scenarios will meet these areas, and when they are due.

The matrix or exercise programme also includes the availability of external control centres. Whilst it is mandated that they be available should an emergency response be required, during peace time the external control centres are operational for other agencies (such as the police).

Due to the review cycle of the off-site emergency plan being three-yearly, an external LRF exercise could test the strategic coordination groups notification arrangements, or the communications arrangements or the media briefing centre etc and invite the nuclear regulator to witness the test of these arrangements. Therefore, that

power stations Level 2 exercise would not necessarily need to include communications, media briefing or SCG notification arrangements so thoroughly in the full Level 2 exercise as these would have been witnessed and assessed within the plan review period. This saves limited resource for a number of external agencies, is cost effective and means facilities and equipment can remain operational for the exercise.

8.2.6 Training & Awareness, Testing & Exercising: Case Study #6 – Nuclear Training and Improvements Programme

A nuclear organisation's technical sector implemented analysis and solutions through the full lifecycle of organisational learning and development this included:

- Design and Implementation of new technical training programmes and infrastructure.
- Development of management and support arrangements and tools.
- Performance gap and training needs analysis.
- Development of innovative training solutions.
- Performance and benefits assessment.

Safety is paramount within the nuclear industry and thus professional qualification and authorisation of staff for work roles is a key part of the technical organisation's responsibilities and represents a significant financial commitment. Every aspect of organisational learning has to stand up to scrutiny of the business leadership, accreditation board and the external regulator, plus support the organisation's safety culture.
Furthermore, the organisation is continually looking for improvement in its people, processes and information to be the world leader in commercially successful nuclear power generation and thus takes a close interest in the realisation of value for money from both the work contracted, and the solutions it provides.

Over time and through diligent and customer focused delivery the following has been implemented:

- Support for the design and implementation of a structured training programme for the internal regulation department of around 60 people.
- Design and support of training-related management information and reporting.
- Design and implementation of a major e-learning PC-based training package on Basic Nuclear Principles Refreshment, to be used by over 400 people on a cyclical basis.
- Participation in key self-assessments relating to organisational learning and development improvements that will support the re-accreditation of the Engineering Support training programme against industry standards.

These support services were a key contributor to achieving training standards accreditation for one of the largest single training programmes in the world providing credibility for lifetime extension programmes for the existing nuclear fleet and new build programmes. With clear demonstration that the business has control of its nuclear resource baseline in a measurable and systematic programme with a clear view of the challenges in addressing an aging demographic and an industry resource market under strain.

8.2.7 Communications & Multi-Agency Partners: Case Study #7 – DEFRA Group Comms

Being a flood victim is completely devastating and sadly with climate change it is happening more regularly. Defra Group comms represents both the Government response to flooding via Defra, and the operational response through the Environment Agency (EA). This gives the group responsibility for multiple messaging, channels and audiences and is why a tried and tested process for responding in a flood has been developed.

Groundwork was laid early. The group delivered a programme of proactive communications on flood prevention, holding EA-fronted media facilities to showcase flood defence work and or ministerial announcements on new flood investment and nature-based flood prevention. It is known flood incidents are unpredictable with their timing, location and severity often changing quickly, so the approach is deliberately flexible but follows a tested process throughout an incident.

As soon as it is known flooding is imminent, a media briefing is organised alongside the Met Office and other government departments, establishing a narrative on the severity of the weather and the preparation of the EA, and delivering vital public safety messaging to ensure that people are prepared.

Staff prepare as a communications team, with staff who usually focus on other policy areas surging into 'flood pods', forming mini comms teams for both Defra and EA as well as bolstering the Newsdesk. Surge capacity helps deliver a regular rhythm of media updates throughout flooding incidents, with daily press notices and

media facilities in affected areas to ensure the visibility of the EA and delivery of important operational updates. Briefing materials are prepared ahead of incidents, spokespeople are scheduled days in advance and press office staff are organised to travel to affected areas.

A ministerial (or Prime Ministerial visit) usually forms a key part of the response, usually taking place 2 to 3 days on from the initial flooding so as not to divert resources from the emergency response. Close working takes place with senior EA officials and in conjunction with LRFs to deliver these visits, building them into the daily rhythm of updates for the media.

During Storm Christoph this strategy was followed carefully, with successful response to nearly 400 media enquiries and 170 interviews conducted over the course of a week. As a result, whilst media coverage rightly reflected the human impact of Storm Christoph, which flooded 600 homes, it also included how 49,000 properties had been protected through government action. It also meant government and the EA was judged to have shown authority and leadership at a time of crisis.

Source: Case studies: crisis communications - GCS (civilservice.gov.uk)

8.2.8 Communications & Multi-Agency Partners: Case Study #8 – Government Communication Service (GCS) Crisis Communication Strategy

The GCS Emergency Planning Framework (2018) outlines how we plan, develop and implement an effective response during a crisis. The resource focuses on 6 critical stages which make up a crisis communications response, known as PRIMER. PRIMER stands for:

- **Plan** – It is essential to have a communications contingency plan in place, regularly update it and know where it is for when it matters.
- **Rehearse** – A crisis response works best if tested in advance, and doing this with partners can ensure we build important relationships in calmer times.
- **Implement** – Getting it right from the start can be critical – it's important to set up a crisis response in the right way to deliver from the get-go.
- **Maintain** – Crisis scenarios can be a test of stamina and character – it's important to maintain quality while supporting your team.
- **Evaluate** – It is crucial to measure what's getting through and what's not – we use the comprehensive GCS Evaluation Framework 2.0 to measure impact in real time and refine our approach.
- **Recover** – Communication has an important role in rebuilding trust and confidence – this includes capturing learnings and updating our structures.

Source: Crisis Communications: Operating Model - GCS (civilservice.gov.uk)

8.2.9 Lessons learned embedment: Case Study #9 – Traffic Incident Management Bulletin

A strategic highways organisation developed a Traffic Incident Management (TIM) Bulletin to disseminate lessons identified and good practice from the post incident debrief process into the incident management community on a monthly basis. Over 4 years more than 40 editions were published featuring approximately 200 articles covering a wide range of topical subjects. Amongst these topics were:

- Innovative methods of managing incidents.
- Incident management research.
- Highways TIM project updates.
- Emerging lessons and good practice from the post incident debrief process.

Due to limited access to e-communications, the Bulletin proved particularly popular with the on-road Traffic Officers and road responders (operational staff).

An extensive network of incident management contacts and knowledge was developed during the lifecycle of the project, this included a contacts matrix with regional contacts used frequently to quantify incident management concepts.

The benefit of developing such a database enabled the editorial team to know and understand issues and concerns facing the Bulletin readers. This ongoing proactive readership knowledge was balanced with having a Project Team composed of incident and operational management specialists.

A key facet to ensuring the longevity of the project was the embedment of existing Project Team personnel, achieved in part through the development of a governance paper which was issued to all personnel. This paper outlined all expected quality and performance control requirements and was further supported by a series of internal Project Team communication processes. Additionally, 'Value Workshops' identified further improvements, such as:

- Working with specialists to provide a more interactive, evolving Bulletin.
- Assisting with creating a ‘knowledge repository’.
- Developing a searchable archive facility.
- Developing a contact and readership database.

The bulletin acted as a blend of national and regional incident management information and was a learning tool for operational staff. It provided a platform for sharing experiences and innovative traffic incident management practices, raised awareness of the issues and risks faced by the on-road staff on a daily basis and supported the attainment of the organisations strategic vision and key targets.

8.2.10 Humanitarian Assistance: Case Study #10 – Incident Care Team Initiative

Incident Care Teams are a joint industry initiative established to provide humanitarian assistance in response to a major passenger rail incident. A key principle of the Incident Care Teams is that there is full mutual support between rail entities, this therefore requires common operating structures, common emergency arrangement procedures and common training and documentation in relation to emergency arrangements. Incident Care Teams are trained to help passengers in the hours and days immediately following a train accident or other serious incident. The team will work closely with emergency services, including police family liaison officers, and local authorities to look after the welfare of passengers.

Emergency services and other agencies will provide medical help and counselling for victims of major incidents. Incident Care Teams are considered an invaluable source of help to those responders, working together to make life easier for passengers as well as their families and friends, following incidents. The role of the Incident Care Team is to give practical help such as organising transport, accommodation, emergency clothing, or sorting out domestic problems. Training is organised to ensure that post incident care is provided consistently across all train operators. The team could be mobilised in the event of any UK train accident.

8.3 Full Provision List

Provision Number	Provision Statement
Chapter 3. Preparedness & Resilience	
3.2.1	Rail Entities ***MUST*** ensure that recommendations of the Rail Accident Investigation Branch (RAIB) are considered and acted upon, where appropriate within emergency planning arrangements.[20]
3.2.2	Rail Entities ***SHOULD*** adhere to requirements of the Railway Group Modular Rule Book when accessing Network Rail infrastructure in an emergency. [17]
3.2.3	Rail Entities' Safety Management System (SMS) ***SHOULD*** include IEM activity throughout all its processes and provisions. [21]
3.2.4	The SMS ***COULD*** clearly demonstrate how the organisation is kept aware of good practice in the rail and other industries, so that continuous improvement can be maintained. [3]
3.2.5	The SMS ***COULD*** be adaptable and responsive to change, to accommodate emerging issues / risks and reasonably foreseeable developments in legislation, technology, social, environmental, and political influences, whilst maintaining assurance. [3]
3.2.6	The SMS ***COULD*** be an integral part of the organisation's overall management system. [3]
3.2.7	The monitoring arrangement ***COULD*** address proportionately and appropriately all the processes and systems within the SMS to ensure their implementation, adequacy, and effectiveness. [6]
3.2.8	Rail Entities ***SHOULD*** implement a Business Continuity Management System (BCMS) determined by the external and internal issues that are relevant to its purpose and that affect its ability to achieve its intended outcome(s). [2]
3.2.9	Rail Entities ***SHOULD*** establish, implement, maintain, and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of ISO 22301. [2]
3.2.10	Rail Entities ***COULD*** proactively seek good practice examples in emergency management. [3]
3.2.11	Stakeholders ***COULD*** be consulted on and informed of best practice, to continually improve collaborative relationships and shared risk reduction. [3]
3.2.12	Risk assessment ***COULD*** be used to drive continual improvement in the risk profile of the organisation. [4]
3.2.13	Enterprise-level guidelines and standards ***COULD*** be in place with best practices incorporated from other industries. [5]
3.2.14	There ***COULD*** be clear evidence of searching for best practice in asset management and condition monitoring as part of the drive to continuous improvement. [5]
3.2.15	Rail Entities ***COULD*** be an early adopter of new standards relating to monitoring and recognised as an 'early complier' organisation. [6]
3.2.16	Appropriate risk assessment processes ***COULD*** be used to make strategic choices related to the totality of the rail infrastructure. [4]
3.2.17	Rail Entities ***COULD*** strive for continuous improvement in risk assessment processes looking at alternative techniques, which challenge the effectiveness of risk controls, by working with other organisations in their own and other industry sectors. [4]
3.2.18	Rail Entities ***COULD*** maintain an external view to identify effective risk controls from other organisations and other industry sectors. [4]
3.2.19	Rail Entities ***COULD*** be recognised as industry-leaders in risk management. [4]
3.2.20	Rail Entities ***COULD*** lead cross-industry risk reduction programmes. [4]
3.2.21	Active steps ***COULD*** be taken to identify, evaluate and utilise novel ways of monitoring to achieve continuous improvement in risk control. [6]
3.2.22	Managers ***COULD*** actively participate in industry-wide and cross-industry groups to improve risk control monitoring techniques e.g., remote condition monitoring. [6]

3.2.23	The organisation ***COULD*** have closely linked outcome and activity indicators which demonstrate risk controls are optimised. [6]
3.2.24	The organisation ***COULD*** be known for mature relationships with collaborators who strive to work again with the organisation as they are assured that risks will be controlled. [6]
3.2.25	Across the organisation monitoring activities ***COULD*** be recognised as vital in improving risk control.[6]
3.2.26	Rail Entities ***SHOULD*** understand the implications of incidents and incident response on corporate reputation. [19]
3.2.27	Emergency planners ***SHOULD*** have an understanding of risk management, train and station operation, command and control, and familiarity of IEM principles. [19]
3.2.28	Information on work history type and cost, condition and performance ***COULD*** be recorded at asset component level. [5]
3.2.29	Systematic and fully optimised data collection programme ***COULD*** be in place with supporting metadata. [5]
3.2.30	There ***COULD*** be evidence of an effective pro-active and predictive maintenance regime across the organisation. [5]
3.2.31	Preparedness for incidents ***SHOULD*** include gaining a level of understanding about the other organisations that may be involved at incidents. [12]
3.2.32	Rail Entity staff ***SHOULD*** be familiar with extreme weather plans and competent in their application. [16]
3.2.33	Rail Entities ***SHOULD*** increase the provision of response staff when weather related incidents are likely to occur. [16]
3.2.34	Additional staff ***SHOULD*** be co-located in strategic locations and in conjunction with emergency response agencies (BTP, for example). [16]
3.2.35	Rail Entities ***SHOULD*** not permit an employee to perform at the same time both the roles of TOLO and the RAIB Accredited Agent for a particular incident. [17]
3.2.36	Rail Entities ***SHOULD*** have a plan for the structure of Crisis Management Team (CMT) meetings. [19]
3.2.37	Rail Entities ***SHOULD*** have a plan to outline the relationship between the CMT and the strategic command. [19]
3.2.38	Rail Entities ***SHOULD*** determine knowledge and experience requirements and skills levels for personnel undertaking specific roles in emergency plans. [19]
3.2.39	Rail Entities ***SHOULD*** undertake a joint review into the response to, and management of the emergency.[19]
3.2.40	Rail Entities ***SHOULD*** produce a detailed report of the review including actions required and how and by whom they will be closed out. [19]
Chapter 4. Planning for Emergencies	
4.3.1	Rail Entities ***SHOULD*** have in place emergency plans which contain information on how they will reduce, control, or mitigate the effects of emergencies. [7, 29, 31]
4.3.2	As part of their emergency planning arrangements, Rail Entities ***COULD*** [10]: • Implement a process of continual improvement. • Update emergency plans to reflect best practice from within and outside the rail industry. • Actively seek ways to improve emergency plans. • Fully involve partner agencies in incident debriefs. [see Chapter 5] • Update emergency plans to reflect lessons learnt from incidents and exercises. [see Chapter 5]
4.3.3	Rail Entities ***SHOULD*** ensure their emergency plans are updated to reflect risk assessments. [7]
4.3.4	Rail Entities ***COULD*** implement a documented and standardised process to cooperate with relevant Category 1 and other Category 2 responders. [7, 28, 31]

4.3.5	Rail Entities ***MUST*** ensure emergency plans include arrangements to assist the RAIB in their investigations. [30]
4.3.6	Rail Entities ***MUST*** ensure emergency plans include arrangements to provide permitted inspectors access to the incident site and instruction that no evidence shall be removed (except in very limited exceptions and having notified the RAIB). [8]
4.3.7	Rail Entities ***MUST*** ensure emergency plans include arrangements to preserve evidence at the scene. [1]
4.3.8	Rail Entities ***SHOULD*** prepare and update emergency plans which include [27]: 1. A Station Plan 2. A Station Security Plan 3. A Station Incident Response Plan (SIRP) 4. An Evacuation Plan 5. An Operational Continuity Plan (including business continuity plans)
4.3.9	Rail Entities ***COULD*** adopt the working ethos of the Joint Emergency Services Interoperability Principles (JESIP). [27]
4.3.10	The Station Plan ***SHOULD*** state its purpose and scope. [27]
4.3.11	Rail Entities ***MUST*** ensure that the requirements of the National Rail Security Programme are communicated to Station Managers to ensure they are carried out as required. [27]
4.3.12	The content of the SSP ***MUST*** be agreed with the DfT. [27]
4.3.13	The measures specified in the Security Response Level (SRL) tables in the NRSP ***MUST*** be applied to a relevant location in accordance with the current SRL, as notified to the Station Facility Owners (SFOs) or operator in writing by the Secretary of State. [27]
4.3.14	The SIRP ***SHOULD*** be implemented when there is any deviation from BAU. [27]
4.3.15	The SIRP ***SHOULD*** set out tasks and activities to be considered by those managing the incident. [27]
4.3.16	A process ***SHOULD*** be put in place to identify any deviation from the defined BAU baseline, e.g., failure of electricity supply, an unusual degree of overcrowding, emergency incident. This ***SHOULD*** include monitoring to ensure tolerable thresholds are not exceeded and recording where appropriate decisions to implement or not implement the SIRP. [27]
4.3.17	Rail Entities ***SHOULD*** consider funding essential training courses for those responsible for station plans to understand the principles of emergency planning, including plan writing, planning, exercising and validation. [27]
4.3.18	Rail Entities ***SHOULD*** ensure that those who are responsible for updating plans, particularly if new to the role and relatively inexperienced, are supported by and the resulting plans reviewed by those with greater skillsets. [27]
4.3.19	In order to facilitate an invacuation or lockdown, Rail Entities ***SHOULD*** seek to identify potential 'safe havens' within the station to which members of the public and/or staff can be directed. [27]
4.3.20	Rail Entities ***SHOULD*** consider whether some of their plans for dealing with specific threats may be restricted. [27]
4.3.21	In addition, Rail Entities ***SHOULD*** ensure their emergency plans include dangerous goods passing through stations. [21]
4.3.22	Rail Entities ***SHOULD*** proactively look outward when planning emergency response to identify and use good practice in a spirit of continuous improvement. [10]
4.3.23	Emergency response arrangements ***SHOULD*** be in place and reflect good practice from both within and outside the rail industry. [10]
4.3.24	Lessons from published reports ***SHOULD*** be included in procedure reviews and incorporated into revised emergency procedures. [10]
4.3.25	Rail Entities ***SHOULD*** actively seek to find and share more effective ways of dealing with emergencies. [10]

4.3.26	Roles and responsibilities ***SHOULD*** be reviewed to ensure they remain in-line with standards in recognised high performing organisations. [11]
4.3.27	Individuals from collaborating Rail Entities ***SHOULD*** recognise and undertake roles and responsibilities allocated during collaborative activities. [11]
4.3.28	Rail Entities ***SHOULD*** identify who within their organisations is authorised to declare a 'Major Incident'. [15]
4.3.29	Rail Entities ***SHOULD*** maintain, review, and regularly update extreme weather plans. [16]
4.3.30	Plans ***SHOULD*** be reviewed and updated regularly. [16, 29]
4.3.31	Rail Entities ***SHOULD*** ensure that services & stations that may be affected by extreme weather are well stocked with emergency supplies of water and basic snacks. [16]
4.3.32	Rail Entities ***SHOULD*** ensure supply of vehicles to move emergency supplies to strategic locations as required.
4.3.33	Rail Entities ***SHOULD*** reference RDG-OPS-GN-023 for the checklist for major incident response within the organisation. [18]
4.3.34	Emergency Plans ***SHOULD*** be exercised and reviewed on a regular basis. [29, 31]
4.3.35	Emergency Plans ***SHOULD*** be distributed and controlled for key stakeholders. [29, 31]
4.3.36	Rail Entities ***SHOULD*** organise a programme of exercises at all levels to validate emergency plan content and roles and responsibilities within the plan. [29, 31]
4.3.37	Rail Entities ***SHOULD*** have a crisis management plan. [19]
4.3.38	Rail Entities ***SHOULD*** have arrangements in place to provide humanitarian support to those involved in or affected by major incidents. [26]
4.3.39	The person responsible for emergency planning within a Rail Entity ***SHOULD*** have the ability to develop documented arrangements for all aspects of dealing with emergencies, including but not limited to[19]: - • arrangements to ensure emergency plans are exercised and reviewed on a regular basis, • the organisation of an exercise programme at all levels, to validate emergency plan content and specifically roles and responsibilities within the plan, • arrangements to ensure emergency plans are distributed on a controlled basis to key stakeholders.[19]

Chapter 5. Training & Awareness | Testing & Exercising	
5.6.1	Rail Entities ***MUST*** ensure that recommendations of the RAIB are considered and acted upon, where appropriate within emergency planning arrangements. *This requires a person (or organisational body) to whom recommendations made by the Branch are addressed to ensure that these are considered and, where appropriate, acted on.* [20]
5.6.2	When designing exercises, relevant responder organisations ***MUST*** be included, and appropriate interoperability and single sector objectives ***SHOULD*** be built into the exercise design. [12]
5.6.3	Rail Entities ***SHOULD*** organise a programme of exercises at all levels to validate emergency plan content and roles and responsibilities within the plan. [19]
5.6.4	Rail Entities ***SHOULD*** include emergency response considerations during the design of enhancements and renewals. [21]
5.6.5	Rail Entities ***SHOULD*** test and exercise their emergency plans. [21]

5.6.6	Rail Entities ***SHOULD*** update emergency plans to reflect lesson learnt from published reports. Use lessons learnt to feed back into the cycle. [10]
5.6.7	Rail Entities ***SHOULD*** use lessons learnt from exercises to feed into a continuous improvement cycle. [10]
5.6.8	Rail Entities ***SHOULD*** use de-briefing sessions that are honest and open, with results disseminated widely. [10]
5.6.9	Rail Entities ***SHOULD*** partake in joint emergency response exercises. [10]
5.6.10	Rail Entities ***SHOULD*** deliver training courses, which are aligned to the JESIP learning outcomes framework and have multi-agency attendance in order to build and maintain an interoperable response. [12]
5.6.11	Rail Entities ***SHOULD*** ensure relevant responder organisations are included when designing Rail sector exercises, and appropriate interoperability and single sector objectives should be built into the exercise design. [12]
5.6.12	Rail Entities ***SHOULD*** where possible attend and contribute to LRF / LRP Training and Exercising working groups. [12]
5.6.13	Rail Entities ***SHOULD*** ensure their personnel, who are required to support the response to an incident, are appropriately prepared and aware of the JESIP models and principles, and how they are applied. To support this, everyone should receive a form of JESIP awareness training annually. In addition, individuals who are responsible for managing an incident at any level, should attend a multiagency JESIP training course, every three years as a minimum. [12]
5.6.14	Rail Entities ***SHOULD*** consider the inclusion of military participants in the planning and delivery of exercises where appropriate. [12]
5.6.15	Rail Entities ***COULD*** consider utilising Joint Organisational Learning (JOL) Online. Uploading all lessons identified from exercises, which affect a multi-agency response, and implementing lessons identified on JOL at the planning stage of the review cycle. Rail Entities ***SHOULD*** implement change at the local level, to reduce the risk of the lessons identified at exercises reoccurring during the response to an incident. [12]
5.6.16	Rail Entities ***SHOULD*** ensure the right people are always in the right place at the right time and there should be inbuilt resilience with some employees competent in both current and next roles. [13]
5.6.17	The organisation ***SHOULD*** use employee involvement to gather ideas for improvement and should put them into practice. [13]
5.6.18	The CMS ***SHOULD*** clearly consider operational competencies related to safety-critical work, referencing relevant legislation where necessary (e.g., ROGS). [13]
5.6.19	There ***SHOULD*** be a clear and well-defined link between the CMS and the need to maintain necessary organisational capability. [13]
5.6.20	Those who might be called on (as a Strategic Commander) to lead the response to Major Incidents on behalf of their organisations ***SHOULD*** be given appropriate training – both initial and on-going – for their role. [15]
5.6.21	Rail Entities Strategic Commanders ***SHOULD*** also be subject to periodic assessments of their continuing competence for the role, undertaken by an appropriate agency. [15]
5.6.22	Rail Entities ***SHOULD*** train, exercise, test and assess competency of Train Operator Liaison Officers (TOLOs) for recertification every 3 years. [17]
5.6.23	Rail Entities ***SHOULD*** maintain and enhance competency through participation in tabletop and live emergency exercises and maintain an exercise logbook. [17]
5.6.24	Rail Entities ***SHOULD*** determine who participates in exercises. [19]
5.6.25	Rail Entities ***SHOULD*** make arrangements for personnel to participate in exercises (internal and external). [19]
5.6.26	Rail Entities ***SHOULD*** capture issues arising from exercises. [19]

Chapter 6. Communication │Multi-Agency Partners	
6.2.1	Rail Entities ***MUST*** make their emergency plans available to aid cooperation and interoperability. [7, 28, 29]
6.2.2	Rail Entities ***MUST*** maintain arrangements to warn the public, and to provide information and advice to the public, if an emergency is likely to occur or has occurred. [7, 28, 29]
6.2.3	Rail Entities ***MUST*** collaborate with Local Resilience Forums (LRFs) and Local Resilience Partnerships (LRPs) to enable information and expertise sharing, enhance understanding of best-practices and current horizon scanning, real-time monitoring and data gathering activities. [7, 28, 29]
6.2.4	Rail Entities ***MUST*** be effectively represented, or effectively represented by another responder, at meetings of the Chief Officers Group for the Local Resilience Area, where reasonably practicable and if invited to do so by the relevant Category 1 Responders; in the case of any other meetings of a LRF/LRP any groups or sub-groups, or, where the general Category 2 responder exercises functions in London, a borough resilience forum, must consider whether it is appropriate for it to attend the meeting or to be effectively represented at the meeting by another responder. [7, 28, 29]
6.2.5	Rail Entities ***MUST*** ensure their warning and informing arrangements include the ability to communicate an incident [22]: a. Location b. Access/egress routes c. Date/time d. Any rolling stock involved, plus its route e. Incident timeline f. Casualties/fatalities g. No of passengers involved h. Damage caused i. Prevailing weather conditions j. Dangerous goods on-board k. Crew on-board l. Railway property owner m. Staff responsible for movement of the rolling stock n. Number and type of vehicles involved o. Emergency services in attendance p. Incident Commander's contact details
6.2.6	Rail Entities ***MUST*** notify the Branch of its occurrence immediately as it learns of the occurrence and by the quickest means available. [22]
6.2.7	Rail Entities ***MUST*** ensure emergency plans include the capability to communicate with vehicles. [22]
6.2.8	Rail Entities ***SHOULD*** ensure their emergency plans include the roles and responsibilities of partner agencies and that this is effectively communicated to them, including [21]: • BTP, • RAIB, • Network Rail, • TOCs, • LUL, • Local Authorities; and • Emergency Services.
6.2.9	Rail Entities ***SHOULD*** maintain plans for notification, communication, and response during an emergency. [23]
6.2.10	Rail Entities ***SHOULD*** have a formalised structure for internal information sharing. [19]
6.2.11	Rail Entities ***SHOULD*** have a formalised structure for internal information sharing. [19]

6.2.12	Rail Entities ***SHOULD*** prepare for the loss of IT services & telecommunications. [2]
6.2.13	Rail Entities ***SHOULD*** have a crisis communications plan. This plan should be updated in accordance with PR and communications policies within the organisation. [19]
6.2.14	Rail Entities ***COULD*** have a media communications plan developed in the event of media interest in an incident. [19]
6.2.15	Rail Entities ***SHOULD*** communicate lessons learned that are honest and open, with relevant stakeholders. [19]
6.2.16	When sharing information or communicating with other agencies, plain language that is free of abbreviations and jargon ***SHOULD*** be used. This ensures that the information shared is clear and easily understood. [12]
6.2.17	Information sharing ***SHOULD*** be fully collaborative both with direct collaborating organisations and others with relevant information and / or experience. [10]
6.2.18	Employees ***SHOULD*** be able to communicate any concerns and issues or identify improvements to information, instructions, standards and procedures. This should be acted upon by managers and feedback should be given promptly. [14]
6.2.19	The organisation ***SHOULD*** look at how other organisations communicate H&S information and implement best practice. [14]
6.2.20	There ***SHOULD*** be active pursuit of continuous improvement in communication within the organisation. [14]
6.2.21	There ***SHOULD*** be active attempts to continuously improve the two-way exchange of risk management information with collaborators. [14]
6.2.22	Effective risk management ***SHOULD*** be based on the provision of adequate information. [14]
6.2.23	The organisation ***SHOULD*** look to other sectors and countries to identify system-safety issues and controls. There ***SHOULD*** be evidence that this has led to continuous improvement. [14]
6.2.24	The procedures and standards ***SHOULD*** drive the organisation to strive for continuous improvement and ***SHOULD*** look for best practice from other industries in the UK and internationally. [14]
6.2.25	Best practice ***SHOULD*** be drawn from, implemented, and shared with other organisations in the UK and internationally. [14]
6.2.26	There ***SHOULD*** be arrangements for sharing information between organisations with shared H&S risks, in order to promote effective reviews and continual improvement. [14]
6.2.27	Rail Entities ***SHOULD*** communicate and disseminate extreme weather plans ahead of time. [16]
6.2.28	Rail Entity staff ***SHOULD*** be aware of changes to any extreme weather plans. [16]
6.2.29	Rail Entities ***SHOULD*** understand the implications of incidents and incident response on corporate reputation. [19]
6.2.30	Rail Entities ***SHOULD*** have a strategy to address corporate and reputation impact to include [19]: • Contact with the media • Social media usage • R&R for CMT • Stakeholder communications

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