Rail Delivery Group

National Rail

RDG Approved Code of Practice:
Rail Emergency Management Code of Practice with Guidance
Part A - Governance

RDG-OPS-ACOP- 008
Issue 2 – 18.09.2023

About this document

Explanatory note

The Rail Delivery Group 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 guidance note has been developed to support recommendations arising from the industry Rail Resilience Project (RRP) Emergency Management Review (completed June 2021) in that it describes a Code of Practice (CoP) for the governance of rail industry Integrated Emergency Management activity. The Code of Practice sets out requirements for effective IEM governance, in both local and pan-industry contexts, and provides guidance for rail infrastructure managers, passenger train and freight operators (the 'rail entity' or 'Rail Entities') with responsibility for the local implementation and management of IEM activities.

Issue record

Issue	Date	Comments
1	13.07.2023	First Draft
2	18.09.2023	Document Issue

This document is reviewed on a regular 3-year cycle.

Written by / Prepared by:

PA Consulting Ltd.

RDG RRP Delivery Team
Contact: Andrew Wade

The RRPWG and RRSG have representatives from the following Stakeholder groups:

- Train Operators
- Infrastructure Manager (Network Rail)
- TfL, TfW, Transport Scotland
- BTP
- DfT
- ORR
- GBRTT

Authorised by:

Rail Resilience Steering Group (RRSG)

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

Contents

About this document 2
Explanatory note 2
Executive summary 2
Issue record 2
Contents 3
1 Purpose and scope 5
1.1 Purpose 5
1.2 Background 5
1.3 Scope 5
2 Definitions 6
2.1 Definitions & Acronyms 6
2.2 Reading the 'provision' statements 8
3 The Rail Industry Resilience Landscape 9
3.1 The State of IEM and Resilience in The Rail Industry 9
3.2 Integrated Emergency Management (IEM) 10
4 Integrated Emergency Management Governance Principles and Structure 12
4.1 Principles 12
4.2 IEM Organisational Governance Structure 13
4.3 IEM Industry Governance Structure 16
5 Leadership, Competency and Responsibility Principle 19
5.1 Overview 19
5.2 Provisions and accompanying guidance 19
6 Awareness Principle 23
6.1 Overview 23
6.2 Horizon Scanning 23
6.3 Real-time monitoring 24
6.4 Data Gathering 24
6.5 Risk Assessments 24
6.6 Provisions and accompanying guidance 24
7 Culture and Maturity Principle 28
7.1 Culture 28
7.1.1 Overview ..... **Error! Bookmark not defined.**
7.1.2 Provisions and accompanying guidance ..... **Error! Bookmark not defined.**
7.2 Maturity 31
7.2.1 Overview ..... **Error! Bookmark not defined.**
7.2.2 Provisions and accompanying guidance ..... **Error! Bookmark not defined.**
8 Inclusive Engagement Principle 34
8.1 Overview 34
8.2 Provisions and accompanying guidance 34
9 Adaptation and Improvement Principle 37
9.1 Adaptation 37
9.2 Improvement 37

9.3 Provisions and accompanying guidance 37
10 References 40
11 Annex 41

1 Purpose and scope

1.1 Purpose

This Code of Practice and Guidance forms Part A of the Rail Emergency Management Code of Practice and Guidance.

This Code of Practice (CoP) sets out requirements, referred to within this document as 'provisions' (See Section 2.1 for definition), for the effective governance of Integrated Emergency Management (IEM). Accompanying these provisions are supporting guidance to enable practitioners, organisations, and industry to implement those requirements. The CoP applies to individual Rail Entities operating in the rail industry and at the pan-industry level.

The CoP contains a series of requirements. Supporting guidance accompanies each provision to enable practitioners, organisations, and industry to implement those requirements.

1.2 Background

This CoP has been formulated in response to 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) and the "Beast from the East" severe winter weather (February 2018). These resulted in fatalities, extensive disruption to passengers and significant negative publicity. Following these, the UK Cabinet Office asked the rail industry to carry out a review of its emergency management capabilities.

In early 2021 the RRP Review was set up and carried out by the rail industry under the sponsorship of the RDG. The report was submitted to industry and Cabinet Office in May 2021. It 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.

The Review identified a number of failings in the way that the rail industry carried out emergency management activities. It made nine overarching recommendations for improving industry emergency management. Of these, Recommendation 3 directly addressed the governance of emergency management, it stated:

"The industry must develop suitable structures to govern EM at both organisational and industry-wide level"

The responses to other recommendations from the review are also impacted by how Rail Entities, individually and collectively, govern their emergency management activities. It is therefore critical that the industry develops robust governance arrangements for emergency management. This requires **better integrating emergency management activities into existing Business-as-Usual (BAU) structures and processes** (e.g. risk management). Where necessary, new ways of working should be developed (e.g. developing a Pan-Industry approach to the operational, tactical and strategic coordination and oversight of emergency management activities).

1.3 Scope

This GN is applicable to all members of the Rail Delivery Group (RDG) that manage infrastructure or operate services over the mainland mainline GB rail network including 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 CoP in Rail as part of their process to achieve their safety licence.

2 Definitions

2.1 Definitions & Acronyms

Key definitions used in the text are described in the table below. 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.

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

Term	Definition in the context of this document
Category 1 & 2 Emergency 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 representatives of 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 and utility companies (UK Resilience Framework: December 2022).
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 framework for civil protection in the UK. The CCA identifies and establishes a clear set of roles and responsibilities for those involved in emergency preparation and response at the local level. It also allows for the making of temporary special legislation (emergency regulations) to help deal with the most serious of emergencies. (UK Resilience Framework: December 2022)
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)
Emergency	An emergency is defined as: 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)
Governance	Human-based system by which an organization is directed, overseen and held accountable for achieving its defined purpose (ISO37000:2021).
Governing Body	Person or group of people who have ultimate accountability for the whole organisation (ISO37000:2021).
Hazard	Hazards are non-malicious risks such as extreme weather events, accidents or the natural outbreak of disease. (UK Resilience Framework: December 2022)

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 Act) and also the voluntary sector, commerce and a wide range of communities. (Preparing Scotland – Scottish Guide on Resilience Chapter 3).
ORR RM3 Model	The ORR's RM3 (Risk Management Model), is a tool for assessing an organisation's ability to successfully manage health and safety 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 addressing specific topics, issues or providing guidelines and recommendations.
Rail Entity	Each passenger train and freight operating company running passenger or freight trains on, or infrastructure owner and manager of, mainline GB rail infrastructure (hereafter Rail Entity) must be compliant with due to the specific activities that they carry out. (RDG-OPS-GN-064)
Resilience	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 (ISO22371:2022).
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 (ISO31000:2018).
Risk Appetite	The amount of risk an individual, business, organisation or government is willing to tolerate. (UK Resilience Framework: December 2022)
Shock	Uncertain, abrupt or long-onset event, that has the potential to impact upon the purpose or objectives of an urban system (ISO 22371:2022).
Stakeholder	Person or organisation that can affect, or be affected by, or perceive itself to be affected by a decision or activity (ISO37000:2021).
Stress	Chronic and ongoing dynamic pressure originated within an urban system, with the potential for cumulative impacts on the ability and capacity of the system to achieve its objectives (ISO22371:2022).
Threat	Malicious risks such as acts of terrorism, hostile state activity and cyber crime. (UK Resilience Framework: December 2022)

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

Acronym	Full Form
BAU	Business-as-Usual
BTP	British Transport Police
BCM	Business Continuity Management
CCA	Civil Contingencies Act 2004
CoP	Code of Practice
DfT	Department for Transport
EM	Emergency Management

FOC	Freight Operating Companies
GALP	Group Assurance Letter Process
GBRTT	Great British Railways Transition Team
GN	Guidance Note
IEM	Integrated Emergency Management
ISO	International Organisation for Standardisation
LRF	Local Resilience Forum
LRP	Local Resilience Partnerships
LoA	Lines of Assurance
MD	Managing Director
MI	Management Information
NARU	National Ambulance Resilience Unit
NFCC	National Fire Chiefs Council
ORR	Office of the Rail Regulation
RACI	Responsible, Accountable, Consulted, Informed
RDG	Rail Delivery Group
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RSBB	Rail Safety and Standard Board
SMS	Safety Management System
TfW	Transport for Wales
TOC	Train Operating Company

2.2 How to read this Code of Practice

This Code of Practice is structured around five key principles that are set out in Section 5. These principles have been developed along similar lines to those used in relevant international standards e.g. BS67000:2019 City Resilience, that the authors are either familiar with or have contributed to.

For each Principle there are a series of 'provisions' that explain **what** is required (see next paragraph for further detail). Each provision has a 3-digit identifier e.g. 6.6.1 refers to the Civil Contingencies Act duty to cooperate. For each provision there is supporting guidance that explains **how** the provision should or could be delivered. The guidance statements have the same 3-digit identifier as their related provision by it is prefixed by 'G', thus G6.6.1 is the supporting guidance to provision 6.6.1.

Each provision statement contains a '**must'**, '**should**' or '**could**'. In the context of this CoP, this means that the Rail Entity/Entities or Rail Industry needs to carry out a specific activity (e.g. forming a particular working group or carrying out an assessment).

The terms are defined below:

Term	Definition
Must	This is a **legal requirement** e.g. compliance with the Civil Contingencies Act 2004 duty to cooperate. The relevant legislation will be stated.
Should	This is **good practice** based on various ISO/BS standards, existing industry good practice, examples of good practice from other industries (notably financial services operational resilience regulations) and academic/professional literature. The literature is supplemented by the expertise of experienced IEM practitioners.
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.

Table 1: *Definition of provision statements*

International standards (ISO, BS) as well as good practice guidelines consulted for this Code of Practice are listed in Section 6.

3 The Rail Industry Resilience Landscape

3.1 The State of IEM and Resilience in The Rail Industry

Rail industry IEM does not exist in isolation. IEM comprises several disciplines that collectively contribute to resilience in a rail entity or the wider industry. Network Rail recognises six main disciplines that make up the 'Resilience Landscape'. These have been accepted by RDG. Hence, they have been adopted for this Code of Practice and are:

- 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.

This IEM CoP repeatedly stresses the importance of inclusive engagement across the resilience disciplines. It is essential to embedding IEM/resilience objectives into overall business strategy and delivery. Cross-discipline engagement forms a key part of governance activities.

A short description of each resilience discipline (based on Network Rail's descriptors) and example activities is contained in **Table 2** below.

Resilience Discipline	Description	Example Activities
Enterprise Risk Management	Risk management helps Rail Entities to identify, understand and manage their threats, hazards, and opportunities (collectively known as risks) by providing a framework to assess their likelihood of occurring and potential impact on the organisation.	• Risk assessments affecting a whole Rail Entity • Processes for escalating risks through a rail entity
Security	Security is about people, processes and technology working together to keep railway businesses, assets, and the customer secure. This includes protection from terrorism, cyber threats, workforce violence and railway crime.	• Physical security measures at stations • Anti-workplace violence activities
Weather Resilience and Climate Change Adaptation	Weather and Climate Change Resilience is 'the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover' from adverse and extreme weather conditions and gradual or erratic changes in weather patterns due to climate change. Industry manages weather and climate change risks by strengthening assets to prevent damage, designing components to operate in a range of conditions, having backup or spare capacity and being prepared and getting back up and running quickly	• Seasonal weather preparedness • Horizon scanning to better understand the impact of climate on the railway • Designing new rolling stock to meet the likely weather patterns of the future, such as increased summer temperatures

Operational resilience	Operational Resilience involves working to prevent (where possible) and prepare for emergencies that may occur on our railway. Planning for emergency situations such as the Stonehaven landslide, immediate impact of severe weather, and/or terrorist attacks means we can respond to any emergency.	• Planning for incidents (e.g. derailments) • Planning for rail input to major public events (e.g. Op London Bridge)
Business Continuity	Business Continuity is the ability to maintain business/time critical services during and after a disruption has occurred. Planning helps organisations understand which services and assets are critical to the operation of their business so they can always maintain the delivery of the train timetable.	• Planning for internally driven disruption to rail services (e.g. industrial action) • Planning for externally driven disruption to critical activities (e.g. power outages)
IT Service Continuity	The loss of industry IT Services (or telecommunications systems) can have a huge impact on the railway's daily business. Planning for the recovery of critical systems at minimum agreed service levels and aligned to business priorities means we can continue to deliver essential services and meet regulatory obligations.	• Planning for disruption to IT systems, (e.g. loss of MS Teams for 24/48hrs)

__Table 2__: Overview of Resilience Disciplines and Definitions
__Source__: Network Rail – The Resilience Landscape at Network Rail

3.2 Integrated Emergency Management (IEM)

Integrated Emergency Management (IEM) is the framework adopted by UK government and Devolved Administrations for anticipating, assessing, 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 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:

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

IEM's key activities operate in a linked framework (see **Figure 1** 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 are then fed back into further **Preparedness** activity.

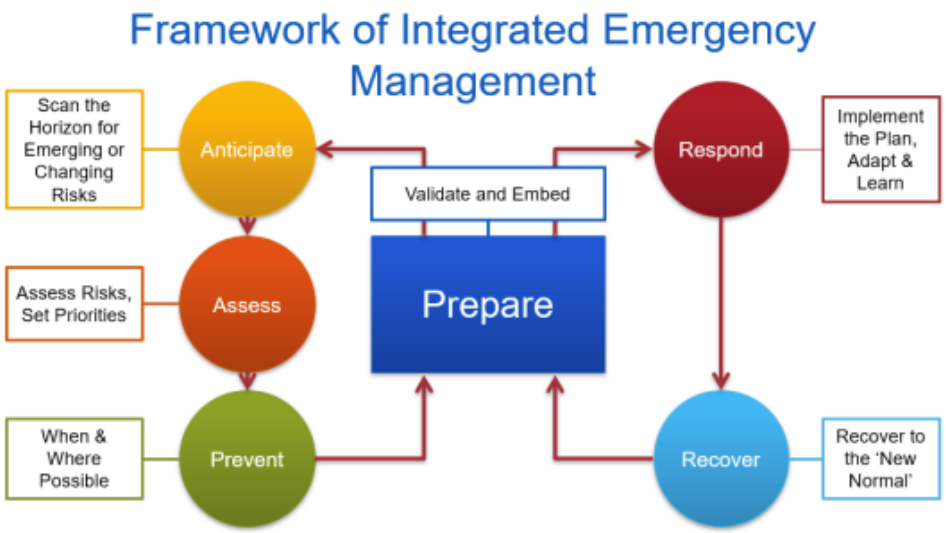

***Figure 1**: Framework of Integrated Emergency Management*
***Source**: Emergency Planning College*

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 activities of the organisation/industry.

4 Integrated Emergency Management Governance Principles and Structure

4.1 Principles

Underpinning effective IEM activity in the rail industry are five 'Principles for Integrated Emergency Management'. 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.

The five Principles for IEM in rail are:

- Leadership, Competency & Accountability
- Awareness
- Maturity & Culture
- Inclusive Engagement
- Adaptation & Improvement

These five principles will be used to structure the provisions and guidance for IEM contained in this Code of Practice.

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)
Culture & Maturity	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. Using a recognised and understood methodology based on ORR's RM3, entities should assess their current IEM 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.
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. Adapting and improving following disasters so that organisations can thrive, not just survive.

Table 3: IEM Principles and Definitions

4.2 IEM Organisational Governance Structure

Rail Entities are the ultimate legal duty holders for IEM. Individual Rail Entities must have in place a formal, documented structure and supporting processes to govern IEM activity. This will provide strategic direction to tactical managers, enabling them to make effective decisions on the implementation of IEM. In turn, this will enable IEM practitioners, and others with IEM responsibilities, to carry out their responsibilities at the operational level.

The governance structure should document:

- The organisational groups (working groups, committees etc) that direct, coordinate and deliver IEM activity at the different levels (operational, tactical, strategic) across the organisation
- The roles involved in IEM activity (both full and part-time)
- The reporting and management lines linking individuals and groups
- The processes that enable the governance structure to function
- Meeting agenda, cadence, and required attendees at each level

The IEM governance structure should be relevant for the context, size, and specific requirements of the organisation, and be integrated in the wider corporate business structure.

The following figure is a general description of key responsibilities and features at each level:

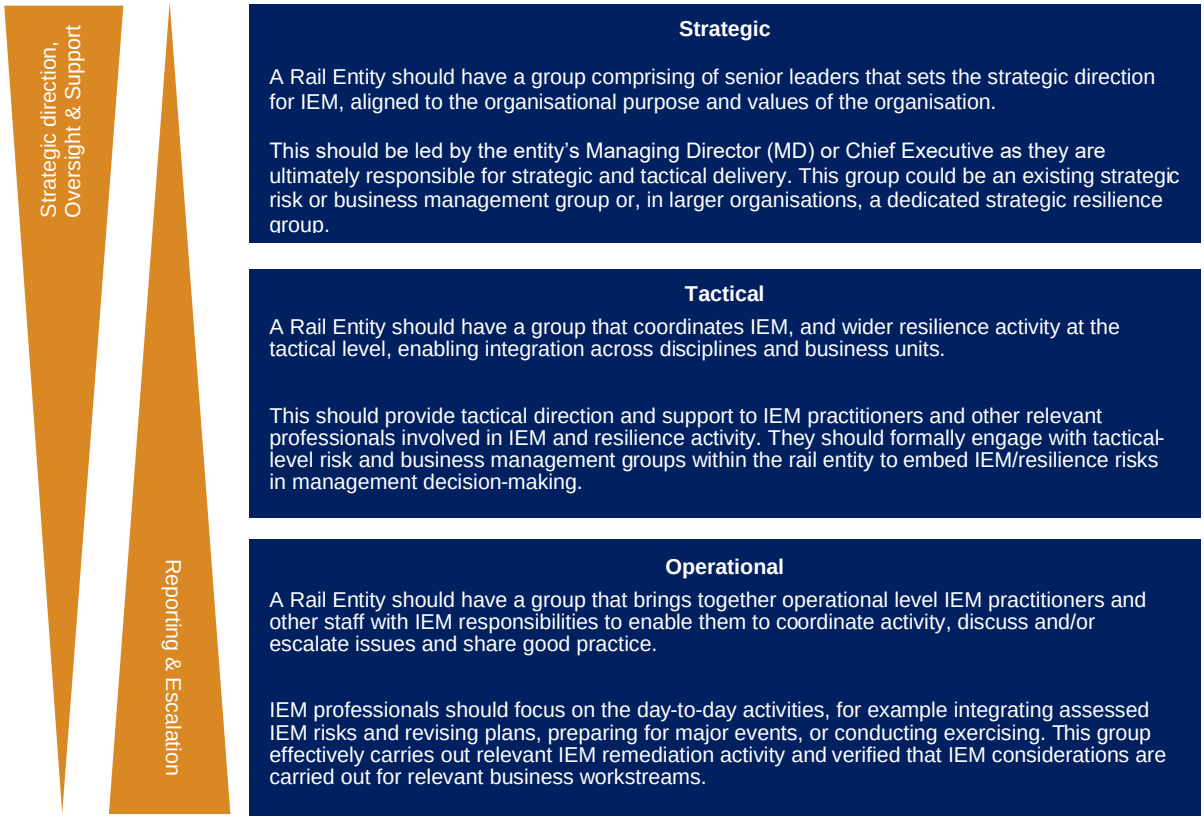

***Figure 2**: Overview of governance responsibilities at an operational, tactical, and strategic level.*

All groups should have clear and agreed Terms of Reference (ToR) that are reviewed at least annually by the membership of the group in question and the level above. In the case of the strategic group these ToR should be reviewed by the organisation's Senior Leadership or Board Audit & Risk Committee (or similar).

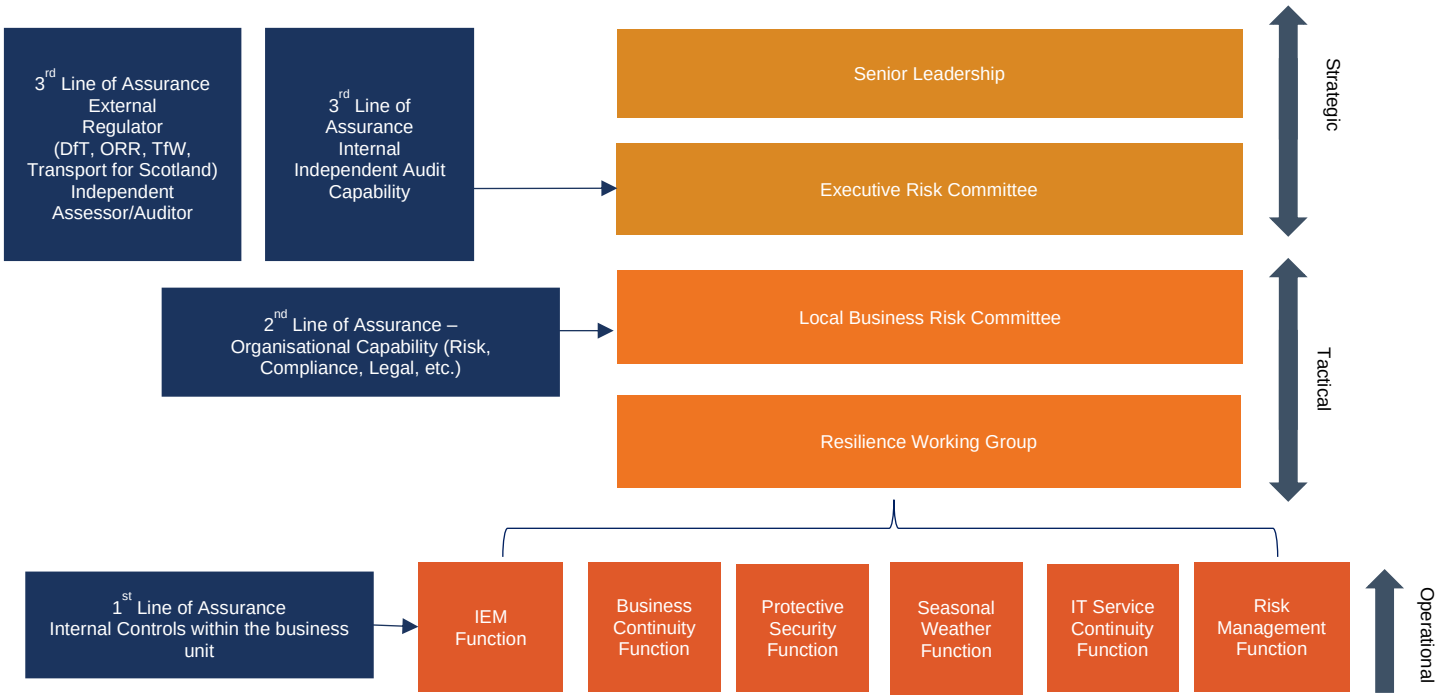

Figure 3: Governance Structure Example

Figure 3 includes a general example of a governance structure, outlining the key responsible bodies for delivering IEM across strategic, tactical, and operational levels. The agenda, required attendees, and cadence of meetings should be relevant and effective for each individual organisation depending on context, size, resources, and IEM requirements. This is described in more detail in the following paragraphs.

Table 4 provides an example of meetings cadence, agenda, and attendees based on the governance structure described above. This is not an exhaustive list of activities across the IEM framework; additional information on reporting requirements across the IEM governance structure can be found in Section 6, Awareness, Accompanying Guidance.

Governance	Cadence	Agenda	Attendees
Senior Leadership	Twice-yearly	• Set organisational resilience strategy and provide direction and high-level supervision on IEM activities • Resilience & IEM Policy approval • Set IEM risk appetite and tolerance levels • Oversee regulatory compliance and liaise with regulatory bodies, based on the recommendations of the Executive Risk Committee • Approve additional resilience investment needs for outstanding IEM/resilience risks escalated through governance • Review high level outputs of the horizon-scanning, real-time monitoring or data gathering activities to enhance awareness and set strategic direction • Review high level overviews of lessons learnt and ongoing high-profile remediation activity	Executive Management
Executive Risk Committee	Quarterly	• Review and approve implementation of organisation's IEM framework, policies and procedures	Members of the Executive Risk Committee,

		• Oversight and support IEM prevention and preparedness activities • Review of reporting provided by Third Line of Assurance, assessing ongoing programmes and outstanding vulnerabilities/risks • Review IEM additional investment requirements • Authorise additional investment or escalate to Senior Leadership for review of funding requirements to remedy outstanding IEM risks • Review high level outputs of the horizon-scanning, real-time monitoring or data gathering activities to enhance awareness and set strategic direction • Review high level overviews of lessons learnt and ongoing high-profile remediation activity • Report to the senior leadership	head of risk management, compliance, and relevant resilience functions. Relevant heads of business departments.
Local Business Risk Committee	Quarterly/ Monthly	• Review of IEM risk controls • Review audits, reports or assessments from Second Line of assurance • Integration of IEM prevention and preparedness activities into ongoing business workstreams • Escalate to Executive Business Risks Committee on resilience risks, and additional investment requirements	Business unit representatives, head of individual resilience functions, relevant SMEs
Resilience Working Group	Monthly	• Drive the implementation of the resilience strategy, focusing on identified resilience risks & opportunities • Integration of risks identified into prevention and preparedness activities (including IEM risks) • Enable integration of resilience disciplines • Monitor remediation activity for IEM risks • Advise Local Business Risks Committees on resilience risks, and additional investment requirements	Individual functions representatives, relevant support functions representatives (e.g., finance, IT, HR)
IEM Function	Monthly/Day-to-day operational requirements	• Review of IEM risks identified during horizon scanning, data gathering, real-time monitoring and risk assessments • Updates on Emergency Management Plans review, update and drafting as required • Review and allocation of relevant IEM risks remediation • Exercising planning, training gap analysis • Escalation of outstanding IEM requirements at Resilience WG or Local Business Risk Committees, including additional investment requirements	IEM practitioners, relevant SMEs (with IEM responsibilities)

Table 4: *Example of agenda, cadence, and attendees*

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.

- **1st Line of Assurance (1LoA)**: this level of assurance is provided by internal controls carried out by an individual or team who ultimately (whether directly or through a direct line) reports to the 'Accountable' or 'Decision Maker' role set out in the appropriate business unit IEM RACI. This type of assurance is typically carried out by operational staff. It should be reported to the business unit's senior leaders and made available to the rail entity's internal assurance and audit functions, including second and third lines of assurance. It involves identifying, monitoring and managing risks in the day-to-day.

- **2nd Line of Assurance (2LoA)**: this level of assurance is typically provided by risk management, compliance, legal, finance or other similar assurance departments. This line of assurance is set to carry out oversight on the first line of assurance, verifying the frameworks are effective and evaluating progress of ongoing remediation activity or IEM assessments. Evaluations and reviews should be conducted on an ongoing basis, agreed by the business, and should include monthly and quarterly reviews. Included in this line of assurance is the

annual maturity assessment referred to later in this Code of practice [See Section 5.2., Leadership, Competency and Responsibility]

- **3rd Line of Assurance (3LoA)**: this level of assurance is completely independent from the remainder of the organisation and is typically divided into internal and external assurance.

  The internal assurance is provided by an assessment carried out by a rail entity's independent audit or quality & assurance function. Outputs of these audits should be reviewed by the rail entity's relevant Executive Risk Committee, or equivalent relevant governing body. Such audits are conducted at a regular interval, established by the business, depending on compliance requirements and risk management framework. They should conduct continuous monitoring and include annual audit plans.

  The external oversight is typically provided usually by reviews or inspections carried out by a regulator e.g. by a DfT or ORR Inspector, or by a suitably qualified and competent independent advisor. This level of assurance is more in-depth than a simple, single site visit by an independent inspector e.g. a DfT inspection of a station under the transport security regulations and should not be conflated with those. The outputs should be shared with Lead Government Departments in central and devolved administrations.

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.

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

4.3 IEM Industry Governance Structure

RDG should, on behalf of the collective Rail Industry, mobilise and coordinate a formal, documented structure and supporting processes to provide oversight of IEM activity.

This structure should:

- Recognise that the ultimate duty holders for IEM and wider resilience activities are individual Rail Entities
- Provide oversight of industry IEM activity
- Enable the industry to take collective decisions (within the bounds of legal, regulatory, and organisational responsibilities)
- Enable collaboration/coordination between Rail Entities, regulators, and other key stakeholders
- Support benchmarking opportunities for individual Rail Entities
- Detail the processes for managing flows of information, requests for escalation, decisions, and actions between these bodies

Figure 4 outlines a suggested Pan-Industry Industry structure and responsibilities across strategic, tactical, and operational levels. **Table 5** provides an example of meetings cadence, agenda and attendees based on the Pan-Industry governance structure described above. While it is not an exhaustive list, it provides a suggestion for the Rail Industry to consider and continuously improve.

Pan-Industry Resilience Group (Strategic)

RDG should, on behalf of industry, mobilise and coordinate a pan-industry strategic resilience group. This group should coordinate and provide oversight of IEM activity across the industry.

It should engage in routine, and structured dialogue with industry regulators (DfT, ORR, TfW, Transport Scotland) regarding the strategic decisions impacting the future of the railway. This group should provide oversight of the annual IEM maturity and resource assessment, identifying areas for improvement and coordinating joint industry and stakeholder activity to deliver this.

Pan-Industry Resilience Group (Tactical)

RDG should, on behalf of industry, mobilise and coordinate a pan-industry resilience group at the tactical level. This group coordinates IEM activity across industry at the tactical level. It provides coordinated industry input to other stakeholders, sharing knowledge and enabling joint IEM activity where necessary.

It provides an opportunity for sharing good practice and industry benchmarking. It escalates risks and issues to the strategic group where necessary.

Pan-Industry Resilience Group (Operational)

RDG should mobilise and coordinate a best practice group bringing together representatives from the various resilience disciplines within Rail Entities and stakeholders.

This group provides opportunities for knowledge sharing and learning lessons. It should offer cross-discipline/rail entity benchmarking to encourage improvement. Where appropriate it should engage on operational IEM, and wider resilience matters, with external partners and regulators.

Figure 4: *Overview of pan- industry structure and responsibilities*

Governance	Cadence	Agenda	Attendees
Pan-Industry Resilience Group (Strategic)	Quarterly	• Provide oversight industry IEM and wider resilience performance • Provides oversight of the annual IEM maturity and resource assessment process • Review industry horizon scanning for IEM risks • Discuss/agree resilience input to strategic investment decisions • Provide collective industry views to central government and Devolved Administrations on UK resilience policy • Discuss impact of resilience regulatory regime on industry performance • Provide a strategic link between the resilience profession and wider industry performance • Considers matters escalated by the pan-industry tactical group	Elected Chair Strategic Representatives from: • RDG • TOC Owning Groups • FOCs • Infrastructure Managers • GBRTT • Chair, Pan-industry Resilience Group (Tactical) • BTP (ACC or above) • National Fire Chiefs Council (NFCC) • National Ambulance Resilience Unit (NARU) • DfT • Devolved Administrations • ORR • RSSB
Pan-Industry Resilience Group (Tactical)	Quarterly	• Provide tactical coordination of IEM activity across Rail Entities • Enable benchmarking of industry IEM and wider resilience performance • Enable coordination of industry IEM/resilience activity with external stakeholders	Elected Chair • RDG Operational Resilience Manager • TOC IEM Managers • FOC IEM Managers • Infrastructure Managers

		• Enable a dialogue and knowledge sharing between the rail industry and the emergency services • Provide opportunities for joint learning and knowledge sharing • Coordinate the rail industry engagement with Local Resilience Fora (Local Resilience Partnerships in Scotland) • Provide coordinated rail industry advice on tactical IEM/resilience matters to DfT, Devolved Administrations and other Lead Government Departments • Escalates risks and issues to the pan-industry strategic group where necessary • Provides pan-industry reports and/or information to the strategic group at their request	(IM) IEM Managers • BTP Head of Emergency Planning • Chair, Heads of Control Forum • Chair, RDG Policing & Security Implementation Group • Chair, Pan-industry Resilience Group (Tactical) Representatives from: • DfT • Devolved Administrations • NFCC • NARU • ORR • RSSB • Rail Entity Heads of BCM (or equivalent)
Pan-Industry Resilience Group (Operational)	Twice-yearly	• Provide coordination across different industry resilience disciplines • Provide a forum for cross-discipline engagement and knowledge sharing (including lessons learned) • Provide opportunities for benchmarking across organisations and disciplines	Elected Chair Representatives from: • Cross-industry IEM practitioners • Cross-industry BCM practitioners • Cross-industry Seasonal/Severe Weather practitioners • Cross-industry technology disaster recovery practitioners • Cross-industry security practitioners • Cross-industry risk management practitioners • Incident care Team Practitioners • Representatives from partners, regulators and stakeholders where appropriate

Table 5: *Overview of pan-industry agenda, cadence, and attendees*

5 Leadership, Competency and Responsibility Principle

***Principle**:* Leadership at all levels of an organisation is critical to successful IEM. Strategic leadership upholds 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.

5.1 Overview

Senior leaders are accountable ultimately for the performance of their organisation and this includes IEM. Responsibility for IEM is vested across all levels of a Rail Entity and everyone has a part to play. Senior leaders set the strategic direction and provide a mandate for IEM. Tactical managers and IEM professionals determine how to deliver against this mandate. Operational leaders deliver on the ground.

Rail Entities' Senior Leaders' direction and support for IEM are critical to its success and the delivery of the performance and cost benefits that derive from it. IEM, and wider resilience considerations should be integral to senior leaders' discussions. They should be considered in all significant business decisions, whether changing rolling stock, delivering a major renewal/maintenance scheme or in contributing to significant public occasions such as ceremonial events.

5.2 Provisions and accompanying guidance

Provisions

5.2.1 Rail Entities **must** have in place a Safety Management System (SMS) that sets out the distribution of responsibilities and how control of the SMS is maintained across different levels of management, (Railway and Other Guided Transport Systems (Safety) Regulations 2006) Schedule 1 paragraph 2(j) of ROGS applies these requirements to emergency planning/management activity.

5.2.2 Rail Entities Senior Leaders **should**:

- Communicate IEM principles, policies, and delivery plans across all levels of their organisations
- Monitor the performance of IEM activity, provide strategic oversight and allocate suitable and sufficient resources accordingly
- Be able to monitor compliance with legal obligations, with internal policies and how IEM contributes to achieving wider business objectives
- Provide assurance to stakeholders, regulators and the travelling public that IEM compliance obligations are being met
- Take ownership of IEM policy and strategic direction
- Advocate, promote and legitimise IEM activity within Rail Entities and the wider rail industry
- Remove barriers to IEM activity
- Promote IEM and wider resilience as enablers of organisational strategic objectives
- Appoint a named role with sufficient authority to direct IEM activity
- Provide accountability for IEM delivery across the organisation

5.2.3 A Rail Entity's Senior Leaders **should** formulate an over-arching resilience policy. This should communicate a clear mandate for, and direction to IEM activity across the organisation

that aligns with the needs and expectations of its stakeholders. This statement should outline the objectives, establish priorities, and provide direction for coordination and capability development across all relevant disciplines within the organisation.

5.2.4 Tactical leaders (often senior IEM professionals) **should** develop clear plans for implementing the strategic mandate/direction provided by an organisation's senior leadership. These plans should be communicated to operational leaders and staff to enable them to deliver activity.

5.2.5 Operational leaders **should** lead delivery activity by their teams to achieve the tactical plans and meet the Rail Entity's strategic direction and objectives.

5.2.6 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.

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

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

5.2.9 IEM **should** be included in an organisation's regular overall 3LoA assurance (self-) assessment process (where one is undertaken) e.g. the Network Rail Group Assurance Letter Process (GALP) or similar. The output of this process **should** be reported to shareholders and/or regulators.

5.2.10 Rail Entities **should** carry out and document a formal assessment of their IEM obligations, the maturity of their IEM capabilities, and available resources on an annual basis to enable better business planning for forthcoming years and drive continuous improvement in IEM capability. This formal assessment **should** be carried out by a rail entity's independent assurance function and is part of the 3rd Line of Assurance activity. The output of the assessment **should** be reviewed by the strategic pan-industry resilience group. [See Section 7, Culture & Maturity Principle]

Supporting Guidance

G5.2.1 Rail Entities should 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 organisations' SMS must include IEM activity throughout all its processes and provisions.

G5.2.2 Executive management level and/or Board support and direction for IEM is critical to organisations developing a strong culture of, and commitment to, effective IEM. Executive leaders should provide visible and consistent support to the whole framework of IEM activity encouraging the organisation to understand emergency management risks, focus on preventing these where possible and building the capacity to respond to and recover from disruptive events. Finally, they should encourage a learning culture enabling the organisation to learn from events and transform. [See Section 9, Adaptation & Improvement Principle].

G5.2.3 Rail Entities should have an over-arching resilience policy that:

- Sets out the organisation's strategic objectives and direction for resilience
- Includes a statement of executive-level support for resilience and its sub-disciplines
- Documents the organisation's 'resilience landscape', describing the various sub-disciplines (IEM, Business Continuity Management, Severe/Seasonal Weather Resilience etc) [See Section 3.1 above for further information] and how these interact
- Documents how collectively the resilience sub-disciplines contribute to the overall success of the organisation
- Documents the governance structure for resilience and its sub-disciplines including IEM

G5.2.4 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.

G5.2.5 Operational leaders lead/manage actual delivery activities by frontline staff following standard procedures and processes.

G5.2.6 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.

G5.2.7 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.

G5.2.8 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.

G5.2.9 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.

G5.2.10 In reviewing their IEM obligations, Rail Entities must give due regard to the Emergency Management Legal and Regulatory Register (RDG Guidance Note RDG-OPS-GN-064) that details minimum, legally required obligations. Rail Entities should also consider non-mandatory obligations arising from good practice and/or non-statutory guidance.

When assessing the maturity of their IEM capabilities Rail Entities should use an accepted and proven maturity assessment framework such as the ORR's RM3 framework.

When using the ORR RM3 framework to assess IEM capability, Rail Entities should consider and assess all relevant criteria from the assessment framework not just RCS5 Emergency Planning. Suggested minimum additional RM3 criteria that should be included are:

- SP1, SP3
- OC1, OC6
- PI1
- MRA2, MRA3, MRA4, MRA5

Additional detail supporting the RM3 maturity descriptors for emergency planning [RM3 RCS5] is included under Section 7 Culture & Maturity Principle in this Guidance Note.

Prior to commencing any maturity assessment, the Rail Entity's senior leaders should review and then confirm the target maturity level for all capabilities under assessment. These target maturity levels should be well known and understood throughout the organisation.

Rail Entities should, having reviewed their IEM obligations and assessed their actual vs desired IEM capability maturity, assess the resources (full and part-time) available and document a formal evaluation of whether these are sufficient.

6 Awareness Principle

Principle: *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).*

6.1 Overview

Awareness is the bedrock of IEM. It is built on a proactive and continuous process of data gathering to identify and assess risks and opportunities. It plays an essential role in prevention, preparedness, response, and recovery from disruption including shocks, incidents, crises, and longer-term stresses.

It is an enabler for effective IEM decision-making across all levels of governance and contributes to establishing a data-driven shared understanding of IEM posture and requirements across the organisation. Key IEM awareness activities include horizon scanning, real-time monitoring, data gathering and risk assessments.

Resilient organisations often adopt three distinct lenses to understand IEM data and leverage such information for strategic decision-making, namely **hindsight**, **insight**, and **foresight**.

- **Hindsight** enables organisations to learn from their past and recognise their weaknesses and strengths. It allows Rail Entities to leverage the available data to inform lessons learned and streamline continuous improvement activities. It enables adaptation and transformation.
- **Insight** implies an actual and current understanding of ongoing IEM challenges. This enables immediate or short-term action and remediation.
- **Foresight** is the key strategic enabler for adaptation and transformation. It enables the mitigation of future disruption or shocks. It also enables the optimisation or exploitation of opportunities. This brings prosperity and maximises value for the organisation.

These three lenses on awareness should be kept in mind when considering the provisions contained in this CoP and their information needs.

Awareness governance is built on documented and functioning processes that enable the reporting of IEM requirements. In this context, IEM Management Information (MI) reporting is a key instrument to capture and analyse the relevant data, as described above, and report, challenge and escalate requirements. This should take place across all levels, from operational to strategic.

Each governing body, or responsible individuals, should produce or receive the type and quality of reporting, to the best of the capability of the organisation, required to inform their decision making and actions. They should also leverage such information to monitor progress of IEM programmes towards the strategic objectives of the organisation as well as provide assurance for ongoing ordinary workstreams and remediation activity.

6.2 Horizon Scanning

Horizon scanning is a systematic examination of information and data to identify potential threats, risks, and opportunities, beyond the short term, allowing for improved preparedness and the incorporation of mitigation measures into the decision-making process. It is an iterative process aimed at informing the long-term IEM and resilience strategy of an organisation and is inherently forward looking.

Horizon scanning should include an average timeframe from five to ten years in the future depending on the requirements of the individual organisation. It should encompass a broad scope to enable an all-round view of potential developments of the external context, from political to social, environmental, regulatory, security and economic emerging trends.

6.3 Real-time monitoring

Real time monitoring and reporting is a process enabling the collection, tracking, and sharing of data immediately after its collection. This should enable organisations to monitor disruption, shocks, or incidents as they unfold and act on the information provided. Use of real-time data should enable a shared situational awareness and facilitate information-sharing, enabling early-warning and facilitating assessment, prevention, and preparedness activities. Automation and information sharing greatly enable acting upon real-time data and enhance adaptable and dynamic decision-making IEM mechanisms.

6.4 Data Gathering

Data Gathering is a process involving the collection, storage, analysis and distribution of data and information providing an actual, relevant, and useful insight into current potential risks, disruption, shocks or the performance and audit of existing IEM and resilience programmes.

6.5 Risk Assessments

Risk assessments should be a systematic and iterative process, effectively informing both short- and long-term IEM, and wider business decision-making. It should include an overall process of risk identification, analysis, and evaluation, enabling data-driven and informed risk treatment measures as well as maximising opportunities.

6.6 Provisions and accompanying guidance

Provisions

6.6.1 Under the Civil Contingencies Act 2004, Rail Entities **must** co-operate with each relevant general Category 1 and Category 2 responders in connection with the performance by the respective responder of its duties under section 2(1). Such cooperation must include the provision of all necessary information for the general Category 1 and Category 2 responders to perform their functions.

6.6.2 Under the Civil Contingencies Act 2004, the Rail industry **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. This greatly facilitates prevention and preparedness workstreams, align risks identified in the community with approach of the rail industry and enhances risk management practices.

6.6.3 Rail Entities **should** individually conduct horizon scanning, real-time monitoring, data gathering activities and risk assessments within a defined systematic process, understood data and information sources and methodology. This process should be relevant to the identified stakeholders and applicable to the context and size of the organisation.

6.6.4 Rail Entities **should** integrate horizon scanning, real-time monitoring, data gathering into Business-as-Usual processes, effectively leveraging their assessment of risks, shocks, stresses, and drivers to take informed decisions across the entire IEM framework and wider business activities.

6.6.5 There **should** be a documented mechanism and clear MI reporting requirements for horizon scanning, real-time monitoring, data gathering and risk assessments outputs across the governance structure. This process **should** also enable reporting and decision-making on IEM by the relevant governing body. Decisions should be made in line with the rail entity's appetite for, and tolerance of, risk.

6.6.6 Rail Entities **should** develop a suite of IEM performance indicators. These enable managers across all levels of the business to quantify the organisation's ongoing IEM performance. The KPIs should contribute to assurance activity across all three levels and the annual assessment of IEM maturity and resourcing.

6.6.7 Rail Entities **could** consider implementing an automation process, appropriate for the size and complexity of the organisation, to enable real-time data collection and sharing.

Supporting Guidance

Horizon scanning, real-time data, risk assessments and data gathering follow the same process for integration into IEM and wider business governance. This includes:

G6.6.1 Rail Entities must have a documented and standardised process to cooperate with relevant Category 1 and other Category 2 responders, enabling such entities to perform their duties listed under Section 2(1) of the 2004 Civil Contingencies Act. This includes assessing the risk of an emergency occurring as well emergency planning, prevention, and mitigation activities.

Rail Entities must:

- Have documented procedures for co-operation activities under this provision, including pre-established agreements setting out scope, requirements, resourcing, and accountability for the processes
- Assign clear roles and responsibilities for conducting awareness activities with relevant Category 1 and Category 2 responders, under the direction, guidance, and support of the relevant governing body
- Identify the relevant stakeholders from Category 1 and Category 2 responders and establish clear communication channels
- Collaborate with Category 1 or other Category 2 responders in conducting and sharing the outcome of IEM risk assessments, enabling an understanding of potential risks and vulnerabilities. This will facilitate streamlining and coordinating prevention and preparedness activities involving multiple stakeholders across the relevant geographies
- Implement clear procedures for escalating or sharing requirements, including where applicable sharing the output of horizon scanning, IEM risk assessments, data gathering or real-time monitoring

G6.6.2 Rail Entities must collaborate with LRFs/LRPs to enable information and expertise sharing. To meet this requirement, Rail Entities must:

- Enable effective representation as indicated under the Civil Contingencies Act 2004 within the relevant areas of the rail entity and regular attendance to relevant LRF meetings, workshops or working sessions. [See also Section 8, Inclusive Engagement]
- Have a process to provide information on identified IEM risks, horizon scanning, data gathering or real-time monitoring activities within the relevant sector in so far as it would enable the relevant stakeholders to perform their duties as indicated in the Civil Contingencies Act 2004, including for planning, prevention, preparedness or exercising
- Collaborate with the LRFs/LRPs in conducting local risk assessments, providing their expertise and sector insight to allow the right resourcing, planning or mitigation measures are incorporated
- Facilitate sharing lessons learnt with relevant stakeholders in the LRF and enable collective learning and improvement across the industry and relevant communities [See Section 9, Adaptation and Improvement Principle]

G6.6.3 Rail Entities should define, establish, and regularly review and improve a systematic process for horizon scanning, IEM risk assessments, real-time monitoring and data gathering.

This includes:

- An agreed methodology for conducting such activities, understood, and shared by the entire organisation. This should cover scope, identified risks and hazards as well as specific timeframes – informing effective identification and review of data sources
- Relevant professionals should leverage industry best practice and promote a shared understanding of ongoing activities across the organisation

- Clear roles, responsibilities, and accountability for conducting such activities and communicating the outputs and requirements to relevant stakeholders across the governance structure
- Relevant professionals should regularly map internal and external stakeholders to inform scope and requirements of the activities and distribute the outputs to all IEM stakeholders
- Resourcing should be proportionate and should reflect the size, complexity, and profile of the organisation

G6.6.4 IEM Governance should include a mechanism to systematically incorporate into BAU activities the output from risk assessments, horizon scanning, real-time monitoring and data gathering across the IEM framework. Data-driven decision-making relies on effective MI across all levels of the governance structure. Based on the guide to MI published by the Financial Conduct Authority (FCA), key principles for producing effective MI include:

- **Consistency**: reporting is produced and distributed at a regular interval
- **Relevance**: the information provided should be relevant to the role and responsibilities of the relevant governance body
- **Timeliness**: Information should be produced to relevant stakeholders in a timely fashion, ensuring there is sufficient time allocated for MI to be distributed, reviewed, and challenged across the governance structure
- **Accuracy**: information should be correct and provided by the competent or responsible professionals

MI requirements vary greatly across organisations, and they should be tailored to the size, complexity, and context of operations. The below includes general guidelines and guidance on how MI might be conducted:

Operational (IEM function): At an operational level, MI could include:

- **Hindsight**: Monitoring and reporting on IEM performance metrics and incident reporting. Reporting on lessons learnt, ongoing remediation programmes and outstanding requirements for escalation to tactical. Reporting on lessons learnt during regular exercising.

- **Insight**: Reporting of outstanding IEM risks, falling outside the organisational risk appetite, requiring escalation to tactical. Reporting of outstanding vulnerabilities, with clear ownership and tracking of remediation or mitigation activity. Reporting on requirements to verify regulatory compliance

- **Foresight**: Reporting of horizon scanning, real-time monitoring, data gathering and IEM risk assessments and implications for IEM planning and exercising. The MI should include an overview of risks, shocks, stresses identified during relevant awareness activities, and link the outputs to the wider planned activities in the IEM framework (especially prevention and preparedness)

Tactical (Resilience Working Group/Business Risk Committees): At a tactical level, MI could include:

- **Hindsight**: Overview of current performance against agreed IEM medium to long term objectives and significant incidents. Oversight and monitoring of remediation activities, outputs from lessons learnt, current IEM and wider resilience disciplines against organisational policies and standard and current regulatory requirements

- **Insight**: Resource requirements and availability to conduct IEM planning, as well as prevention, preparedness, and exercising activities. Collaboration between IEM professionals and relevant local business heads to discuss IEM requirements for ordinary and extraordinary business workstreams. Review and assessment of outstanding IEM risks, falling outside the organisational risk appetite as reported by operational, and escalation of investment requirements to the executive committees. Monitoring of ongoing and future exercising programmes

- **Foresight**: Alignment of IEM horizon scanning, real-time monitoring, risk assessments and data gathering activities with wider resilience disciplines. Oversight and monitoring of the overall performance of the resilience and IEM programmes at a local business unit level

Strategic (Executive Committee/Strategic Leadership): At a strategic level, MI could include:

- **Hindsight**: High level overview of IEM performance against the strategic and long-term objectives of the organisation, and significant or critical incidents. Monitoring of ongoing remediation activity, identified during both regular assessments and following lessons learnt

- **Insight:** High level assessment of IEM considerations for ordinary and extraordinary business workstreams, relevant for the attention of senior executives. Review and assessment of outstanding IEM risks, falling outside the organisational risk appetite as reported by tactical, to enable decision making on IEM risk acceptance or review and approval of additional resource requirements

- **Foresight**: High level overview of output of IEM horizon scanning, real-time monitoring, risk assessments and data gathering activities. Long-term strategic planning and alignment to organisational values, leveraging horizon scanning and IEM risk assessments to inform decision-making. Effective preventive decisions on risk acceptance or authorisation/escalation of additional investments to remedy relevant outstanding IEM risks

The above overview provides an example of relevant IEM MI reporting requirements and a guideline for streamlining identified risks during the anticipation and assessment phases into effective prevention and preparation activities across the governance structure. The agenda, cadence, attendees, MI requirements for awareness activities should be tailored to the individual organisation.

G6.6.5 Rail Entities suite of performance indicators (and supporting management information) should help managers at all levels of the organisation to monitor and understand IEM performance. These performance indicators should be structured to allow for progressively deeper granularity to enable the root cause of performance to be understood and to align with individual, team and department-level performance assessment. The KPIs and management information should contribute to assurance activities – both ongoing and periodic.

G6.6.6 Key Performance Indicators for IEM activities are detailed in a separate RRP guidance document.

7 Culture and Maturity Principle

***Principle**: 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.*

Using a recognised and understood methodology based on ORR's RM3, entities should assess their current IEM 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.

7.1 Culture

7.1.1 Overview

An organisation's culture is defined by its shared attitudes, behaviours, and values. The attitude towards resilience determines how things are delivered, communicated and how individuals are encouraged to support the delivery. To engage individuals in IEM and resilience each rail entity needs to develop a culture of resilience, setting the tone from senior leaders of the importance of IEM and associated resilience activities.

Rail Entities should design an approach to IEM and resilience that is at the heart of the culture. It should align with the existing organisational norms, leadership, communication, and engagement approaches.

7.1.2 Provisions and accompanying guidance

Provisions

7.1.2.1 Senior Leaders of Rail Entities **should** instil in the organisation a culture that promotes both organisational resilience and a resilient workforce.

7.1.2.2 Senior Leaders of Rail Entities **should** set the appropriate tone by endorsing the IEM and resilience policy and approach.

7.1.2.3 Senior Leaders of Rail Entities **should** continually encourage and emphasise the importance of IEM and resilience by exhibiting behaviours that demonstrate resilient mindset and culture.

7.1.2.4 Senior Leaders of Rail Entities **should** provide direction to all individuals in the organisation to conduct activities within the IEM and resilience policy and framework.

7.1.2.5 The resilience and IEM policy and frameworks **should** be aligned to the mission and strategy of the rail entity and aligned initiatives and programmes.

7.1.2.6 Roles and responsibilities of individuals responsible for and delivering IEM and resilience activities **should** be defined in the policy and approach to provide clear ownership.

7.1.2.7 Individuals **should** be provided with relevant resources to deliver these activities and wider resilience awareness initiatives alongside other roles and responsibilities.

7.1.2.8 The IEM governance structure **should** support two-way communication providing individuals and leadership with voice on IEM and resilience [See Section 8.2, Inclusive Engagement].

7.1.2.9 Rail Entities **should** make a statement on the importance of a resilience culture in the IEM and resilience policy including a requirement to assess cultural maturity.

7.1.2.10 Rail Entities **should** empower decision-making and ownership of resilience at every level of the organisation.

7.1.2.11 Rail Entities **should** identify a desired maturity state for the resilience culture, regularly review appropriate indicators and monitor the existing culture on at least an annual basis.

7.1.2.12 Rail Entities **should** identify IEM and resilience champions to lead resilience awareness activities and initiatives at different levels of the organisation.

7.1.2.13 Rail Entities **could** implement a change program focussed on embedding a resilience mindset throughout the organisation.

Supporting Guidance

G7.1.2.1 Creating and sustaining a culture of resilience requires an approach that is integrated with the rail entity approach to delivering the business. IEM and resilience need to be designed to align to existing systems and process, they need to align to attitudes, behaviours, and values, and it needs to be continual focus of the rail entity. This guidance note refers also to Provisions

Developing and empowering a culture of resilience requires establishing appropriate policies and structures to promote resilience, providing individuals with the opportunities to talk about IEM and making resilience part of everyday life and operations.

Rail Entities should consider each element in developing a resilience culture. **Figure 6** outlines guidance for developing and promoting a culture of IEM and resilience in a rail entity. This guidance note refers also to Provision 7.1.2.2, 7.1.2.3, 7.1.2.4, 7.1.2.13.

DESIGN THE SYSTEM	CONNECT WITH HEARTS	NUDGE THE RIGHT HABITS
Systems, processes, and structures are some of the most fundamental drivers of behaviours across an organisation. Ensuring you purposefully design these to provide a consistent message will reinforce that IEM is something you care about getting right and help drive the desired behaviours. **Ask yourself:** Do your policies, organisational structures, and governance clearly promote IEM and resilience requirements? Are your processes easy to follow, or do they prevent colleagues from being effective in their primary role?	Individuals need to feel comfortable talking about IEM and resilience and how it relates to them both inside and outside of work. Helping colleagues to realise that good IEM and resilience knowledge and skills will keep themselves and their families safe at home as well as protecting the organisation can be very powerful. **Ask yourself:** Do you talk about IEM and resilience as a core component of managing business risk? Is IEM owned and championed at board level? Do leaders and managers role-model the right attitudes and behaviours when it comes to resilience?	When it comes creating a culture of IEM and Resilience, continual nudges will create engagement. Simple strategies such as making IEM part of ways of working to reduce the hassle factor of adopting new behaviours and providing practical and regular reminders will drive changes in attitudes and behaviours. **Ask yourself:** Do we talk about IEM and resilience in team meetings and other regular discussions? Are we incorporating IEM and resilience into our ways of working? Are we using communication channels to create a drumbeat of messages around the importance of IEM and resilience

***Figure 6**: Guidance for developing and promoting a culture of IEM*

G7.1.2.2 The IEM policy for each Rail Entity should set the expectations for the resilience culture, empowering the organisation from senior leaders. The policy should define roles and responsibilities each level of the organisation to support creating a culture of resilience and be signed off by senior leaders. This guidance note refers also to Provisions 7.1.2.5, 7.1.2.6, 7.1.2.7.

G7.1.2.3 Rail Entities should empower decision-making and ownership of resilience at every level of the organisation. This requires staff training and a cultural change programme to instil a resilience mindset and culture with staff. Fostering a no-blame culture where staff feel safe to fail and learn. Decision making should be devolved to the lowest appropriate level to develop employee empowerment. This guidance note refers also to Provisions 7.2.2.8, 7.1.2.9, 7.1.2.10.

G7.1.2.4 Using the ORR RM3 methodology, as outlined in Section 7.2 Maturity Principle, Rail Entities should initially assess the maturity of their resilience and IEM culture and establish a desired level of maturity. Their progress towards this should be monitored annually using surveys and check-ins as indicators of change. This guidance note refers also to Provision 7.1.2.11.

G7.1.2.5 Rail Entities should identify resilience champions to provide additional resource to engage the wider organisation in IEM and resilience. Champions will be able to lead activities to raise awareness across the entity, this could include:

- Webinars / seminars
- Annual campaigns to promote resilience and IEM activities
- Lunch and learns focussed on particular topics or events
- Participating in national preparedness campaigns

They will be focal points across the entity supporting all levels of the organisation in creating a drum beat around resilience. This guidance note refers also to Provision 7.1.2.12.

7.2 Maturity

7.2.1 Overview

Maturity will vary across each principle and between entities. Resilience should be assessed to understand whether the maturity meets the internal and external expectations of the entity's stakeholders. The desired maturity should be based the entity's regulatory requirements and board strategy. Using a recognised and understood methodology based on ORR's RM3, 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.

To achieve the desired maturity level Rail Entities will need to create a culture of resilience that promotes IEM and resilience approaches and behaviours. Senior Leaders' direction and endorsement for such activity should be provided in the resilience/IEM policy and framework. Defining clear parameters for success, enabling, and encouraging ownership of IEM is imperative. Agreeing activity across organisational grades and boundaries and dedicating relevant resourcing for appropriate resilience awareness activities is essential.

7.2.2 Provisions and accompanying guidance

Provisions

7.2.2.1 RDG, on behalf of the industry, should develop enhanced assessment criteria to support the application of ORR's RM3 model to IEM.

7.2.2.2 The Rail Industry **should** agree the categories, within which maturity will be measured. Each category should have appropriately defined metric (the suggested example uses people, processes etc).

7.2.2.3 The Rail Industry **should** require each entity to undertake a regular documented assessment of maturity [See Section 5 Leadership, Competence and Responsibility Principle]

7.2.2.4 Rail Entities **should** agree what level of the maturity framework (Ad Hoc, Managed etc.) is acceptable to them. The industry should collectively agree whether the target maturity level should be the same throughout the industry, or whether there can be variations.

7.2.2.5 The Rail Industry **should** clarify the type of exercising or other activity each entity should carry out to determine current maturity against the framework.

7.2.2.6 Rail Entities **should** then define a plan/programme to mitigate gaps in maturity against requirements agreed. This programme **should** record the timescales to carry out the documented assessment, exercising and mitigation planning required to reach the desired maturity level.

Supporting Guidance

G7.2.2.1 The maturity model is based on the Capability Maturity Model Integration (CMMI). The CMMI is a methodology developed by a US university to enable organisations to measure, build and improve capabilities in order to drive overall performance improvement. This framework model has been chosen as it aligns well with the ORR RM3 methodology. Below is an example of this maturity model using six categories (people, processes, technology, locations, suppliers, and data/information) and maturity level based on the ORR's RM3 methodology. A complete and more accessible version of this table can be found in Section 11, Annex.

	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 have 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.

For the purposes of reflecting our current understanding and to describe future areas for improvement, the processes described here at each level are examples and are not exhaustive.

Figure 5: *Guidance on IEM Maturity*

G7.2.2.2 The criteria developed should enable a greater degree of detail and clarity in the assessment of IEM maturity. Criteria should be aligned to the provisions with the Code of Practice for Emergency Planning in rail and/or relevant legislation (e.g. the Data Protection Act must be considered in maturity for Data/ Information). To reach the level of "Excellence", criteria should be met consistently for a specified time period. In the case of the example described later this is set at 12+ months. The maturity levels taken from the ORR RM3 methodology should be retained for consistency.

- **Ad Hoc:** tasks are not organised to be repeatable. Performance is uncertain and unpredictable
- **Managed**: organised to provide repeatable performance. Similar tasks might be performed differently
- **Standardised**: similar task are performed in the same way
- **Predictable**: delivery can be predicted by the management system. Variation and change are controlled
- **Excellence**: Proactive and continual improvement

The model enables organisations to measure, build, and improve capabilities—to improve overall performance. Each entity could use the model to demonstrate maturity levels to external stakeholders, such as regulators, and the wider ecosystem of suppliers

The categories used to support the maturity levels should be consistent across the industry. The worked example suggests the following categories – People, Processes, Technology, Places, Suppliers, Information / data.

- **People**: What is expected of people throughout the organisation. Each will have different responsibilities, training requirements, contractual obligations, annual objectives, and amount of time focussed on emergency planning
- **Processes**: This should provide a guide to assessing the frequency, documentation, and repetitive nature of existing processes. Indicating the expectation at each stage of maturity
- **Technology**: Consideration should be given to the level of technology used, the way it is used and how technology is secured
- **Locations**: Locations require physical security and can be used as physical back-ups. The maturity of how physical locations are used and maintained, should be assessed against agreed criteria, relevant for each entity
- **Suppliers**: Looking at the wider supplier network, how do external parties contribute or affect Emergency Management for each entity. How can you evaluate that maturity?
- **Information / Data:** This category looks at the maturity of the information being handled by each entity. Entities should agree on whether they want to use 'Information' or 'Data' as a title for this section. Depending on the language they currently use

G7.2.2.3 See Section 5 Leadership, Competency and Responsibility Principle for guidance on the annual maturity assessment process. This process should use the enhanced RM3 maturity model developed under the provisions in this chapter.

G7.2.2.4 A Rail Entity should agree and document its maturity expectations for each category. The Entity should record the rationale for its decision(s). The IEM maturity expectations should be widely known and discussed throughout the organisation. They should form part of senior leaders' discussions and be subject to regular review. RDG should lead industry discussions regarding whether target maturity levels should be the same across industry.

G7.2.2.5 The Rail Industry should collectively identify the different activities that can be used by Rail Entities to demonstrate that they meet the various maturity levels. This might include carrying or tests or exercises, producing documentary evidence (meetings minutes etc) or third-party reviews.

G7.2.2.6 For this type of maturity model, each of the requirements listed need to be met for the category (e.g. people, process) to be defined as reaching the specified level of maturity (e.g. Measured). It will be the case that categories are at different levels of maturity. That is to be expected. Ideally each category would be brought up to the same level of maturity before developing further. But this is not strictly necessary.

Rail Entities should agree and document the timescales for reaching target levels of IEM maturity. This should include, where necessary, the balance to be struck between making improvements and coordinating different levels of maturity. (e.g. focusing on technology at the exclusion of process / training, will not deliver the required improvements to resilience).

Rail Entities should development and document a programme of work to enable them to reach their target IEM maturity level. This programme plan should comply with the Entity's BAU project/programme methodology including governance and reporting arrangements. This is required at each level and for each category in the maturity model should be adapted for each entity:

- Each entity should tailor a specific version of the model relevant for their needs. The model will then provide specific, clear and achievable goals for each level of maturity
- Each entity should agree a desired maturity level and timescales to reach that level

8 Inclusive Engagement Principle

***Principle**: Inclusive engagement helps to build consensus, trust, and an integrated approach to resilience across disciplines and organisational boundaries.*

8.1 Overview

Inclusive engagement is a key enabler for effective IEM governance. It is built on continuous stakeholder engagement, transparent communication, as well as community and industry collaboration.

Bringing together professionals, members of the organisations and wider industry with a varied background and expertise is essential for IEM programmes to reflect the current challenges of the organisation. This process should extend beyond the traditional EM or resilience professions. It should include all relevant stakeholders within the organisation (e.g. infrastructure managers' project sponsors responsible for upgrade projects or TOC driver managers), and the community. This should be done though an inclusive stakeholder engagement, with a clear strategic direction and support from Senior Leaders.

Inclusive engagement should also enable an integration of the needs of all relevant members of the community across the IEM framework. This should include vulnerable individuals that may be impacted by disruption that affects the railway.

8.2 Provisions and accompanying guidance

Provisions

8.2.1 Under the Civil Contingencies Act 2004, 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.

8.2.2 Rail Entities **must** comply with inclusivity legislation during all five phases of the IEM framework.

8.2.3 Senior Leadership **should** provide direction to relevant individuals or governing body to conduct stakeholder engagement and provide the required endorsement, support, and resourcing for such activity.

8.2.4 Rail Entities **should** have a clear process to identify and involve relevant stakeholders across the five phases of the IEM framework. The process should consider a variety of internal and external stakeholders, adopting a whole-system approach to stakeholder mapping and engagement.

8.2.5 Rail Entities **should** integrate IEM with wider resilience disciplines, including but not limited to Protective Security, Business Continuity, Weather Resilience, IT Service Continuity and Risk Management.

8.2.6 Rail Entities **should** have a documented process to involve IEM professionals in strategic planning and business change, allowing for review and appropriate IEM considerations and plans to be implemented in a timely manner.

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

Supporting Guidance

G8.2.1 Rail Entities must have a mechanism in place that provides for effective representation in the LRFs/LRPs. This must include:

- One or more designated individuals (depending on the specific requirements of the organisation) formally tasked as point of contact and ensuring effective representation at

the LRFs/LRPs. This should be included in job descriptions and be part of the regular performance appraisals of the professional(s)
- Clear and regularly updated two-way communication channels
- Relevant individuals are provided with adequate resources to engage with the LRFs. For example, this includes allocating sufficient time to participate in meetings, prepare MI to facilitate information-sharing and engagement, as well as collaborate on awareness activities (horizon scanning, real-time monitoring, data gathering or risk assessments) as well as planning and exercising [See Section 6, Awareness, 5.2.6.1/G.5.2.6.1]
- That the requirements or outputs of LRFs/LRPs should be reported and discussed at the relevant governing body within the organisation. In line with the procedures outlined in [See Section 6, Awareness, 5.2.6.1/G.5.2.6.1] relevant IEM activities and outstanding requirements should be integrated into the governance process and reported to the relevant governing body or responsible individuals

Rail Entities should maintain representation and collaboration with the RDG EPG to streamline engagement with relevant LRFs/LRPs. They should maintain and continuously improve the existing mechanism for nominating and regularly updating rail contacts for each LRF and LRP – enabling continuous and effective engagement across industry and wider community.

G8.2.2 Rail Entities must comply with anti-discrimination legislation, including the 2010 Equality Act, and make the appropriate considerations across the five phases of the IEM framework. Rail Entities must make reasonable adjustments for disabled users, falling under the protected categories of the act, to any relevant policies, plans and procedures. This should be an anticipatory process, taking positive steps to remove barriers and prevent harm.

Rail Entities must be proactive in identifying potential discriminatory practices and consider the specific needs of vulnerable individuals when assessing, preparing, preventing, responding, and recovering from disruptive incidents.

G8.2.3 Senior Leadership plays a key role in setting the strategic direction of inclusive stakeholder engagement by ensuring commitment, determining resilience vision and values, and providing the adequate support and resourcing for relevant activities.

The relevant governing body, or responsible individuals, should:

- Provide clear direction and alignment of the stakeholder engagement to the core values and strategic IEM and resilience priorities of the organisation. This should be captured in the relevant policy documents
- Assign roles and responsibilities
- Provide adequate resourcing
- Conduct continuous monitoring, evaluation of progress and facilitate continuous improvement activities

G8.2.4 Rail Entities should develop, regularly conduct, and continuously improve their effective stakeholder engagement through a clear 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.

Rail Entities should seek to identify, map, assess, and engage stakeholders – empowering their role in the IEM strategy. The relevant governing body, or responsible individuals, should:

- Identify the goals and desired outcome of the engagement. This should be based and aligned to the strategic vision for IEM as set out by Senior Leaders
- Identify and map relevant external and internal stakeholders, adopting a whole system approach
- Evaluate the needs and interests of the identified internal and external stakeholders, assessing interdependencies across the whole system. There should be a clear understanding of the varied interests, needs, priorities and sensitivities in the specific operating context of the rail entity
- Develop a communication and engagement strategy and plan. This can include a variety of different formats such as training, exercising, awareness campaigns, dedicated intranet site or continuous development programmes
- Adopt simple and inclusive language. IEM activities often require involving professionals who are not primary experts in the subject Information, requirements as well as plans and procedures should be communicated in simple language, avoiding jargon, technical references and ensuring it is accessible to all relevant stakeholders
- Promote alignment and encourage buy-in. The engagement strategy and plan should reflect and promote a shared understanding of the benefits of integrating IEM into BAU
- Enable participation of relevant stakeholders at each relevant governing body. The relevant governing body should verify there is a process to involve and engage the stakeholders to achieve the agreed IEM strategic objectives

G8.2.5 IEM is an integral component of resilience and sits alongside parallel functional disciplines such as Security, Business Continuity, Weather Resilience, IT Service Continuity and Risk Management. There should be a clear direction, endorsement, and support for coordination of different functions of resilience across the organisation to promote an alignment and common

understanding of requirements, methodology, outstanding risks as well as prevention, preparedness, and remediation activity.

Depending on the size, context, and resourcing of the organisation, some of these functions might sit within the same team or have more complex structures aligned to routes or geographical divisions.

Coordination procedures and mechanisms should be aligned to the existing governance structure and help ensuring that there is a documented process for ensuring information sharing, allocation of resources and alignment between IEM and wider risks identified across the business and functions. This should include:

- Clear strategic direction set out in a resilience policy [See Section 5, Leadership, 5.1.2.1/G5.1.2.1]
- An established Resilience Working Group, or equivalent governing body, where IEM professionals and relevant colleagues from parallel functions coordinate activity and share information. As highlighted in Section 4.2 IEM Organisational Governance Structure, the group should have a clear agenda, agreed roles and responsibilities and an adequate process for monitoring performance and ownership of remediation activity, or escalation to Local Business Risk or Executive Risks Committees
- A documented procedure for aligning prevention and preparedness activities, based on a shared situational awareness. This can include for example an alignment of the IEM risks and associated emergency planning and the identified Business Continuity Plans, or incorporation of existing access controls and asset protection measures in existing IEM plans

G8.2.6 Inclusive engagement should facilitate an integration of IEM into BAU. This means that there should be clear processes and procedures enabling IEM anticipation, prevention, and preparedness activities to be conducted as part of the standard process for ordinary and extraordinary workstreams. This includes:

- A documented process for relevant IEM assessments to be conducted before final project approval. This would enable integrating IEM activities, considerations, or assessments into the strategic planning of ordinary and extraordinary work streams
- Ordinary or extraordinary work streams, requiring IEM assessments or considerations, are discussed at the relevant governing body (for example, Resilience Working Group/ Local Business Risk Committee) and the relevant preparedness or prevention activities assigned and conducted by relevant EM practitioners

G8.2.7 Rail Entities should regularly engage with their key regulators, including ORR, DfT, TfW and Transport Scotland. Maintaining an open and continuous dialogue will greatly contribute the regulators to understand current operating environment and IEM challenges and will support Rail Entities ensuring continuous regulatory compliance.

Rail Entities should:

- Identify responsible individuals to liaise with the regulators. There should be clearly assigned professionals, with the appropriate authority and seniority, to engage with the regulator. This should be included in their recognised responsibilities, and they should be given sufficient time and resourcing to conduct engagement (including attending meetings, participating in industry-wide groups)
- Share relevant IEM MI, information, horizon-scanning outputs, or data, where available. This would greatly enhance transparency and the awareness of the regulator of current challenges, assessed IEM risks, as well as progress of IEM programmes
- Engage with the regulators in pan-industry forums. This would contribute to an inclusive engagement across the industry, addressing regulatory concerns and contributing to shaping policy and requirements

9 Adaptation and Improvement Principle

***Principle**: 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. Adapting and improving following disasters so that organisations can thrive, not just survive.*

9.1 Adaptation

The ability to adapt is an essential part of resilience that creates systems that can evolve and manoeuvre quickly in a changing landscape – addressing risks and capitalising on opportunities. Building flexibility and resourcefulness is key in an era of ever-increasing uncertainty and change so that existing resources can be applied for new purposes when needed. Being able to rapidly find different ways to achieve desired outcomes or meet needs during a shock or when under stress is vital. It is important to mobilise human, financial and technical resources (inside or outside of traditional response structures) to deliver innovative solutions in the face of adversity.

9.2 Improvement

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

9.3 Provisions and accompanying guidance

Provisions

9.3.1 Senior Leaders **should** consider the effect of uncertainty and change on the organisational purpose and associated strategic outcomes.

9.3.2 Senior Leaders **should** provide decision-making that is agile and keeps pace with the changing environment; rapidly allocating resources where needed.

9.3.3 Senior Leaders **should** require those to whom they have delegated responsibilities or activities to provide timely and accurate reports on all material aspects of IEM for the organisation.

9.3.4 Rail Entities **should** utilise assessment, monitoring, evaluating and progress reporting to inform modifications to improve performance and support adaptation to changing circumstances.

9.3.5 Rail Entities **should** provide assurance that any new actions or modifications to existing actions are assigned and implemented by an appropriate representative and that these are adequately delivered and measured for effectiveness.

9.3.6 Senior Leaders **should** implement a process for continual improvement and active learning development to support long-term resilience building and inform decision-making around planning and investment.

9.3.7 Senior Leaders **should** empower people to identify potential issues and opportunities early, to be more nimble and agile, and to respond more competently.

9.3.8 Rail Entities **should** collect information through audits, post-exercise reports, and post-incident reports to facilitate preparedness and learning, identifying further actions and implementing improvements with the purpose of making systems stronger and more adaptive to future disruption.

,

9.3.9 Rail Entities **should** assess all capabilities delivered as part of the IEM strategy as part of a whole system approach, with learning and recommendations feeding back to leadership and governance systems.

9.3.10 Rail Entities **should** share organisational knowledge and learning with industry partners.

9.3.11 Rail Entities **should** provide robust mechanisms to capture and store organisational knowledge for the benefit of all employees and broader rail industry.

9.3.12 Senior Leaders **should** exhibit the behaviours and facilitate the development of a culture of learning and innovation, including transfer of knowledge and capability within their organisation and across the rail sector.

9.3.13 Rail Entities **could** agree and include resilience and adaptability criteria within design and procurement requirements.

Supporting Guidance

G9.3.1 Senior Leaders should consider the effect of uncertainty and change on the organisational purpose and associated strategic outcomes. This can be achieved through requiring uncertainty in decision-making to be understood and through building the adaptive capacity of the organisation. Adaptive capacity is the ability to adapt to change and leads to competitive advantage.

This can be built through:

- A holistic approach that acknowledges the importance of a systems view
- A clear vision unifying the organization, with strong understanding of how individual roles align unites and engages teams
- Driving collaborative working which in turn
- Facilitating innovation, knowledge sharing and overall learning
- Distributed leadership providing autonomy and freedom so that employees feel empowered to drive positive change and shape the business, as well as respond to external/internal impacts
- Situational awareness and foresight enabling horizon scanning so that potential impacts are discovered and embraced
- Mechanisms are put in place to enable adaptation in response to feedback from customers
- Adopting flat structures and empowering teams to make decisions
- Regularly reviewing the organisational vision considering future scenarios, needs and changes in circumstance
- Tackling causes of change resistance and actively managed through a strong change narrative and effective engagement

Uncertainty in decision making can be understood and improved through:

- Analysing emerging threats and industry trends and understanding gaps in information and risk understanding
- Measuring the resilience of the organisation and the uncertainty in this measurement
- Implementing a training programme on leading through uncertainty

G9.3.2 Senior Leaders should provide decision-making that is agile and keeps pace with the changing environment; rapidly allocating resources where needed. To achieve this, organisations should take every opportunity to learn and develop. Rail Entities should build their capacity for adaptation. This can be achieved by devolving authority and resources, embedding a culture of learning from successes and failures, and having flexible processes that can easily and swiftly move resources and decision-making authority to where they are needed e.g. providing nominated incident commanders with spending authorisations beyond what they might normally have during BAU. Decisions should take into account the best possible evidence, including future scenarios and innovations and be supported by suitable decision-support methodologies e.g. using decision trees or pre-developed decision-making models such as Joint Emergency Services Interoperability Principles (JESIP) National decision Model (NDM).

G9.3.3 Senior Leaders should require those to whom they have delegated to provide timely and accurate reports on all material aspects of IEM for the organisation. Specific performance targets and metrics should be agreed and tracked, and regular meetings held to review progress. [See Section 7, Culture & Maturity Principle].

G9.3.4 Rail Entities should utilise assessment, monitoring, evaluating and progress reporting to inform modifications to improve performance and support adaptation to changing circumstances. There should be robust resilience reporting mechanisms to enhance speed, accuracy, pertinence, and clarity of information sharing, especially during and immediately following incidents. [See Section 6, Awareness Principle]. Existing policies and strategies should be assessed against resilience performance; how well it creates, sustains and protects organisational value. Performance of resilience capacity building should be assessed against specific, measurable, and accountable goals/targets defined within an organisation-wide, comprehensive IEM strategy. The performance and learning from tests and exercises should be openly reported and linked to top level governance arrangements.

G9.3.5 Rail Entities should provide assurance that any new actions or modifications to existing actions are assigned and implemented by an appropriate representative and that these are adequately delivered and measured for effectiveness. A routine review should confirm that actions or modifications have been effectively implemented and the impact of implementation. Similarly, assurance should be provided that reports and evidence received are accurate and that the review and learning system is effective.

G9.3.6 Senior Leaders should implement a process for continual improvement and active learning development to support long-term resilience building and inform decision-making around

planning and investment. This could include a response and recovery capability continuous development programme. Learning should be formed into an action plan and delivered as a project with open and transparent governance.

G9.3.7 Senior Leaders should enable people to identify potential issues and opportunities early, to be more nimble and agile, and to respond more competently. A training and education programme should be made available to all relevant stakeholders in support of resilience capacity building. Developing a resilient leadership programme fostering resilient skills and mindsets within staff is recommended [See Section 7, Culture & Maturity Principle].

G9.3.8 Rail Entities should collect information through audits, post-exercise reports, and post-incident reports to facilitate preparedness and learning, identifying further actions and implementing improvements with the purpose of making systems stronger and more adaptive to future disruption. Rail Entities should enable after every incident, an open and honest debrief to capture lessons learned. These should be cross-sectoral including all relevant stakeholders and focused on collective performance and improving risk reduction efforts and recovery. There should be no allocation of blame. Successes should be celebrated, and lessons learned from failures. Learning should be formed into an action plan, with clear owners for activities, dates and monitoring for completion and measurement of impact. Resilience strategies and plans should be updated based on this learning.

IEM good practice is to:

- Hold a ‘hot debrief’ immediately/shortly after the incident has concluded and a second, more comprehensive, ‘cold debrief’ within 28 days of the incident concluding where necessary
- Appoint a senior leader to be the Debrief Sponsor. The sponsor is responsible for the effective delivery of the cold debrief, apportioning actions arising to owners and confirming when these have been delivered
- Use an independent, trained and competent facilitator to deliver the cold debrief.
- Provide dedicated administrative support to plan and deliver the cold debrief and collate the post-debrief report
- Avoid the ‘cold debrief’ merely focussing on “what happened and when” by developing an agreed incident timeline before the cold debrief. This timeline should be shared and agreed with all partners prior to the event
- For large and/or complex incidents produce a pre-debrief report that identifies key themes for discussion during the cold debrief
- Include all relevant partners involved in the incident
- Remind all debrief participants that the debrief report will be widely circulated and that it will not be redacted

G9.3.9 Rail Entities should assess all capabilities delivered as part of the IEM strategy as part of a whole system approach, with learning and recommendations feeding back to leadership and governance systems. Capabilities of people, systems and organisations should be reviewed and continually adapted to reflect changing circumstances. Monitoring and data review systems should be adaptable to technological and information management advances as they occur.

G9.3.10 Rail Entities should share organisational knowledge and learning with industry partners. Learning should be encouraged across the organisation and between Rail Entities. The rail industry should work with other industries to share learning and experiences, to strengthen resilience capacity building and avoid mistakes. Learning should be sought from the positive and negative experience of other organisations and contexts.

G9.3.11 Rail Entities should provide robust mechanisms to capture and store organisational knowledge for the benefit of all employees and broader rail industry. Structures, roles and responsibilities for the rapid gathering, collation, sharing and use of data and information should be defined. New knowledge and information should be integrated into the decision-making processes as the evidence base matures. There should be an open data platform allowing wide access to data, enabling knowledge sharing, data collection and awareness to be created.

G9.3.12 Rail Entities could agree and include resilience and adaptability criteria within design and procurement requirements. This will help improve supply chain resilience but also make sure that procured equipment is designed to be adaptable, with effort made to avoid future obsolescence.

G9.3.13 Senior Leaders could exhibit the behaviours and facilitate the development of a culture of learning and innovation [See Section 7, Culture & Maturity Principle], including transfer of knowledge and capability within their organisation and across the rail sector. Small pilots and trials can be used to prove concepts. Enabling new innovations to more rapidly enter the rail market should be facilitated.

10 References

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

Name of the document	Reference number
Risk management - Guidelines	ISO31000:2018
Security and Resilience – Community and Resilience – Principles and framework for urban resilience	ISO22371:2022
Governance of Organisations – Guidance	ISO37000:2021
Security and Resilience – Crisis Management – Guidelines	ISO22361:2022
Societal security - Business continuity management systems - Requirements	ISO22301:2019
UK Resilience Framework - December 2022	
BS67000 City Resilience – Guidelines, 2019	BS67000:2019
Railways and Other Guided Systems (Safety) Regulations 2006	
Blackstone's Emergency Planning, Crisis and Disaster Management, 2nd Edition Brian Dillon Oxford University Press 2014	ISBN: 978-0-19-871290-9
Security Risk Management Body of Knowledge Julian Talbot & Miles Jakeman Wiley 2009	ISBN: 978-0-470-45462-6
Professional Security Management: A Strategic Guide Charles Swanson Routledge 2021	ISBN: 978-0-367-33961-6
The Intelligence Handbook, Fourth Edition Various Authors Cyberedge Press 2022	ISBN: 978-1-7371618-2-0
Strategic Risk and Crisis Management David Rubens KoganPage 2023	ISBN: 978-1-3986-0975-4

11 Annex

As described in Section 7, the following maturity model is based on the Capability Maturity Model Integration (CMMI). This framework model has been chosen as it aligns well with the ORR RM3 methodology. Below is an example of this maturity model using six categories (people, processes, technology, locations, suppliers, and data/information) and maturity level based on the ORR's RM3 methodology. This is a complete version of the table shown in Section 7, Maturity and Culture Principle.

	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 have 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 suppliers 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 suppliers 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).

Information / Data	• Little understanding of the data/information needs e.g. performance management, for IEM governance. • No documented IEM governance information requirements. • Management information to support IEM governance is provided on an ad hoc basis. • IEM management information is rarely provided to generate hindsight, insight or foresight. • Management of data is poorly controlled.	• There is some understanding of the overall information needs for IEM governance but this is inconsistent. • Some IEM governance information needs are documented e.g. risk assessments. • Some relevant management information is provided regularly. • IEM management information if focussed primarily on generating current insight. • Management of data	• There is a clear understanding of IEM governance information needs • IEM governance information requirements are clearly identified and mainly documented. • Most IEM management information is provided consistently in terms of timeliness and quality. • IEM management information provides a good level of insight (current) with some hindsight (experiential learning) and foresight (horizon scanning). • Management of data complies with relevant regulations e.g. GDPR, Data Protection Act.	• IEM governance information needs are fully understood including wider organisation information. • IEM governance information requirements are fully documented • Management information is consistently delivered to both time and quality requirements. • Management information provides real insight and increasingly is used to generate hindsight and foresight. • Data management regulations are consistently applied and regularly reviewed.	• IEM governance's information needs are embedded (12+months) in the organisation. • IEM governance information requirements are fully documented and routinely reviewed to inform improvements. • Management information is consistently delivered and quality / timeliness subject to a process of continuous improvement. • Data is leveraged to provide hindsight, insight and foresight to consistently enhance IEM performance. • Data management regulations are fully complied with and supported by a process of active risk management to minimise the opportunities for breaches.

End of Document

Rail Delivery Group

National Rail

Rail Delivery Group Limited Registered Office, 2nd Floor, 200 Aldersgate Street, London EC1A 4HD
www.raildeliverygroup.com 020 7841 8000 Registered in England and Wales No. 08176197