Rail Delivery Group

National Rail

RDG Approved Code of Practice: Rail Emergency Management - Anticipation, Assessment and Prevention

RDG-OPS-ACOP-009
Issue 2.0 – 10.03.25

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.

Issue record

Issue	Date	Comments
0.3	30 Jan 2024	Third Draft Version endorsed by WG on 23 Jan 2024, sent for approval and sign off by Steering Group on 8 Feb 2024.
1.0	19 Feb 2024	Document Issue
1.1	17 May 2024	Minor formatting changes only
2.0	10 Mar 2025	Changes following a formal review of the content, against ACOP 008-12 which are now published.

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

Written by / Prepared by:
Louise Elstow, Thomas Croall and Keith Newton of Fynbos Consulting Limited.

RDG RRP Delivery Team
Contact: John Melville

Authorised by:
Rail Resilience Steering Group (RRSG)

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

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

Train Operators (Passenger & Freight), Infrastructure Manager (Network Rail), GBRTT, DfT, TfL, TfW, Transport Scotland, BTP, ORR, and RSSB.

Executive summary

This Code of Practice has been developed to support the recommendations from the industry Rail Resilience Project (RRP) Emergency Management Review (completed June 20211). It describes the need for a Code of Practice (CoP) for the Anticipation, Assessment and Prevention of rail industry Integrated Emergency Management activity.

The UK railway faces a range of risks, threats, hazards, and operational challenges which could jeopardise its ability to run services safely and securely, and to uphold passenger expectations and confidence. In recent years the rail industry has dealt with a number of major passenger derailments,2 some with fatalities3, ongoing structural changes within the industry4, technological upgrades5, the impacts of climate change on ageing infrastructure6, repeated industrial action7, cyber-attacks8, and fires9. This demonstrates that the management of risks that would give rise to a major emergency, major impacts and major long-term recovery issues is something that needs to be taken seriously.

In order to have the most success in preventing - where possible - and reducing the impact of such emergencies, the industry needs to be able to clearly identify, assess and evaluate emergency management (EM) risk using robust and repeatable processes. These processes should integrate into existing rail management systems and take advantage of existing sources of information such as the UK National Risk Register. An understanding of EM Risk should be used to inform proactive risk treatments including preventative and responsive controls to mitigate the impact should the risk materialise. Efforts to manage risk will only remain effective if the Rail Entity regularly reviews its assessments of risk and the effectiveness of its controls in light of changes to the organisation and risk landscape. This considered approach to risk management aligns to the tenets of 'integrated emergency management' (hereafter IEM and referred to in more detail in Section 1.6).

To effectively manage EM Risk the Duty Holders (RAIB, 2018) - hereafter 'Rail Entities' - should identify and understand their critical assets and activities including any vulnerabilities that may exist. The impact of identified risks should be considered in relation to the Rail Entity's risk appetite and their legal responsibility to ensure that unacceptable risks are reduced 'so far as is reasonably practicable (SFAIRP)'. Any risks outside risk appetite should be managed to within appetite. Residual risks that cannot be managed should be consciously accepted by top management and regularly reviewed.

IEM provides the critical link between various functions in a Rail Entity (risk management, emergency management, asset management, security management, safety management, business continuity management, etc.) which should work in close partnership. However different Rail Entities prioritise organisational functions differently, according to the varied management commitment, experience of regulatory scrutiny and operational resources they are allocated. Consequently, the link between these important functions is not always clear and often disjointed. EM Risk understanding does not always drive decisions around activities that support EM prevention, planning and preparation. Furthermore, Rail Entities' collective understandings of risk do not always form the basis of the management of shared risks and controls.

This CoP sets out 29 provisions (provided in the Appendix A: Table of Provisions) for the Anticipation, Assessment and Prevention of EM Risk. Each provision is accompanied by guidance immediately below it, which describes what Rail Entities 'must', 'should' or 'could' do to demonstrate good practice in the management of EM Risk. Chapter 2 establishes what is meant by EM Risk and the risk environment. The provisions and associated supporting guidance are provided in the remaining chapters. The relevant IEM phases are identified in brackets alongside more commonly used risk management terms.

It is the intention that the provisions established in this document will be introduced, embedded, maintained and built into existing Rail Entity management systems within a reasonable timeframe. The management of

---

[1] https://www.raildeliverygroup.com/media-centre-docman/12968-rail-resilience-project-report-final-version/file.html
[2] https://www.gov.uk/government/news/report-122023-collision-between-passenger-trains-at-salisbury-tunnel-junction
[3] https://www.gov.uk/raib-reports/report-02-slash-2022-derailment-of-a-passenger-train-at-carmont
[4] https://assets.publishing.service.gov.uk/media/60cb29dde90e0743ae8c29c1/gbr-williams-shapps-plan-for-rail.pdf
[5] https://www.bbc.com/news/uk-england-67370072
[6] https://www.networkrail.co.uk/who-we-are/publications-and-resources/our-delivery-plan-for-2019-2024/
[7] https://www.bbc.com/news/business-61634959
[8] https://www.orr.gov.uk/search-news/keeping-britains-railway-safe-cyber-threats
[9] https://www.gov.uk/government/news/report-012022-derailment-and-fire-involving-a-tanker-train-at-llangennech-carmarthenshire and https://www.independent.co.uk/travel/news-and-advice/leeds-station-chaos-train-fire-b2424536.html

this process should be established and monitored to maturity and reported on through the provisions set out in the CoP for the Governance of IEM (RDG-OPS-ACOP-008) available here.

Contents

1 Purpose and scope

1.1 Purpose

This Code of Practice (CoP) is one of several, which collectively as the Rail Emergency Management Code of Practice, address the full Integrated Emergency Management (IEM) cycle. This CoP sets out requirements (Provisions) for the effective Anticipation, Assessment and Prevention elements of IEM, explained in more detail below. Each provision is accompanied by relevant guidance and signposting to enable practitioners, organisations, and the industry to implement them. By working to meet the provisions set out in this CoP Rail Entities should: Understand emergency management (EM) threats and hazards and their consequence on critical assets and prioritised activities, so that relevant plans for EM and business continuity management (BCM) responses can be developed;

- Understand EM Risks that they are responsible for managing;
- Have appropriate controls in-place to mitigate such risks;
- Have confidence that these controls are operating effectively and can demonstrate this.

1.2 Rail IEM Codes of Practice

This CoP should be read in conjunction with the 'RDG OPS GN 064 Rail Emergency Management Legal and Regulatory Register' and as a part of the collective set of IEM CoPs produced by Rail Delivery Griup (RDG):

- RDG OPS ACOP 008 Rail Emergency Management - Governance;
- RDG OPS ACOP 010 Rail Emergency Management Preparation;
- RDG OPS ACOP 011 Rail Emergency Management Response; and
- RDG OPS ACOP 012 Rail Emergency Management Recovery

1.3 Audience

The management of EM Risk involves collaboration across multiple parts of the organisation (See Provision 7 which covers assurance and oversight) and this CoP is directed to all those with roles contributing to the management of EM Risk.

At a strategic level, this document is intended to inform Top Management's knowledge and understanding of how they can support and govern the organisation to achieve effective risk-based decision-making – establishing a clear link between risk management and prevention of and readiness for EM Risks.

At an operational level, the intended audience for this CoP are functions which collectively contribute to the management of EM Risks. These functions are likely to include risk management, EM, BCM, security, asset management, health & safety and assurance and audit functions. EM professionals in particular tend to focus their attention on the Prepare, Respond and Recover aspects of IEM (See section below on Risk Anticipation, Assessment and Prevention). However, their work must link with and be driven by the Anticipate, Assess and Prevent parts of IEM, often coordinated in other parts of the organisation. The exact roles and teams involved will be determined by the structure, size and configuration of each Rail Entity.

1.4 Background

The Rail Resilience Project (RRP) report10, 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. In relation to anticipation, assessment & prevention,

[10] Rail Delivery Group (2021). *Rail Resilience Project (RRP) Emergency Management Review: Findings and Recommendations Report.* https://www.raildeliverygroup.com/media-centre-docman/12968-rail-resilience-project-report-final-version/file.html

the report noted that: *Formalised and transparent processes for anticipation and assessment of EM Risk are absent, meaning that risk management is not being effectively used to drive EM activity.* This CoP establishes a set of requirements which if adopted should forge more effective links between risk and emergency management.

1.5 Scope

The contents of this CoP apply to individual Rail Entities and at a pan-industry level. It is applicable to all members of the RDG that manage infrastructure or operate services (duty holders) over the GB mainland mainline 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 as part of their process to satisfy licence conditions. It is important to consider longer-term changes in the industry, organisation, economy, and climate of course, as that forms part of good business planning, however the timescales involved might be much longer.

1.6 Document Structure

This CoP is structured into two sections. Section 1 details who the document is for, the scope of the document and how it is arranged – enabling a reader to navigate the document easily. Section 2 sets out the provisions (requirements) and is broken down into 6 chapters.

- **Chapter 3 (EM Risk Environment)** defines the structural and organisational environment within which effective EM Risk management process takes place – it considers for example organisational context, governance structures, and roles and responsibilities.

Chapters 0 to 7 follow a broadly linear path through the risk management process (in the centre of Figure 2). Although the risk management process presented in this CoP as sequential, in practice it is often iterative, cyclical, and ongoing:

- **Chapter 0**
- EM Risk Identification (Anticipation)**)** examines how various sources of information can employed to identify EM Risks.

Key Terms

Risk identification is the process of finding, recognising and describing risks so that they can be assessed or analysed, and this knowledge can inform the allocation of resources to manage the risk or prepare for the consequences.

Data management involves the collection, storage, analysis and distribution of data and information so that it provides current, relevant, and useful insight into current or potential issues, risks, disruption, or shocks. Data management involves finding out information about existing known risks as well as identifying new risks.

Risk velocity refers to the rate at which a risk event develops from its onset to its peak impact. Understanding risk velocity can help to understand how quickly an organisation must respond to indicators the risk may be manifesting.

- **Chapter 5 Risk Analysis and Evaluation (Assessment)** sets out the requirements for the assessment of identified EM Risks and their potential impacts on the organisation, so the organisation can make an evaluation of whether any further action is needed to manage the risk.
- **Chapter 6 Treatment (Prevention)** describes the requirements for treating and controlling EM Risks.
- **Chapter 7 Monitoring & Reviewing** addresses how EM Risks and associated processes are monitored and reviewed over time so that they continue to be fit for purpose – feeding back into risk identification activity.

The last chapter (EM Risk Communication) describes the provisions for effective collaboration and communication with internal and external stakeholders about risks and their impact on the

preparation for emergencies, which occur throughout the risk management process described in chapters 3-6.

In each chapter each provision statement is followed by its associated guidance. As some readers may not be risk management specialists, where new terms are introduced, these are explained in the 'Key Term' boxes that can be found throughout the document and are supplementary to the glossary at Appendix B: Definitions

Green boxed sections and text in BOLD green, provide industry context and rail-related information.

1.7 Risk Anticipation, Assessment & Prevention

This document covers the Risk anticipation, assessment and prevention elements of IEM. IEM's key activities operate in a linked framework with Preparedness at its centre (depicted in Figure 1). Anticipation, Assessment and Prevention (which are commensurate with risk management activities) are the backbone for Preparedness activities, as they enable Rail Entities to prioritise resources effectively so that they are directed towards the risks which would have the most impact. This means the organisation has a better chance of being able to quickly *Respond* to and *Recover* from incidents and emergencies that would otherwise have the greatest detrimental impact on the organisation's objectives. Lessons from response should then feed back into further Preparedness activity.

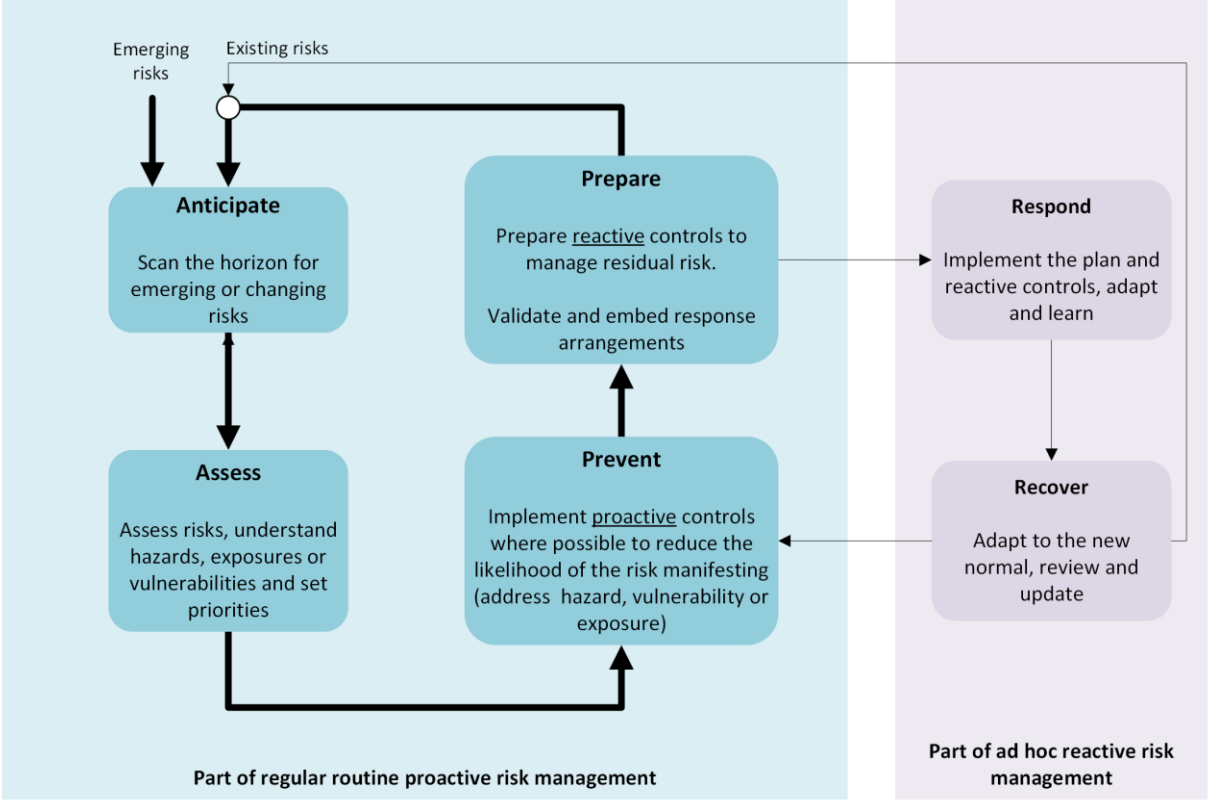


Figure 1: IEM Framework adapted from Emergency Planning College

As its name suggests, IEM activities need to be integrated throughout individual Rail Entities, across the wider rail industry and with other civil responders. Numerous disciplines and functions collectively contribute to overall resilience. IEM activity is not a separate or distinct function within Rail Entities and should therefore be woven through the business-as-usual activities of the organisation/industry.

Resilience relates to the ability of a Rail Entity to provide services effectively and sustainably in a way which anticipates, assesses, prevents, mitigates, responds to, and recovers from shocks which may affect that delivery. Resilience encompasses multiple strands of activity which could include EM and BC, Asset Management, Security, Health and Safety, IT, Incident Care Teams, Risk Management, as well as other parts of the organisation. Resilience therefore requires cooperation and collaboration

from multiple teams in order for the organisation to be able to identify, assess, and control risks, and for the EM and BC plans to be effective, should the risks materialise into live issues.

This Rail EM CoP specifically addresses Anticipation, Assessment and Prevention elements of IEM:

- **Anticipation**: The role of assessment is the proactive scanning of different sources of information in order to identify threats, hazards, and opportunities before they manifest.
- **Assessment**: The role of assessment is to understand the likelihood and impacts of any identified threats, hazards, and opportunities. This helps to make sure resources for mitigation, prevention and preparation activities are allocated most effectively according to priorities.
- **Prevention:** The role of prevention is to take steps to prevent/reduce risks manifesting, and/or reducing their impact should they occur.

Figure 2:: The contents of this Code of Practice align to ISO 31000's visual representation of the risk environment and its prescribed risk management process. The outer arrows have been added to show the relationship to key IEM activities.

1.8 Risk Management in relation to Emergency Management

Key Terms	The UK Resilience Framework (2022) defines risk as: An event, person or object which could cause loss of life or injury, damage to infrastructure, social and economic disruption or environmental degradation. The severity of a risk is assessed as a combination of its potential impact and its likelihood. The Government subdivides risks into hazards [non-malicious risks] and threats [malicious risks].

Every policy, investment or operational decision taken by the GB railway industry impacts rail safety in some way. Keeping people safe costs money - this should be embraced as part of a Rail Entity's business planning. Safety is an integral part of a business, not an add on feature.

Rail systems are complex. They have multiple interconnected processes and assets which have different lifespans, maintenance and renewal schedules, and critically different exposures to threats and hazards. Whilst this part of the EM CoP relates to risk management – it does not seek to establish any kind of separate EM Risk management process. Each Rail Entity will already have existing risk management capabilities, processes and structures in place in order to manage risks affecting their organisation. RSSB is leading a programme of work on Risk, underpinning the new Rail Resilience Strategy.

Instead, the intention is that EM Risks are appropriately considered and addressed within existing structures and that EM practice (e.g. the work of preparing for, responding to and

recovering from emergencies) is driven first and foremost by a good understanding of what kinds of risks might cause an emergency, the impacts of those risks manifesting, what is done to limit the likelihood of that risk manifesting and the measures that can be taken (including plans that might be needed) to mitigate the consequences if the risks nevertheless materialise.

1.9 What is an 'Emergency Management Risk'?

Key Terms

In this document an *Emergency Management (EM) Risk* is a risk which might give rise to:

An emergency *(an event or situation which threatens serious damage to human welfare, or to the environment; or war, or terrorism, which threatens serious damage to security. (UK Resilience Framework: December 2022))* or,

A major incident *(an event or situation with a range of serious consequences which requires special arrangements to be implemented by one or more emergency responder agency (JESIP[11])).*

Whilst there are routine and standardised processes for managing all kinds of risks (see categories on next page) they become EM Risks when standard organisational structures and processes would be insufficient to deal with the consequences of the materialised risk. EM Risks tend to involve or affect multiple departments working beyond routine arrangements. They can arise from risks affecting all parts of the railway (RSSB, CHAMOIS, 2023; p14):

Railway Vehicles / Rolling Stock - The trains that operate on the railways.

Operations - The functions required to deliver an operational railway – e.g. what is often a 'Significant Disruption' or a 'Sever Disruption' in common railway terminology, are likely to illicit a need for an IEM response.

Maintenance and renewals - The functions required to maintain or renewal the physical assets e.g. rolling stock and infrastructure.

People - The people and roles that deliver the functions defined in 3 & 4 above (e.g. workforce) or are affected by the rail system and its operation (e.g. rail users).

Organisation - The processes that the rail industry organisation follows to deliver the operational railway.

EM Risks are not a distinct standalone category and are not mutually exclusive from other risks. EM Risks are concerned with the scale of the impact and consequences that might need managing, less than the cause.

Many different kinds of risks could affect a Rail Entity's ability to operate as a going concern providing its intended business function and the delivery of its objectives. Risks can be categorised in a variety of ways – including thinking about the cause of the risk or the consequences of the risk manifesting. The UK government breaks down risks into those with a malicious intent (threats) or a benign intent (hazards). The UK rail industry tends to think about the risk categories listed below:

- **Security risks** - a person, thing or situation which poses a possible threat (a malicious intent) to the security of the UK rail system. Security involves the protection of people, hardware, software, network information and data from physical actions, intrusions and other events that could damage the organisation or its assets. A security risk may involve attacks or theft, which typically include either the damage or the threat of damage to physical (including humans) and digital assets. Security risks can be small, repeated risks (e.g. non-service impacting vandalism) or significant (e.g. a terrorist attack, or major vandalism affecting the safety of rail users or staff). They are typically managed (owned) by the Rail Entity's Security team along with IT security.

[11] JESIP: https://www.jesip.org.uk/

- **Health, Safety and Environmental risks** – UK employers are required by law to protect their employees and others from harm, under the Management of Health and Safety at Work Regulations 1999. These kinds of risks include slips, trips and falls, safe working environments, working hours and fatigue, public health concerns. It also includes environmental risks such as loss of containment of dangerous goods, leading to major accident/hazard and subsequent environmental damage. These risks are typically managed (owned) by the Rail Entity's Health, Safety and Environment team along with Human Resources.
- **Engineering risks –** the UK rail network is made up of a significant amount of physical infrastructure (stations, lines, signalling, depots etc.) and physical assets (rolling stock) which may fail, become accidentally / intentionally damaged or defective if not maintained appropriately. These risks and critical assets are typically managed (owned) by the Rail Entity's Engineering and Maintenance teams along with Fleet.
- **Operational risks –** risks that could cause harm to operational service delivery of the UK rail network – insufficient staff to crew trains, delays on other services holding up the line, minor derailments, etc. These risks are typically managed (owned) by the various teams in the Rail Entity, including Control and Operations Teams (driver management) as well as Communications, Customer Services or Public Relations Teams.
- **Financial risks –** the possibility of losing money on an investment or revenue generating activity. These risks tend to arise from contractual or legal obligations and are typically managed (owned) by the Rail Entity's Finance/Treasury team along with the corporate contracts teams.
- **Reputational risks –** the possibility of damage to the reputation of the organisation. This may affect the future willingness of other individuals (staff or rail users) or organisations (business partners, suppliers) to work with the organisation. These risks are typically managed (owned) by the Rail Entity's Communications, Customer Services or Public Relations Teams.

The UK Government's 'The Orange Book - Management of Risk – Principles and Concepts[12]' provides several additional risk categories in *Appendix 4 Example Risk Categories*, although they do not examine Emergency Management Risk (EM Risk). Therefore, this CoP provides the following explanation for an EM Risk as these kinds of risk are the focus of this document.

1.10 Interdependencies between EM and other Risks

EM Risks are complex and interwoven; managing one risk could have knock-on effects elsewhere in the organisation or involve multiple risks materialising at the same time. For example, a train crash could involve multiple primary and second-order risks to materialise:

- The cause of the incident could have been from a malicious cyber-attack (security risk) and involve damage to critical assets (engineering risk).
- The incident itself could cause significant service delays whilst the line is closed, and passenger/freight travel is disrupted (operational risks).
- New working arrangements to manage the incident at site might mean new dangers to safe working arrangements (health and safety risks).
- Injuries and fatalities to rail users and staff (health and safety risks)
- Additional scrutiny from investigators and regulators (financial and legal risks) leading to possible prosecution, fines, improvement notices and additional costs (e.g. insurance claims).

[12] The Orange Book - Management of Risk – Principles and Concepts, page 54. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf

- Civil action and compensation claims (legal and financial risks) from affected parties, including injured passengers, bereaved families, or businesses impacted by the incident.
- Rail users may not feel confident in travelling with the organisation anymore, resulting in lower ticket sales (financial and reputational risks).
- Delays to major projects as staff and resources are diverted to manage the consequences of the incident (financial, engineering, contract risks etc).

Categorising a risk as an EM Risk is a tool to assist EM and resilience professionals to identify risks they should be aware of. As a result, these risks should be driving prevention, preparation and ongoing assurance activities. Table 1 shows how EM Risks relate to other kinds of risk categories, which tend to be based around control ownership.

Risk Category	Addressed by BAU arrangements	Emergency Management Risks
Security Risks	Non-service impacting vandalism, petty theft	Terrorist attack, major cyber-attack, theft of critical equipment, major arson
Health, Safety & Environmental Risks	Slips, trips and falls	Public Health (e.g. Pandemic) or major fire. Loss of containment of dangerous goods in Site of Special Scientific Interest (SSSI)
Engineering Risks	Non-critical component failure, minor infrastructure risks	Critical component/asset failure or rolling stock safety failure
Financial Risks	Financial risks do not typically give rise to an emergency management risk but might be caused by emergency management risk manifesting. Strained financial resources may exacerbate the ability to control EM Risk and respond effectively to an emergency.	
Reputational Risks	Rail emergencies can cause reputational damage, and reputational damage may hinder a Rail Entity's ability to effectively plan for and respond to a rail emergency.	
Operational Risks	Service delays, crew non-availability etc, severe weather	Major derailment, stranded rail users

Table 1: BAU risks vs EM Risks

Timely and integrated monitoring of relevant hazards will enable Rail Entities and the industry as a whole to anticipate exposures, identify vulnerabilities and prepare for risks. Hazards may include chronic stresses (such as ageing infrastructure, changing demographics, crime or environmental degradation) or short-term shocks (such as extreme weather events, transport accidents, public protest or terrorism). Chronic stresses might be driven by political instability, institutional change, climate change, economic instability, etc. and these gradually alter the performance, reputation, safety, and security of the Railway for better or worse over longer periods of time. EM Risks tend to focus on short term shocks (current issues or near-term risks) rather than chronic stresses or long-term change. Resilience principles suggest that resilience can be inbuilt into systems proactively to address long-term risks and change.

1.11 Assurance and Maturity

Rail Entities are guided to the Maturity Model process outlined in the Code of Practice on Governance (RDG-OPS-ACOP-008) section 7.2 as a means to assess their maturity against the provisions established here. A forthcoming Guidance Note on Maturity will also support delivery of these activities.

2 Provisions

This section establishes a suite of numbered provisions statements about what a Rail Entity is expected to be doing. Each provision (shown in an orange box) is immediately followed by associated guidance in the text below. This text explains in more detail what the provision is about and how Rail Entities can demonstrate compliance with it. Where possible, examples from the rail industry are provided. Unless otherwise specified the provision statements are directed at an organisation level, rather than at an industry level. It is for each Rail Entity to determine which function/s or job role/s in their organisation have an accountability and responsibility for delivering these provisions.

The RDG Emergency Management Legal and Regulatory Register (RDG-OPS-GN-064)13, a range of standards (ISO, BSI), industry guidance (RSSB standards, guidance and tools) and good practice guidelines (OECD Toolkits, CCA Emergency Preparedness) were consulted and informed this Code of Practice. Of particular note are RSSB's 'Taking Safe Decisions Framework14' and the ORR's Risk Management Maturity Model (RM3). A well-understood document in the rail industry, RM3 makes a number of provisions relating specifically to risk management as part of good health and safety management (rather than EM Risks). Therefore, a significant number of provisions established in this Guidance Note on Assessment and Prevention aligned to and adapted from an original requirement set out in RM3 for health and safety risk management.

The provisions are given as 'must,' 'should' or 'could' statements and are determined based on the following definitions established in the Code of Practice on IEM Governance (RDG-OPS-ACOP-008).

Term	Provision 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. What follows in the text below the provision is guidance about what must be done at a more detailed level to achieve the headline MUST provision.
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. What follows in the text below the provision is guidance about what should be done in order to demonstrate the SHOULD provision is being addressed.
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 2: Provision Description

2.1 ORR Enforcement Management Model

The ORR Enforcement Management Model is included below to demonstrate how the provision statements used in this CoP can be mapped against enforcement models used by regulators, noting that not all legislative elements are enforceable in this manner. The ORR statements can be cross-referenced with the provisions in **Error! Reference source not found.** as follows:

[13] RDG Emergency Management Legal and Regulatory Register (RDG-OPS-GN-064)**:** https://www.raildeliverygroup.com/media-centre-docman/acop/12969-rdg-ops-gn-064-emergency-management-legal-and-regulatory-register-final/file.html
[14] Registered members can access the 'Taking Safe Decisions' framework and guidance on the RSSB website: www.rssb.co.uk

Provision Term	ORR Description	ORR Definition
Must	Defined	The minimum standard specified by Acts, Regulations, Orders and CoPs. For example, the defined standards for welfare; the defined standards for edge protection/scaffold; the defined standard for a train protection system formed in response to it.
Should / Could	Established	CoPs and other published standards endorsed by ORR, Health & Safety Executive (HSE), industry or other credible organisations that are well known and link to legislation. For example Network Rail and RSSB standards.
Should / Could	Interpretive	Standards that are not published or widely known/available but are those required to meet a general duty. These may be interpreted by inspectors from first principles. For example, how industry dealt with the COVID-19 pandemic and the standards that were quickly formed in response to it.

Table 3: Alignment to ORR Enforcement Management Model

3 EM Risk Environment

This chapter describes the environment in which EM Risk activity takes place, signposting where necessary to the existing IEM Code of Practice on Governance[15].

3.1 Overarching need for EM Risk management

Provision 1 (Risk assessments inform EM and BC)

Rail Entities MUST have in place arrangements for assessing the risk of emergencies occurring, (MHSWR 1999, HSWA 1974) and SHOULD use this to inform emergency and business continuity management.

All employers are legally mandated to conduct regular risk assessments for all workplace hazards under the Management of Health and Safety at Work Regulations (MHSWR). Employers must:

- Assess risks to self, employees, and any other people who have contact with the workplace or work processes;
-
- Review any assessment over time to address any changes; and
- In the case of organisations with five or more employees, keep a record of risk assessment findings, and identify people who are considered especially at risk.

Under The Railways (Licensing of Railway Undertakings) Regulations duty holders must have a management system that ensures that they safely manage the operation of their infrastructure and vehicles. Duty holders must carry out risk assessments, ensure where there is a duty of care for others that risks have been reduced 'so far as is reasonably practicable – SFAIRP' (also a general requirement of the Health and Safety at Work Act, 1974). Risk assessments for significant risks should be assessed in accordance with the RSSB's Common Safety Method for Risk Evaluation and Assessment Regulation (RSSB, 2017). Furthermore, they must co-operate when acting to safely operate their part of the railway system. Co-operation takes place at the strategic level, for example: in planning to manage interface risks, and at the tactical, local, and day to day level, where systems are in place to manage hazards and prevent accidents.

The ROGS require most Rail Entities to maintain a Safety Management System (SMS) (Reg 5). They also place a specific duty on Rail Entities to carry-out and keep up to date risk assessments (Reg 19) and put in place measures necessary to make sure the transport system is run safely. The regulator, the Office for Road and Rail (ORR) also recommends that potential emergencies arising from tasks are identified as part of risk assessments [Risk Management Maturity Model (RM3) RC5 Emergency Planning]. ORR also highlights the importance of EM as part of the SMS and is the 'last layer of protection' in preventing escalation of an already unfolding incident.[16] The implication being that other layers of protection and controls will be in place before that.

Adapted from the Civil Contingencies Act (2004) section on 'Risk Assessment'[17], the wording below provides a useful overview of what an organisation should do in order to link an understanding of circumstances or events which may lead to an emergency occurring, to the plans and arrangements to prevent (where possible) and to respond to the emergency. It is therefore good practice to:

- Periodically assess the risk of an emergency occurring.
- Periodically assess the circumstances under which a Rail Entity might need to provide (or support) an emergency response.

[15] RDG Emergency Management Legal and Regulatory Register (RDG-OPS-GN-064): https://www.raildeliverygroup.com/media-centre-docman/acop/12969-rdg-ops-gn-064-emergency-management-legal-and-regulatory-register-final/file.html
[16] Section 131 of ORR's (2017) Strategy for regulation of health and safety risks.
[17] Although the CCA duty to carry out risk assessments only falls to category 1 responders (and rail entities are only category 2 responders under the Act), the explanation is useful to highlight how risk assessments should inform emergency management activities.

- Maintain plans and arrangements to provide (or support) an emergency response.
- Maintain plans and arrangements to:
  - prevent the emergency;
  - reduce, control or mitigate its effects; or
  - take other action in connection with it.
- Periodically review and amend any plans and arrangements.
- Collaborate and share all or part of assessments made, and plans maintained, with relevant partners to facilitate:
  - preventing an emergency;
  - reducing, controlling or mitigating the effects of an emergency; or
  - enabling other action to be taken in connection with an emergency

These activities are likely to be undertaken through collaboration between various functions which contribute to risk and emergency management. This includes risk management specialists, emergency management specialists managing the Rail Entity's response to emergencies, business continuity specialists managing the continuity of critical activities in the event of a disruption and functions such as Security, IT, Asset Management and Health & Safety. #

This overarching provision underpins the rest of the provisions within this CoP.

3.2 Integrating EM Risk into Organisational Management

Provision 2 (Business Integration)

[EM] Risk management processes **SHOULD** be an integral part of management and decision-making and integrated into the management system governance, structure, operations, and processes of the Rail Entity. [ISO 31000]

Risk management, specifically the management of EM Risks, should be integrated into normal organisational management and decision-making activity of the Rail Entity, so that there is a systematic approach to risk control, even during periods of change [18]. It is good practice for:

- EM Risk to be recognised as part of the overall risk to the organisation and visible within the Rail Entity's risk management structures, documentation and processes.
- The Rail Entity's Top Management to be able to use the completed risk register to direct strategy and assess organisational risk exposure against its risk appetite.
- Top management, risk management professionals and EM professionals to be able to explain the relative significance of EM Risks within the range of organisational risks, and how important EM is to the organisation.
- The Rail Entity's risk appetite to inform resources and time allocated to EM Risk management (see provision 4 on Risk Appetite).
- Top management to be ready, able and encouraged to test strategies put forward to reduce exposure to risk from whatever source.
- Those responsible for EM Risk management activities to be using industry good practice to inform their practices and procedures.
- EM, like health and safety, and security, to be embedded in day-to-day practice and culture.
- Ownership may need to be pushed down to local level to generate culture of resilience, as these owners can be best placed to control some of the risks, rather than through a large central function.

3.3 Understanding the organisation and its context

[18] Much of this section is informed by the ORR's RM3 guidance on integrating health and safety risk into risk management processes and arrangements.

Provision 3 (Context)

[EM] Risk management SHOULD relate to the Rail Entity's purpose, governance, leadership and commitment, strategy, objectives, and operations. [ISO 31000]

The Rail Entity's risk management framework (the overall approach to managing risk) should be customised to the Rail Entity's needs and culture, as well as to the internal and external context. It is good practice for the risk management framework to:

- Consider personnel as well as process/system EM Risks.
- Consider the way work is done in reality.
- Engage employees, volunteers and/ or their representatives.
- Identify relevant external stakeholders – to involve them in controlling or planning for risks and to understand their needs (see Section 7 EM Risk Communication, Collaboration and Consultation).
- Recognise the impact of ageing assets, interfaces and shared risk.
- Apply human factors knowledge about behaviours.
- Consider both the risks of performing work and the impact of work on other risk controls.

The Rail Entity should determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of the organisation. These issues are influenced by the Rail Entity's overall objectives, its products and services, and the amount and type of risk that it may or may not take (See provision 4 on Risk Appetite). These points also support embedding EM into BAU practices (See provision 2 on Business Integration) and supporting cultural change.

External Context might include	Internal Context might include
The social, cultural, political, legal, regulatory, financial, technological, economic, and environmental factors, whether international, national, regional, or local. Key drivers and trends affecting the organisational objectives. External stakeholders' relationships, perceptions, values, needs and expectations. Contractual relationships and commitments. The complexity of networks and dependencies.	Vision, mission, and values. Governance, organisational structure, roles, and accountabilities. Strategy, objectives, and policies. The organisation's culture. Standards, guidelines, and models adopted by the organisation. Capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, intellectual property/assets, processes, systems, and technologies). Data, information systems and information flows. Relationships with internal stakeholders, considering their perceptions and values; contractual relationships and commitments. Interdependencies and interconnections.

Table 4: Context

3.4 Risk Appetite[19]

Key Terms

Risk appetite [also known as risk tolerance] defines the level and type of risk that an organisation is willing to pursue or tolerate in order to achieve its goals. It aligns the risk management strategy with the vision, mission, values, and culture. Risk Appetite addresses:

Optimal risk position: the level of risk with which an organisation aims to operate.

Tolerable risk position: the level of risk that can be tolerated by an organisation having regard to its legal obligations and its own prioritised activities.

Being clear about Risk Appetite helps organisations to make informed management decisions. Defining both optimal and tolerable positions clearly sets out both the target and acceptable position in relation to achieving the organisation's prioritised activities. Defining organisational risk appetite:

Supports informed decision-making and performance improvement.

Reduces uncertainty to the delivery of prioritised activities.

Improves consistency across governance mechanisms and decision-making.

Focuses on organisational priority areas, informing spending and resource allocation.

Provision 4 (Risk Appetite)

Rail Entities **SHOULD** clearly articulate their risk appetite, so that this informs decisions about how EM Risks are managed and resource allocation.

Rail Entities should clearly articulate their risk appetite, however it is noted that historically this is not always shared. They may document this in the form of a **risk appetite statement**. When developing their risk appetite, the organisation should consider legal and regulatory obligations, the norms of the environment and the sectors in which it operates, its own strategic objectives and culture, as well as governance and decision-making processes. Risk appetite is also informed by contractual arrangements, timescales, obligations and funding any given Rail Entity is operating under.

The stages involved in developing risk appetite statements (adapted from IRM, 2017) are:

- Identify stakeholders and their expectations, together with analysis of risks in the risk register.
- Establish a set of qualitative and quantitative statements about risk appetite.
- Establish a set of qualitative and quantitative statements acceptable risk tolerances.
- Reconcile the risk appetite, risk tolerances with the current level of risk exposure and plan actions to bring current risk exposures into line with risk appetite.
- Formalise and ratify a risk appetite statement(s), communicate the statement with stakeholders and implement accordingly.

It is good practice for risk appetite statements to:

- To be shared so that those who own risks or their controls are aware of how the organisation wants to address different kinds of risks and impacts.
- Align to strategic objectives.

[19] This section of the CoP is informed by the 'Risk Appetite Guidance Note' published in 2021 by the UK Government Finance Function.

- Provide a structure the Rail Entity to make decisions with about risks which exceed risk appetite.
- Drive thinking about results and outcomes the organisation seeks to realise, as well as about what would need to change if outcomes were not acceptable.
- Describe the organisation's typical challenges and justifications for different outcomes.
- Describe the organisation's acceptable behaviour in reasonable circumstances. Risk appetite statements should be adapted and applied to help make decisions in novel circumstances.
- Be set against a sliding scale, with relevant descriptors (separate from scales used to assess the likelihood and impact of a risk).
- Dynamic and updated as necessary to reflect any significant changes.

The Government Finance Function provides an example table of risk appetite levels by risk category and a summary risk appetite statement[20] which may help Rail Entities develop risk appetite statements. The IRM Risk Appetite Statements document[21] provides an example from Network Rail published in its 2015 Annual Report and Accounts.

3.5 Ownership, Assurance & Oversight of EM Risks

The Rail EM CoP for Governance Section 4.2 "IEM Organisational Governance Structure" outlines provisions for governance structures in general, and which relate to risk management in particular (e.g. the requirements of the Executive Risk Committee and Local Business Risk Committees set out in table 4). The provisions established in the RDG-OPS- ACOP-008- Governance relating to governance structures will not be repeated here.

Key Terms

Effective risk management involves two key roles: risk owners and control owners. The organisation must be able to effect change in order to control a risk.

- The risk owner is the individual or group accountable for managing and mitigating specific risks within a project or organisation.
- The control owner is accountable for designing, maintaining and operating controls to manage those risks effectively.

The risk owner and control owner may or may not be the same person. In the rail industry, the larger the risk, the more senior the risk owner is likely to be. In some organisations, a member of Top Management may own the largest risks, as this affects how those risks, and their controls are maintained and monitored.

Provision 5 (Leadership)

Rail Entity leaders **SHOULD** demonstrate leadership and commitment to the management of EM Risks. (ISO 45001, Clause 5.1 Leadership and Commitment)

Top Managers who demonstrate accountability, as well promoting and supporting a positive EM culture, together with effective governance structures, are vital for ensuring that EM Risks are considered and addressed within risk management practices and processes. Top Managers demonstrate good practice in leadership and commitment with respect to the EM Risk by ensuring:

- The risk process and EM objectives are established and are compatible with the strategic direction of the Rail Entity.
- The integration of the EM Risk requirements into the Rail Entities business processes;
- The resources needed for the EM Risk activities are available.
- The importance of effective EM and of conforming to the requirements of the EM Risk management process are communicated.
- The EM Risk activities achieve their intended outcome(s).

[20] https://assets.publishing.service.gov.uk/media/61239758e90e0705481fc085/20210805_-_Risk_Appetite_Guidance_Note_v2.0.pdf

- Safety decisions are rational, equitable and defensible.
- Cultural and contractual arrangements are designed to support the leadership stance.

A lead Top Manager for risk is identified, whilst not absolving individual Top Manager from responsibilities for any specific risks or contribution to broader support.

Provision 6 (Framework)

The Rail Entity **SHOULD** have in place an overarching risk management framework with clearly articulate associated processes, roles, and responsibilities, for managing [EM][21] risks.

An effective framework and governance structure, specifically in relation to EM Risk articulates: The organisation's *risk appetite*, how it is understood and informs decisions related to resource allocation for prevention and preparation (See Provision 4 Risk Appetite).

How *Existing EM Risks* are owned, mitigated or managed; and then:

- Effectively recorded and reported; and
- Monitored and reviewed.
- How *new EM Risks* are scanned for, identified, controlled and where necessary planned for.

It is good practice for the Rail Entity to define and document roles, responsibilities, and accountabilities for conducting EM Risk management activities, including:

- Risk anticipation (using information sources to identify new information about risks);
- Risk analysis and evaluation (using information to understand risks and impacts and how these are currently controlled and whether these are within risk appetite);
- Risk controls and treatments (implementing controls and treatments to ensure that target risks positions are within risk appetite (where possible);
- Risk monitoring and review;
- Risk communication (collaborating with and sharing relevant information with stakeholders internally and externally).

Resourcing should be proportionate, reflecting the size, complexity and profile of the organisation. People involved in EM Risk management typically undertake one or more of the following roles:

- Those who 'own' EM Risks in each part of the organisation.
- Those that operate risk controls.
- The process owners who create and maintain systems of risk control.
- Subject matter experts / advisors who may contribute to understanding the EM Risk.
- Those who undertake EM assurance and audit (internal or external) activities.
-

Provision 7 (Lines of Defence)

Rail Entities **SHOULD** have in place a Three Lines of Defence model for the assurance and audit of EM Risks.

The Three Lines of Defence (3LoD) model establishes the assurance and audit of several functions including risk management activity. The purpose of 3LoD is to ensure the effective and transparent management of risk and is detailed in the CoP on Governance in section 4.2. The specifics as they relate to risk management are detailed here and illustrated in Figure 3.

- **1LoD: Risk and control owners.** Their roles involve identifying, monitoring and managing risks in the day-to-day, which includes control effectiveness testing.
- **2LoD: Typically provided by an independent risk/assurance function.** This establishes independent oversight of the 1LoD, verifying that frameworks are effective and evaluating

[21] This is written in brackets because EM Risks are only one kind of risk the organisation should be considering, however only EM Risks are being considered in this document.

progress of ongoing remediation activity or IEM assessments. The Rail Entity's 2LoD assurance function should regularly review the effectiveness of the EM Risk control environment as part of their ongoing oversight/assurance plan.

- **3LoD: The independent audit function.** It is completely independent from the remainder of the organisation and is typically divided into internal and external audit. It is there to establish oversight of the risk management environment overall. The audit plan may include random sample control testing. Rail Entity 3LoD assurance function should regularly review the effectiveness of the EM Risk control environment as part of their ongoing audit plan.
- It is good practice for any findings arising out of assurance and audit reviews to trigger a review of the root-causes to avoid re-occurrence, and a review of the associated risk and controls to improve the control environment (See Section 6 Monitoring and Reviewing).

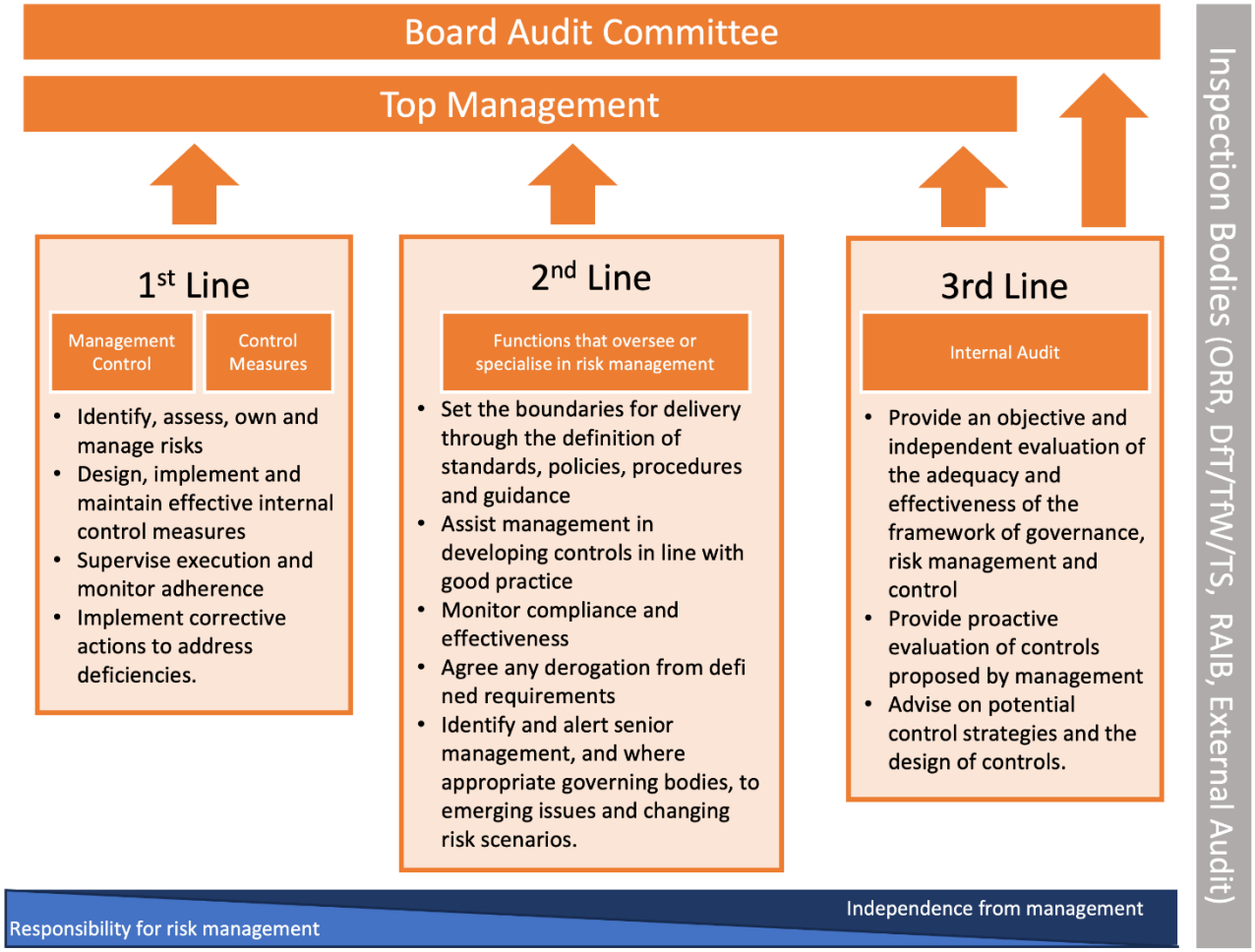


Figure 3: Adapted from Three Lines Model, taken from The Orange Book (HM Treasury, 2023)

3.6 Criticality Assessment

Key Terms

A ***criticality assessment*** is an assessment which identifies and ranks the most critical assets/activities in the organisation's operations (facilities, systems, sites, property, information, people, networks and processes). Identifying criticality helps to prioritise the allocation of resources to where they are most needed.

Asset/activities refers to the required assets and/or activities the Rail Entity is materially dependent on to meet its organisational objectives including the safe, secure, and reliable provision of services to rail users.

Critical National Infrastructure (CNI) refers to those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life (Cabinet Office, 2018).

Provision 8 (Asset/Activity Interdependency)

Rail Entities owners **SHOULD** understand systemic dependencies between their assets and activities. [OECD Policy toolkit on governance of critical infrastructure resilience]

Those accountable for the day-to-day management of an asset/activity (Asset/Activity Owners) should understand the how the asset/activity links to or depends on other assets/activities, both within and outside the railway. Systematic dependency mapping is a dynamic and ongoing process essential for effective risk management and resilience planning. It helps in identify critical assets/activities (see Provision 9 Criticality) and vulnerabilities (see Provision 13 Vulnerability Assessment) and informs the development of proactive measures to mitigate shared risks and controls (see Provision 29 Sharing and Cooperating).

A systems approach to critical infrastructure resilience tackles criticality in the whole system, rather than just the asset: "*Some of the system's assets are more critical than others, because of dependencies or (non)-existing redundancies for instance. A system approach allows for prioritising the most critical components, through dependency modelling and criticality assessments, as well as addressing weak points that otherwise create critical vulnerabilities for the entire system." (OECD, 2019).* Systematic dependency mapping should be used to identify concentration risk and single points of failure.

Asset/Activity Owners may need to employ one or more if the following approaches to map systematic dependencies and may consider tooling to support the activity:

- Identify prioritised assets and activities: Consider both physical assets (like infrastructure, rolling stock, track, and control centres) and non-physical elements (like timetabling systems or communication networks).
- Map geographical dependencies: Analyse geographical dependencies where key rail assets are located. This may include reliance on external critical infrastructures like power supplies, fuel supplies, water supply systems, or telecommunication hubs.
- Assess the dependence on external suppliers and service providers, including contractors for maintenance (entities in charge of maintenance) and logistics services.
- Establish dependency relationships: Develop a relationship mapping to visualise the connections and dependencies between different rail assets and external systems. Use this mapping to understand how one asset or activities could affect others.

Provision 9 (Criticality Assessment)

Asset manager/activity owners **SHOULD** be accountable for assessing, documenting, and communicating the criticality of their assets/activities to stakeholders.

Those accountable for the day-to-day management of an asset/activity should work with appropriate technical subject-matter experts (SMEs), EM and BC colleagues to assess the criticality of their asset/activity. A Business Impact Analysis (BIA), typically conducted as part of BC management may

provide a useful starting point to inform EM criticality assessments. It is good practice for assessment inform a risk-based approach to the ongoing management, maintenance, and assurance (including exercising) of the asset/activity. In assessing asset/activity criticality Rail Entities should consider (non-exhaustive):

- Other assets/activities which are dependent on it (e.g. a railway line or station serving multiple Rail Entities).
- If an incident occurred involving that asset/activity:
    - How many people, including rail users, staff, suppliers, contractors, members of the public, other Rail Entities (TOCs, FOCs, infrastructure managers etc.) could be physically harmed or impacted by the incident;
    - The nature and extent of that harm or impact (travel delays or disruption, injuries, fatalities, diverted freight, environmental contamination);
    - The availability of existing, and proven substitutions or redundant capacity (e.g. rail replacement routes or as alternate line routing, including via other modes), where functionality and capacity are comparable to the asset/activity affected;
    - The proximity (including above and below) of the asset/activity to vulnerable sites and structures e.g. crowded places & 'Sites of Special Scientific Interest' (SSSIs); and
    - The regional and national economic impact of the asset/activity were unavailable (including Critical National Infrastructure assessments as required under the National Railway Security Programme (NRSP) may provide a helpful starting point).
- Demand upon/usage of an asset/activity over time, considering normal peak usage plus any conditional seasonal variances.

The NR Common Consequences tool provides a method of estimating the potential safety consequences (such as injuries or fatalities) arising from a train derailment. It establishes a location-based consequence rating and has the ability to compare different assets in terms of overall safety criticality. This could be used by Network Rail to identify single-point failures and other areas of risk on critical freight and passenger paths, necessitating the development of appropriate industry and multi-agency controls.

4 EM Risk Identification (Anticipation)

Key Terms

Risk identification is the process of finding, recognising and describing risks so that they can be assessed or analysed, and this knowledge can inform the allocation of resources to manage the risk or prepare for the consequences.

Data management involves the collection, storage, analysis and distribution of data and information so that it provides current, relevant, and useful insight into current or potential issues, risks, disruption, or shocks. Data management involves finding out information about existing known risks as well as identifying new risks.

Risk velocity refers to the rate at which a risk event develops from its onset to its peak impact. Understanding risk velocity can help to understand how quickly an organisation must respond to indicators the risk may be manifesting.

Before being able to manage a risk, a Rail Entity must first identify it as such. Anticipating risks is about having a process for finding and reviewing sources of risk intelligence so that they inform the risk assessment and evaluation processes outlined in the following chapter. Data can be gathered and analysed in advance (covering shorter timeframes – up to five years – or longer 5-10 years) and it can be gathered in real-time through monitoring. Data gathering and information management will help identify new and emerging risks, pick up trends and long-term changes, and manage known risks.

4.1 Anticipating Risks through data gathering and horizon scanning

Provision 10 (Process for Anticipating Risks)

Rail Entities **should** define, establish, and regularly review and improve a systematic process for data and intelligence gathering around EM Risks to allow them to be identified and understood - which then allows them to be assessed, evaluated, treated and monitored.

The CoP for Governance articulates the need for information to be reported through each level of the governance structures to make effective decision-making at each stage. Therefore, Rail Entities should have in place an agreed and understood method for conducting data and intelligence-gathering activities; and for information and insight arising from these activities to be disseminated in governance arrangements for risk and risk reporting (hindsight, insight, foresight). This will allow the Rail Entity to identify and understand new information relating to existing risks, as well as to identify new and emerging risks and trends, and long-term changes which may affect the organisation's strategic objectives.

It is good practice for the Rail Entity to:

- Have a process for data gathering and analysis with a clear scope and purpose which identifies the kinds of information sources used, and timeframes involved for current state (issue monitoring), short-term future states (risks / emerging trends) and long-term states (changes).
- Understand the risk velocity to inform the state of readiness that should be in place should the risk event should it manifest.
- Understand the 'normal' operation of an activity/asset and have sufficient resources, technology, processes, and controls in place to identify where an activity/asset is experiencing abnormal behaviour and note that any monitoring regimes should be cognisant that abnormal behaviour may have slow or rapid onset.
- Report incidents, deviations and near misses by exception where risks are starting to become live issues, to provide timely escalation and action.
- Subscribe/register to available alert/notification services that can provide timely notification of a potential change in risk profile.
- Have an approach to EM Risk management which is adaptable and responsive to change highlighted in monitoring activities.

Real-time monitoring

Real-time monitoring and reporting involves collecting, tracking, and sharing data immediately after its collection. Real-time data can highlight **current issues** affecting the organisation now (whether previously identified as risks, or unanticipated emerging issues). This information will enable those responsible for preparation, response and mitigation measures to monitor disruption, shocks, or incidents as they unfold and act on the information provided to address the issue. Real-time monitoring can feed into early-warning systems and ongoing assessment, prevention, and preparedness activities, especially if linked to Key Risk Indicators (see Provision 26 Key Risk Indicators). Automation of real time monitoring can make decision-making quicker, simpler and better informed.

Regular data gathering and deep dives

Risk information is also captured in future-orientated documents, including risk registers, control documentation and change management procedures. Risk registers tend to deal with risks which might manifest in the relative short-term, e.g. the next 6-12 months (see the box below on timeframes), whereas longer-term risks, trends and changes tend to be captured in horizon-scanning and change management programmes. Where risks are poorly understood, deep dive sessions involving subject matter experts can help Rail Entities get a better understanding of the implications and potential control options.

The organisation may have to put in place temporary ad hoc arrangements to manage short-term risks where this cannot be addressed through BAU processes[22]. In contrast with longer-term risks, there is theoretically time to reorganise organisational practices, infrastructure design and so on, to address the potential or anticipated change (see Provision 20 Resilience by Design/ Through Change).

Horizon scanning and scenario planning

This is the systematic examination of data about potential longer-term changes and futures. It is an iterative process which informs the long-term IEM and resilience strategy of an organisation and is inherently forward-looking. A wide range of factors are normally considered which could include the organisation's strategy, sectoral changes, expected service lifetime of buildings, plant and equipment. Consideration of risk over different time horizons will allow Rail Entities to better track the evolving risk landscape and to identify capability gaps and risk treatment measures that may need to be tackled over a longer-term period.

Horizon scanning generally adopts longer timeframes (+ 5 years) but this depend on both the requirements of the individual organisation (for example, the NSRA covers up to 20 years ahead) or the specific issues or risks under consideration. It should encompass a broad scope to enable both potential developments of the external context (covering political, economic, social, technological, legal/regulatory, environmental and security emerging trends) and the internal context (covering the organisation and the rail industry) to be monitored. 'Scenario planning' is a related activity which could be adopted by Rail Entities to provide insights in to possible alternative future risk and operating environments to help inform strategy planning.

Table 5:

[22] To all intents and purposes this is what a Major Incident is – an incident of such scale and severity that it cannot be managed using BAU incident management procedures.

Different audiences consider different timeframes when they talk about risk and the potential for change, so it is useful to appreciate different timescales and different risk activities within those timeframes. There are no hard or fast rules about exactly where to draw the line – make clear if you are using terminology that might infer a timescale, that you are specific about the timescales you are using so there is no confusion or potential for misunderstandings. Issues are hazards and threats which have materialised and are having an effect on the organisation now. Real-time monitoring identifies new and ongoing current issues are affecting the organisation now. Risks are potential situations which might arise at some point in the future. Risk registers tend to focus on risks which might arise within the next 6-12 months. The working environment within which the risk might occur is likely to look quite similar to the working environment as it looks today. Data gathering identifies emerging risks not previously identified on the risk register (emerging risks) and new details about known risks. Horizon scanning is an active process associated with longer timescales and timeframes – often 3, 5, 10 or 20 years into the future. It relates to the identification of areas of change, the evolving risk landscape and larger scale changes and risks which require longer lead times to plan for. Both the external and the sectoral environments might be quite different by then. The further into the future we start to look the greater the uncertainty, and the less certain we can be about what it will look like and what our specific plans need to be for managing risks. Scenario planning is about identifying a specific 'issue of concern' and exploring how, from the conditions of the present day, different alternative outcomes may emerge. . Scenario planning aims to define critical uncertainties and develop a range of plausible scenarios in order to help an organisation identify their assumptions about the future, discuss the potential impacts and evaluate how the organisation may respond. Scenario planning helps foster organisational anticipation. Acute risks give rise to discrete events which can be relatively easily pinned to one time and place, whereas the impact of a chronic risk materialising might be more geographically and temporally dispersed (e.g. in multiple places and over a long time/multiple times).

Table 6: Timeframes and timescales considerations when talking about risks

4.2 Information sources to inform risk identification and assessment

Provision 11 (Gathering Data)

Rail Entities **SHOULD** conduct a broad review of internal and external data sources to inform their identification and assessment of EM Risks. [ISO 31000]

A wide range of sources of information are available to support data gathering and intelligence gathering around risk management. A table of suggestions is detailed below – it should be noted that many more risk specific sources may be available.

Real time information sources

Possible alert/notification services which can inform real-time warning may include:

- UK's Joint Terrorism Analysis Centre and Security Service's (MI5) terrorism threat levels
- Flood (and other hazard) warnings provided by the relevant national body
- Met Office Severe Weather Warnings
- Infectious disease and outbreak data from the UK Health Security Agency (UKHSA) data dashboard
- Signing up to local alert services such as the 'City Alert' provided by the City of London
- Being embedded in any LRFs that the organisation passes through and being included in incident distribution normally facilitated via Resilience Direct.

Other periodically updated sources of insight and risk information

Information sources for anticipation activities might include:

- National Security Risk Assessment (NSRA): This is a classified assessment of risks that could cause a national-scale emergency in the UK and informs plans to mitigate those risks. Some members of Rail Entities' Security Teams may have access to elements of this document depending on security clearance. The horizon on this document is up to 20 years because it includes societal changes to political structures and the economy.
- National Business Resilience Planning Assumptions: This guidance helps companies to check that their resilience planning is in line with the government's assessment of the impact of a range of potential threats and hazards (Cabinet Office, 2015).
- UK National Risk Register (NRR) : The NRR is the public facing version of the NSRA and is the government's assessment of the most serious risks facing the UK. It provides the government's updated assessment of the likelihood and potential impact of a broad range of risks that may directly affect the UK and its interests. Several of the risks are specifically-rail related – e.g. a malicious rail incident, a cyber-attack on the transport sector, a rail accident but many of the listed threats/hazards could impact the railway.
- Local and Community Risk Registers: Local Resilience Forums (LRFs) in England and Wales, and Local Resilience Partnerships (LRPs) in Scotland, publish Community Risk Registers (CRR) which translate NRR risks into the local context for the geographic area covered. Each LRF may add additional risks which are locally relevant or ignore national risks which are not present in their area.
- Joint Organisational Learning – Lessons Identified : JOL provides a structured mechanism for capturing, analysing, and sharing lessons identified from incidents, exercises, and operational experiences across multiple agencies, including rail entities. It enables the systematic application of improvements to risk management and emergency preparedness by ensuring that past incidents inform future resilience planning.
- Models: A risk model is a mathematical representation of a system (e.g. the rail network), commonly incorporating probability distributions about how frequently X might happen. Models use relevant historical data as well as information from "expert elicitation" from people versed in the topic at hand to understand the probability of a risk event occurring and its potential severity. Various models exist in the rail industry including NR's Common Consequences Tool.

- Risk and Horizon Planning Reports: Regular insight reports such as the World Economic Forum's annual Global Risk Report and the BCI's annual Horizon Scan Report.

Rail industry specific sources of information

- RAIB Incident/Loss records: The Rail Accident Investigation Branch (RAIB) is responsible for investigating the causes of railway accidents and incidents where we believe our investigation will bring safety learning to the industry. They will identify the factors that may lead to a similar accident or make the consequences worse and highlight gaps in the railway industry's safety defences that are revealed during their investigations. Common trends and occurrences are summarised within the RAIB Annual Report. Organisations also often hold their ow' records of historical incidents and their consequences in the form of post incident reports – these can be valuable sources of risk information.
- Industry and organisational accident and incident records: Industry and organisations should maintain records of accidents and near miss events. Sources of information include Safety Management Intelligence System (SMIS), Close Call System, National Incident Reporting System, Rail Notices, Confidential Incident Reporting & Analysis Service (CIRAS), Safety Alerts IT Tool (SAIT) .
- RSSB: Horizon Scanning capability and services, RSSB Annual Health and Safety Report, Common Hazards for the Management of Industry Safety (provides a common way of classifying hazards that could be used throughout the GB rail industry to promote a consistent approach to hazard identification and management), Safety Risk Model (SRM – integrates common hazards and provides a network-wide view of risk and can be used to support risk-based decision making), Signal Passed at Danger (SPAD toolkit – precursor events to buffer stop collisions and derailments).
- NR Common Consequences tool. This provides a method of estimating potential safety consequences (such as injuries or fatalities) arising from a train derailment. It establishes a location-based consequence rating and has the ability to compare different assets in terms of overall safety criticality.
- National Freight Safety Group (NFSG). Undertakes a strategic look at new and emerging risks for the freight sector by making use of RSSBs horizon scanning capability. Ensuring that NFSG is prioritising the right risk areas.
- Rail Industry Risk Forum, Rail Incident Care Team Management Group and RDG Emergency Planning Group, Control Forum – information sharing between peers.
- A wide range of subject matter expertise on specific risks is also available across the rail industry, government entities, scientific community, academic institutions and related organisations such as the aviation or public transport industry.
- Train Accident Risk Group (TARG). Monitors the strategic risk profile and industry safety performance related to train accident risk on the national rail network (excluding at level crossings).

4.3 Defining risks clearly

Key Terms

A ***risk taxonomy***, also known as a risk library, is a structured framework that categorises and organises various types of risks, providing a standardised way of identifying and describing them. By using the same terminology, stakeholders can consistently compare like with like and more easily aggregate risks across multiple organisations.

Provision 12 (Risk Identification and Terminology)

Rail Entities **SHOULD** use consistent terminology for identifying and defining risks and they **COULD** use a taxonomy as the basis for this. [OECD Policy toolkit on governance of critical infrastructure resilience AND RSSB: Common Hazards for the Management of Industry Safety (CHAMOIS)]

To help them to measure and monitor EM Risks and to communicate clearly with other risk partners, Rail Entities should use clear definitions and consistent terminology when referring to threats and hazards, vulnerability, exposure and capacity, which all contribute to EM Risk.

Using a common way of classifying hazards promotes a consistent approach to hazard identification and understanding of safety risk, leading to an efficient, consistent and robust way of managing safety. It is possible to monitor impacts without clearly defined risks, but it is difficult to use this information effectively to understand or measure risk and develop appropriate treatment measures. Using a risk taxonomy (See Appendix E: Taxonomy of Threats and Hazards) offers several benefits, including:

- **Taking safe decisions**: Supports robust risk-based decision making.
- **Compliance**: Demonstrates that Rail Entities have ensured safety 'so far as is reasonably practicable' as required by law.
- **Standardisation**: A standardised framework for categorising and naming risks, helping ensure consistency in risk assessment and reporting across the organisation and partners.
- **Improved Communication:** A common risk language facilitates better communication among stakeholders, making it easier to discuss, understand and in turn manage risks.
- **Risk Identification**: It aids in the systematic identification of risks by providing a structured way to categorise and classify potential threats and hazards.
- **Risk Assessment**: A risk taxonomy allows for more accurate and efficient risk assessment by breaking down complex risks into manageable components. Supporting the use of the Common Safety Method for Risk Evaluation and Assessment (CSM RA)[23].

Rail Entities could develop the taxonomy further to include any additional threats and hazards identified through their review of information sources (see Provision 10 Process for Anticipating Risks). RSSB's CHAMOIS project offers a common way of classifying GB rail hazards and is summarised in the box overleaf.

[23]Guidance on the Common Safety Method for Risk Evaluation and Assessment: https://www.rssb.co.uk/-/media/Project/RSSB/RssbWebsite/Documents/Registered/Standards/2020/09/16/10/37/GEGN8646-Iss-1.pdf

Rail Information Box: RSSB: Common Hazards for the Management of Industry Safety (CHAMOIS)

RSSB's CHAMOIS project (2023) developed a common way of classifying GB rail hazards. This promotes a consistent approach to hazard identification and management, and a consistent understanding of safety risk, so that rail safety is managed efficiently, consistently and robustly.
The purpose of hazard description is to provide a meaningful, common, precise, easily understood, and unambiguous meaning to a hazard, so that those responsible for risk and hazard management can effectively and efficiently discuss the hazard and its appropriate management.
The CHAMOIS project defined and structured both a hazard list and a rail system ontology at three levels, each level including more detailed granularity. There are eighteen Level 1 Hazard categories and six Level 1 Ontology categories (See Appendix E: Taxonomy of Threats and Hazards).

As an example, the improved consistency in hazard identification arising from the common hazard lists will enable RSSB to link safety requirements in standards to the hazards that they are intended to manage. The use of common hazard lists will also improve the alignment of various RSSB safety risk management products and services (as examples, bowtie risk analysis, Safety Risk Model, safety performance measuring, standards, and R&D projects) as they will be based on a common hazard framework.

https://www.rssb.co.uk/safety-and-health/risk-and-safety-intelligence/safety-management-resources/generic-hazard-list

A complementary approach to threat and hazard identification has been adopted by East Midlands Railway:

Rail Information Box: East Midlands Railway: Review of NSRA to identify reasonably foreseeable rail hazards

The Cabinet Office's NSRA is reviewed and updated to identify the current and emerging threats and hazards. It is distributed to category two responders through Local Resilience Forums (LRF). East Midlands Railway (EMR) reviews the NSRA annually to identify reasonably foreseeable threats and hazards within rail settings for which EMR is accountable. The identified threats and hazards are recorded in and Emergency & Incident Hazard Register (there are currently 38 threats and hazards, of which 6 are viewed as critical risks, identified within the register).

Each threat and hazard is risk assessed according to a Hazard Risk Assessment Matrix and then:
- Aligned to the appropriate rail setting (e.g. Station/Depot/Train).
- Have an appropriate response plan template (aligned to appropriate SMS response plans).
- Identify dependencies to other responders, including other railway undertakings.

As a CCA Category 2 responder EMR is shares its emergency plans with other responders, enabling them to understand specific local, or operational risks and emergency response activities.

5 Risk Analysis and Evaluation (Assessment)

Risk is a consequence of interactions between a threat or hazard and the characteristics that make assets and activities critical (important to organisational objectives) and vulnerable (susceptible to adverse impacts or harm in the face of potential threats or hazards).

Key Terms

Risk analysis is the process of examining a risk to determine the impact it would cause if it was manifested and the likelihood of that happening.

Risk evaluation is the process of comparing the results of risk analysis with risk appetite to determine whether the risk and/or its impact is acceptable or tolerable.

A ***vulnerability assessment*** determines the vulnerability of an asset/activity to being lost, disrupted, taken, damaged, or destroyed.

Reasonable worst-case scenarios are not a prediction of what is most likely to happen, instead, they represent the worst plausible manifestation of that particular risk (once highly unlikely variations have been discounted).

A plausible manifestation means a scenario that, once highly unlikely variations have been discounted, is grounded in reality, and as such scenario selection will be traceable to events which have occurred within (including near misses), the UK or international rail industry or more broadly in other sectors. This approach will allow Rail Entities to undertake proportionate risk-based planning and deployment of resources when designing their control environment.

5.1 Vulnerability Assessment

Provision 13 (Vulnerability Assessment)

Station emergency plans MUST address likely instances involving dangerous goods that pass through a station where this is relevant. [ORR's Strategy for regulation of health and safety risks, Ch 5 – interface system safety. V3 (Dec 2017)]

Asset managers and/or activity owners SHOULD be accountable for ensuring the vulnerability their asset/activity is assessed, documented, and communicated to stakeholders.

These two provisions are provided as one, given the specificity of the MUST provision would be included in the SHOULD provision where a Rail Entity is responsible for a station. The specific reference to dangerous goods in a station environment is specified by the regulator and therefore an absolute requirement. Adherence only to this specific requirement would leave other assets and activities unaccounted for. Therefore, the provision provided here is more generally applicable. It may also be helpful to think of dangerous goods 'passing close by' rather than just 'through' a station.

Those accountable for the day-to-day management of an asset/activity should work with the appropriate technical SMEs and EM and BCM colleagues, and appropriate rail and EM partners to assess the vulnerability of their asset/activity.

A three-step assessment process should be undertaken to identify threats and hazards facing Rail Entities and their consequence on critical assets and prioritised activities:

- Threats and hazards: Use the developed list of threats and hazards that the Rail Entities is exposed to by filtering them by likelihood and consequence to identify those with the potential to damage, disrupt or degrade rail assets and activities. (See Provision 12 Risk Identification and Terminology).
- Exposure: Identify critical assets (infrastructure and train asset classes including any dependency on connected systems), key geographical locations (i.e. single point of failure (SPOF) locations), and activities (e.g. high-consequence dangerous goods paths with exposure outside the range of their competent operating conditions) to disruption from

threats and hazards (see Provision 8 Asset/Activity Interdependency and Provision 9 Criticality).

- Vulnerability: Understand exposure (where and how critical assets, SPOF locations, and prioritised activities and priority threats and hazards intersect); and sensitivity (i.e., high volume passenger routes or high-consequence dangerous goods paths) and adaptive capacity (i.e., the availability of viable alternative routes).
- Where the Rail Entity has primary concern for either infrastructure or train assets, vulnerabilities will link in many cases directly to the asset management strategy. Asset management is already a highly developed area and many of the processes and concepts are directly transferrable to mitigate the impact of threats and hazards (including those arising from climate change). The ISO 55000 family of international standards provide reliable advice on undertaking effective asset management. Specific guidelines for railway entities' adoption of ISO 55001 are also published by the Union of International Railways (UIC, 2016).

In assessing asset/activity vulnerability Rail Entities should consider:

- Exposure to threats and hazards;
- The complexity of the asset/activity;
- Size/scale of the asset/activity;
- Confidence of recoverability (this may be a function of the quality of documented information about the asset and currency of experience in maintaining it);
- Age/condition of the asset/activity;
- Remoteness in the context of response time;
- Site-based communication capability/restraints;
- Ease of access/egress;
- Attractiveness to hostile actors (individuals and/or group);
- The proximity of the asset/activity to hazardous sites e.g. a COMAH or REPPIR site;
- The exposure to dangerous goods in transit;
- The rate of deterioration of the asset due to use; and
- Similar assets being involved in incidents elsewhere

By considering the above criteria Rail Entities that manage stations should be able to take an informed approach to addressing likely instances involving dangerous goods that pass through a station.

Rail Information Box: Network Rail Asset Management - Climate Change Vulnerability Assessment

Climate change (the long-term shifts in temperatures and weather patterns (UN, 2023[24])), is not one single risk but as the name suggests a change in the operating environment. Climate change is however a major driver for many of the risks which Rail Entities might need to consider now as the UK is already beginning to experience some changes already. More immediate consequences of climate change include:

- Increased risk of fatigue and challenges to safe working conditions for staff working outside in more protracted periods of severe weather (extreme heat, cold, rainfall etc.).
- Increased risk of trackside fires if dry vegetation catches fire and fire-fighting organisations stretched across multiple events.
- Infrastructure failure or reduced asset condition and safety in severe weather conditions e.g. landslides, track failure in hot temperatures, flood defences overtopped.
- Reduced network availability and/or functionality.
- Challenges to maintaining safe conditions for rail users during delays and incidents.

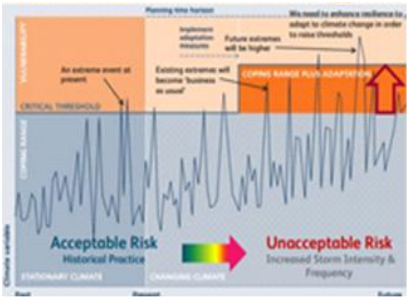
Other consequences of climate change may take longer to materialise and are therefore more speculative. These may be considered through scenario planning activity and Resilience by Design considerations (see Provision 20).

Weather-related events over the past 15 years cost Network Rail (NR) at least £3bn in delays and cancellations, insurance claims and autumn preparation. The reduction in NR's performance caused by such weather events has a negative impact on passenger and freight customers and inhibits their ability to deliver on the governments' targets.

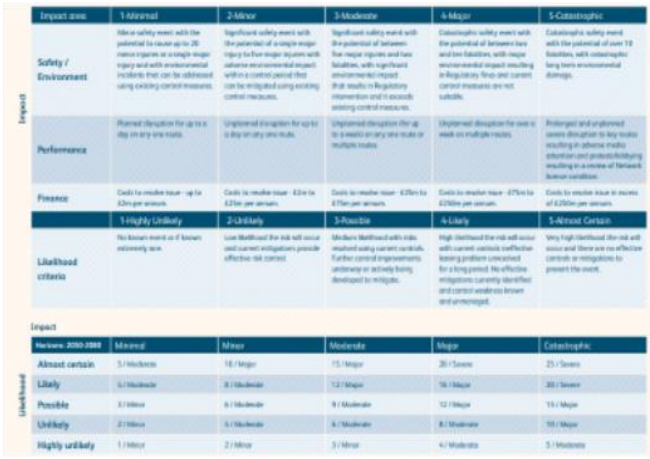
NR's Climate Change Projections Guidance (NR/GN/ESD/23) was used to assess asset risk against the latest climate change projections available (UK Climate Projections 09). Risk evaluation identified vulnerabilities across each of NR's assets with temperature, rainfall, wind and flooding being the most likely causes of significant disruption, and an understanding that local topography can have a significant impact on how these weather events affect a particular asset.

The climate change impact on each asset class was assessed against current mitigations and asset designs to determine where gaps may exist that require further investigation or adaptation to be put in place to provide additional resilience to changing weather conditions. These identify dependencies between different assets to provide a broader understanding of the challenges NR face with the future climate, and the actions required to address any system vulnerabilities.

[24] https://www.un.org/en/climatechange/what-is-climate-change



Future Climate Risk Assessment Matrix aligned with Network Rail Corporate Risk Assessment Matrix (CRAM)



An assessment was made by aligning the Future Climate Risk Assessment Matrix with NR Corporate Risk Assessment Matrix, to determine current and future risk scores, taking account of the impact of current weather parameters and their effects on NR Assets. Assessments were carried out for 2019, the 2050s and the 2080s. Scores were generated based on existing controls and designs, assuming that no new adaptation was applied. The evaluation was to determine the gaps in current asset designs, standards and controls that would result in significant disruption to the network as a result adverse and extreme weather, which could result in safety related incidents.

See NR Asset Management Weather Resilience and Climate Change Adaptation Plan: https://www.networkrail.co.uk/wp-content/uploads/2021/11/Asset-management-WRCCA-plan.pdf

Further information on NR's approach to climate adaption can be found here: https://www.networkrail.co.uk/sustainability/climate-change/climate-change-adaptation/

See also NR's reports and recommendations relating to the resilience of the UK's rail infrastructure prompted by the Stonehaven crash in August 2020: https://www.networkrail.co.uk/who-we-are/our-approach-to-safety/stonehaven

5.2 Risk Analysis

Provision 14 (Risk Analysis and Processes)

Rail Entities **SHOULD** analyse EM Risks using their own internal risk processes[25].

Risk analysis provides an input to risk evaluation decision-making about whether the risk needs to be managed or treated and how, and about the most appropriate risk treatment strategy and methods (see Provision 17 Treatment).

The purpose of EM Risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. EM Risk analysis involves a detailed consideration of

[25] This provision assumes that organisations already have well defined risk management processes for risks in general.

uncertainties, risk sources, consequences, likelihood, events, scenarios, preventative and recovery controls, and their effectiveness. An event can have multiple causes and consequences and can affect multiple organisational objectives.

Risk assessments should be a systematic and iterative process, effectively informing both short- and long-term EM, 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.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

Each Rail Entity should analyse and evaluate EM Risks using their internal risk processes to identify:

- Potential causes of EM Risk occurring (from known EM events, change arising from horizon scanning activities, relevant taxonomy threats/hazards identified through vulnerability assessments (See Provision 12 Vulnerability assessments). The CHAMOIS tool by RSSB and other models such as bowtie or fishbone models can help this process.
- The impact (assessed against Rail Entity specific impact matrices) and likelihood of those risks occurring **(i.e. fire damage to rolling stock and/or lineside infrastructure, or loss of containment of dangerous goods, leading to major accident hazard).**
- The consequences/impact should the risk occur.
- **This can be thought of as the direct the impact on critical assets and activities, other human (staff, rail users, contractors and other members of the public), economic and financial, legal, reputational, project management, political consequences of the risk, which may be second order consequences and consequences for achieving business objectives. The Legal and Regulatory Register will help Rail Entities determine their minimum obligations; however additional legal advice may be needed.**
- **It should also include considering other partners who would need to be informed of the incident or involved in its response (e.g. other rail industry partners, resilience organisations Cat 1 and 2 responders, voluntary agencies), coroners and investigating agencies, media organisations, loss adjusters and insurance organisations etc).**
- **Another aspect of impact is to consider whether the incident would lead to long term social or organisational change (e.g. a new normal).**
- The effectiveness of existing controls (confidence levels should be determined from assurance and/or control effectiveness testing to determine current/residual risk).

Target risk positions should be established, aligned to risk appetite (see Provision 4 Risk Appetite).

Provision 15 (Reasonable Worst-Case Scenario (RWCS))

Rail Entities **SHOULD** regularly determine and assess the 'Reasonable worst-case scenario' for each EM Risk and document the criteria used to determine its plausibility.

Risk analysis should be based upon a 'reasonable worst-case scenario' (RWCS) to ensure a robust evaluation of potential impacts (see Provision 14 on analysis), allowing for proportionate risk-based planning and deployment of resources when designing risk treatments.

The justification for the phrase 'worst case scenario' being preceded by the word 'reasonable' is to prevent scenarios being formulated that are considered so unrealistic or unlikely that they are implausible. Methods to determine RWCS's may include:

- Historical data analysis: Reviewing past incidents and near misses within the rail industry.
- Scientific data analysis: Using scientific data, studies, and research on the specific risk.
- Modelling: Using mathematical models and simulations to project potential worst-case scenarios based on different variables and inputs.

- Trend surveillance: Monitoring trends and emerging patterns in the industry to anticipate evolving risks and incorporate them into RWCS considerations.
- Seeking input from industry experts and professionals with domain-specific knowledge and experience to provide informed judgments on potential worst-case scenarios.
- Conducting workshops involving stakeholders to identify various scenarios.
- Cross-industry benchmarking to identify scenarios that have occurred in different contexts but share similarities in risk factors and consequences.
- The quality of information used in the assessment, the assumptions and exclusions made, and any inherent limitations of the techniques employed should be acknowledged. These factors should be thoroughly considered, documented, and effectively communicated to decision-makers to ensure transparency and informed decision-making.

Rail Entities should maintain clear and well-documented records of the RWCSs selected and the rationale behind their selection. This documentation should include the specific risk, its variations, and the criteria used to determine its plausibility.

Provision 16 (Diverse Perspectives)

Rail Entities **SHOULD** ensure that risk assessments are carried out by a diverse group of professionals and subject matter experts with a pragmatic mix of divergent of opinions, biases, perceptions of risk, and judgements. [ISO 31000]

When carrying out risk assessment to support decision making, the approach should be balanced, pragmatic and proportionate to the size and complexity of the decision and its risks. Details of requirements for employers to '*make a suitable and sufficient assessment*' are contained in the Management of Health and Safety at Work Regulations 1999 regulation 3 on risk assessment.

Decisions with significant scale and scope, higher levels of uncertainty, involving novel technology or ways of working, large scale or national in character, will involve multiple organisations and more consultation. These types of decisions require industry to work together to agree the most appropriate options to take forward and should be considered at a senior level.

When conducting significant risk assessments and to ensure good decision-taking, and to obtain a well-rounded and nuanced understanding of potential risks, Rail Entities should involve a diverse range of contributors, with diverse skills, knowledge and experience. For example, top management, safety management and technical specific subject matter experts, external partners and key suppliers (i.e., Entities in Charge of Maintenance). This will foster a pragmatic mix of divergent opinions, biases, perceptions of risk, and individual judgments. These types of assessments will likely also entail extensive consultation, particularly with other owners of the risk if it is shared. Rail Entities should also recognise the impact of human factors and potential psychological phenomena, such as groupthink[26], within the assessment process. Vigilance against the influence of these factors is essential for maintaining the integrity and objectivity of the risk assessment.

RSSB's 'Leading Health and Safety on Britain's railway' has been developed by leaders of the rail industry and is an example of an industry-wide agreed approach to voluntary collaboration. It focuses on those elements of health and safety risk management that can be improved by Rail Entities working together, both within and beyond legislative interface requirements.

[26] Groupthink is a psychological phenomenon where the desire for harmony or conformity in a group result in irrational or dysfunctional decision-making outcomes.

6 Treatment (Prevention)

Risk treatment is the process of determining the most appropriate response to a risk where current risk position is greater than the planned/ideal or outside risk appetite. It is then about managing the threat to achieving objectives. It is a vital element of good risk management that appropriate effort should be expended on risk response, action planning, and delivery, as on identification and assessment. This section also provides the 'Prevention' element of IEM, noting of course that not all risks are preventable, but are managed in other ways and explained in the provisions below.

Key Terms

Risk Treatment is the process of selecting and implementing of measures to modify risk in some way. It involves an iterative process of:

- Formulating and selecting treatment options (Avoidance: Not taking on the risk by avoiding actions that cause it. Reduction: Taking mitigation actions to reduce the risk. Transfer: Transferring all or part of the risk to a third party. Acceptance (Risk retention): Choosing to face the risk)
- Planning and implementing a treatment;
- Assessing the effectiveness of that treatment; and
- Deciding whether the remaining risk is acceptable and taking further action if needed.

Risk treatment is a vital element of good risk management and appropriate effort should be expended taking action to treat the risk, as on identification and assessment.

A ***control*** is any action or process that is implemented to reduce a risk (likelihood or impact). Controls can be a policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk.

Controls are categorised by control type:

- ***Directive controls*** say what to do. These set policy and minimum standards to be followed e.g. policies, asset strategies, ROGS, rail industry standards.
- ***Preventative controls*** stop or minimise the risk of events happening.
- ***Detective controls*** identify a risk event that has or is about to happen (e.g. KRIs and early warning notifications are common detective controls).
- **Responsive controls** minimise the impact of the risk even once it has happened. (Emergency Response Plans and Recovery Plans are common responsive controls).

There are three different control execution methods:

- **Automated**: Controls operated and enforced by a system without human intervention.
- **Semi-automated:** Automated control activity with some additional manual activity. The use of data or reports counts as automated control activity where there is automated assessment within them. E.g. identification of issues or exceptions or highlighting potential errors. Manual activity is directly linked to addressing the items highlighted by the automated part of the control.
- ***Manual***: Controls that are operated and enforced with human intervention.

SFAIRP/ALARP: The term SFAIRP is used in the Health and Safety at Work etc. Act 1974 which places duties on employers in the UK to ensure safety 'so far as is reasonably practicable' (SFAIRP). It is similar to the term ALARP which refers to the principle of reducing risk to 'as low as reasonably practicable'. Although SFAIRP and ALARP are different in law, they are used interchangeably in the GB rail industry and are regarded as representing the same health and safety legal test (RSSB 'Taking Safe Decisions framework').

6.1 Risk Treatment

Provision 17 (Treatment)

Rail Entities MUST take all steps, so far as is reasonably practicable, to reduce safety related EM Risk. (Health & Safety at Work Act 1974)

Rail Entities SHOULD formulate and select risk treatment options to reduce all EM Risk to within risk appetite. (ISO 31000)

Rail entities must reduce safety related risks SFAIRP. Selecting the most appropriate risk treatment option/s involves balancing the potential benefits from achieving organisational objectives and obligations against the costs, effort, or disadvantages of implementation. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The viability of options may change over time, so it is important to regularly review the approach taken.

Specific statutes, regulations or standards may set out specific, prescriptive requirements that must be met. For example, technical requirements may mandate certain safety parameters or performance inputs or outputs. Prescriptive requirements in these categories must be met at all times and Rail Entities need to be familiar with all such requirements that relate to their business. These requirements are not enough in themselves. They are ‘essential’ but not ‘sufficient’ for safety. Over the years, ORR has moved from a prescriptive measures regime to a risk-based, goal setting approach to safety management.

Risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The judgement shall ensure the aggregated contribution of all broadly acceptable risks does not exceed a defined proportion of the overall risk (CSM RA Regulation – Annex I, point 2.2.3).

A key determinant of what treatment options must be implemented is the concept of SFAIRP and Rail Entities must make a suitable and sufficient assessment of EM Risks that may have safety implications (ORR, 2017 GEGN8646).

When risks are assessed as unacceptable, it means putting in place the highest level of protection considering what can be done and whether it is reasonable given the circumstances. In the context of reducing risks, it also considers the operating environment, the benefits to safety gained and costs (money, resources and creating different risks). Deciding which risk treatment option(s) to use should not just be financially driven; decisions should align with Rail Entity's objectives, legal and regulatory duties, risk criteria and available resources. See Provision 21 (Investment Decisions). Decisions should also consider obligations, voluntary commitments, and stakeholder views. It doesn’t mean that every conceivable safety measure must be taken, or that every risk must be reduced immediately. There are practical limits to what is technically possible, what is available, what is cost effective and how fast it can be done.

The SFAIRP test is intended as a practical indicator of whether risks have been reduced sufficiently; that the duty of care to others has been considered, and practical steps taken to acknowledge that duty of care. As resources are normally limited it is good practice to have a process in place to work out the best options and level of controls (see Provision 21 Investment Decisions), as it relates to the individual EM Risk and overall EM Risks together.

Different kinds of control can be layered on top of one another to act as a protective barrier, contributing to the overall resilience of the system (as articulated in figure 4). For instance, in the rail industry, layered controls could encompass preventive maintenance, safety protocols, cybersecurity measures, emergency response plans, and infrastructure redundancy.

RSSBs ‘Taking Safe Decisions’ framework provides guidance on aspects of good practice on how to take decisions that are properly grounded in risk-based evidence, and that protect the safety of rail industry staff, rail users and others, satisfy the law, and respect the interests of stakeholders, whilst remaining commercially sound. The ‘Taking Safe Decisions’ framework is compatible with other mandatory and voluntary management frameworks a Rail Entity might already be using, such as:

- ROGS Safety Management Systems.

- Risk Management Maturity Model (RM3).
- BS EN ISO Standards (i.e. ISO 45001 - Occupational health and safety; ISO 31000: Risk management); ISO 22301: Business continuity management systems; ISO 55001: Asset Management).
- Corporate Governance and Enterprise Risk Management frameworks.

Figure 4 shows how the decision-making process takes account of legal requirements, SFAIRP judgements, commercial responsibilities, and Government policy making.

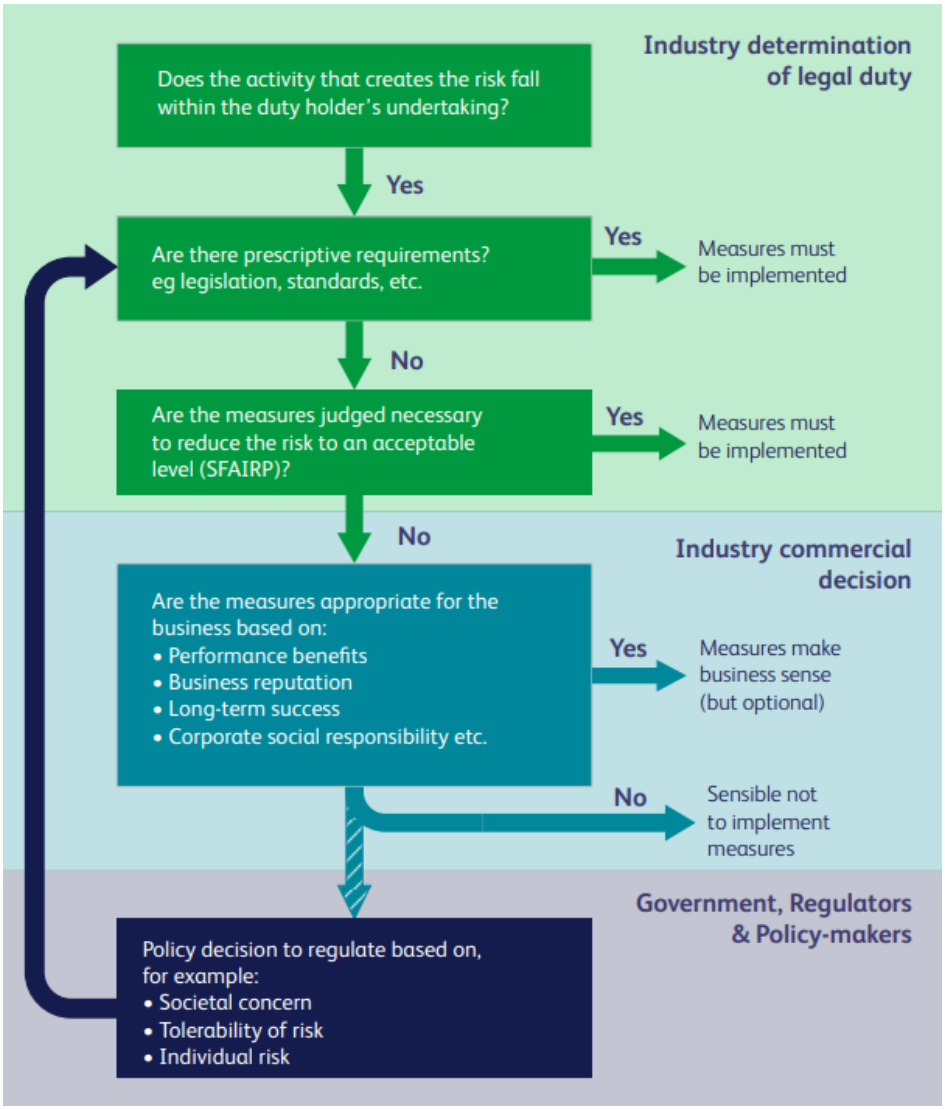


Figure 4: Safety decision-making responsibilities (Extract from RSSBs 'Taking Safe Decisions')

Options for treating risk may involve one or more of the following:

ISO 31000 Risk Management Treatment Options		EM Risk Considerations
Avoiding the risk	Prevention	This involves not starting/ continuing the activity that gives rise to the risk. Rail Entities are inherently exposed to EM Risk by the nature of the activities and physical nature of the operations they coordinate. It is therefore difficult to avoid EM Risk or to avoid all circumstances of exposure. However, a Rail Entity could decide to avoid EM Risk in some limited situations whilst still operating to deliver rail services. **An**

		example includes decommissioning an asset from service where its level of safety, security and reliability cannot be relied upon.
Removing the risk source		Rail Entities are rarely able to remove the source of EM Risks (underlying threats / hazards), however **an example would be undertaking earth works to remove a land slip hazard from a cutting.**
Controls: Changing the likelihood		Often the most viable approach to managing EM Risk involves controls including policies, procedures, practices, processes, technology, techniques, methods, or devices that modifies or manages risk. The primary objective of layered controls is to prevent emergencies before they occur. **By employing proactive measures, such as regular maintenance, safety training, and robust cybersecurity practices, the aim is to reduce the likelihood of risks materialising into full-blown emergencies. Security checks at stations will reduce the likelihood of a security risk manifesting.**
Controls: Changing the impacts	Consequences reduced	While preventing emergencies is ideal, not all risks can be completely eliminated or made less likely. **Minimising the impact of the emergency in the railway context, means having well-defined emergency response plans in place, advanced communication systems for rapid decision-making, and contingency measures to reduce disruptions and enhance the recovery process after an emergency. E.g. a Rail Entity's BC Plan, on call arrangements and Emergency Plan all reduce the impact.**
Sharing the risk		Sharing the risk typically only allows for the transfer of financial risk. E.g. through contracts, buying insurance. **Whilst this may support the Rail Entity's ability to finance post-event response and recovery it is almost impossible to share operational, safety, security, environmental legal and reputational consequences of an EM Risk event.**
Retaining the risk	Likelihood / impact retained	It is rarely possible to eradicate all EM Risk therefore, after all reasonably practicable options have been exhausted a Rail Entity will likely need to retain a certain amount of residual risk by informed decision. **Rail Entities should determine whether they retaining risk is within their risk appetite, if not they need additional controls.**

The effectiveness of risk treatment options tends to decrease as you move along the spectrum from preventative controls to responsive controls. Figure 5 visualises how it is generally better to prevent a risk from occurring – automated (where possible) preventative controls are typically more effective than responsive controls that can only reduce the impact once the risk event has materialised. However, both types of control are required in a good control framework.

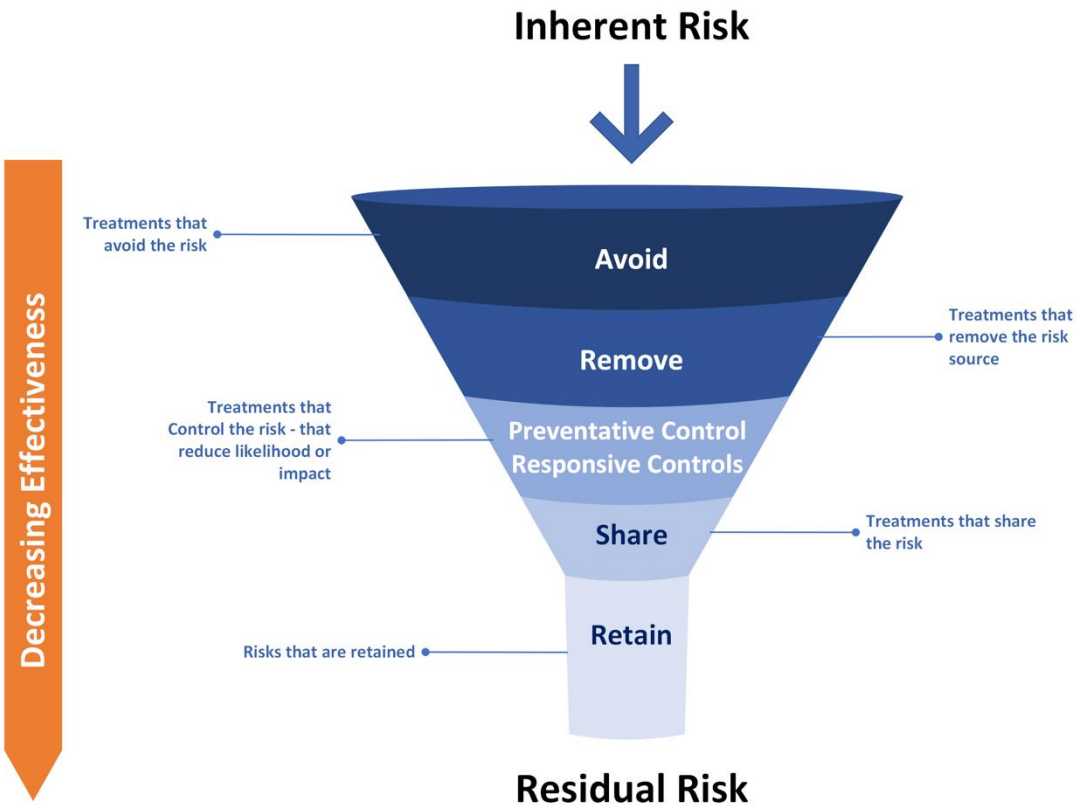


Figure 5: Funnel diagram visualising how each kind of treatment can overlay to contribute to a greater aggregated reduction of risk exposure

Directive controls set minimum standards to be followed e.g. policies, asset strategies, ROGS, rail industry and standards.

Preventative controls, which proactively stop or minimise risks before they occur, are generally more robust and sustainable. They often seek to address the root cause and/or reduce the likelihood of the risk event.

Detective controls, such as signal failure detection systems or weather warning notifications, can provide pre-emptive or real-time notification of risk events enabling responders to assess the situation and deploy responsive controls that may be required.

Responsive controls, such as emergency response plans, on the other hand, come into play after a risk event has occurred. While they can mitigate the impact, they are inherently less effective in comparison because the risk has already materialised. These controls focus on managing the consequences rather than preventing the event.

ISO 55000 family of international standards provide a wealth of reliable advice on undertaking effective asset management that can be used to inform the design of EM Risk controls. Rail Entities may also find it beneficial to identify effective risk controls used in other organisations and industry sectors.

Automated risk controls are preferable to manual controls due to their efficiency, consistency, and reliability. Automated controls operate without human intervention, reducing the risk of errors and

ensuring a swift response. They provide real-time monitoring, quick detection, and immediate action, enhancing the Rail Entities ability to manage risks effectively. Manual controls, dependent on human intervention, are more prone to inconsistencies, delays, and potential errors, making them less reliable in dynamic risk scenarios.

Investing in preventative controls and automating them where possible, aligns with the principle of addressing risks at their source, offering a more resilient and sustainable risk management strategy.

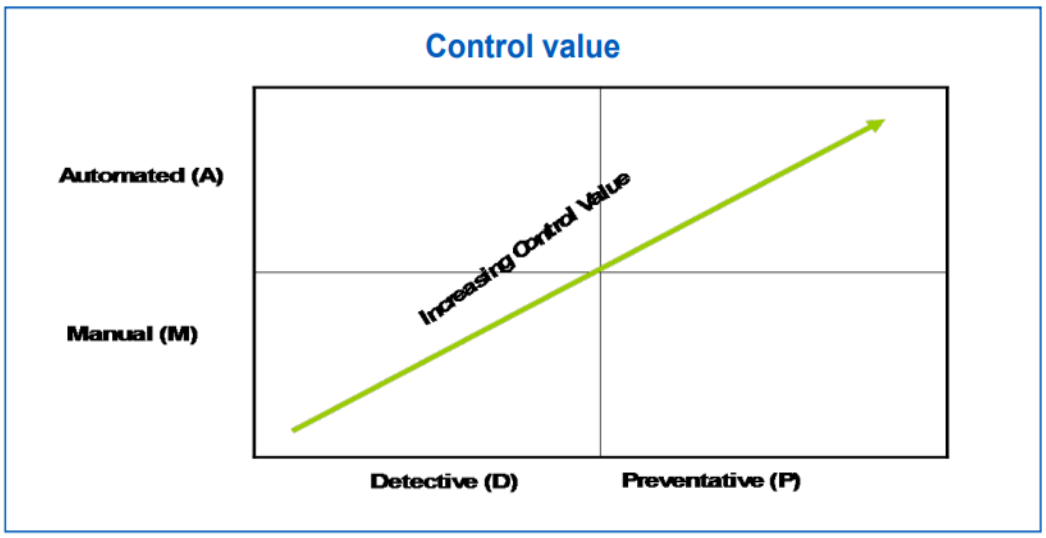


Figure 6: Visualising control value

Provision 18 (Residual Risk)

Rail Entities **SHOULD** ensure that residual risk that is outside of documented risk appetite is only retained by informed decision of Top Management, communicated to internal and external stakeholders, and subject to regular monitoring and review.

As shown in Figure 4, the Rail Entity will always take on some residual risk as it is not possible to remove or eliminate risk entirely whilst still meeting organisational objectives of Rail Entities collectively (e.g. running the GB mainline rail network and services thereon).

Risk owners should ensure that all residual risk that cannot be reasonably practicably managed and is outside the Rail Entities' documented risk appetite is escalated to Top Management and only retained by informed decision in accordance with the organisation's governance arrangements. The remaining risk should be documented and subjected to monitoring, and review. Internal and external stakeholders should be aware of the nature and extent of any residual risk.

6.2 Control Design

Provision 19 (Control Operation)

Rail Entities **should** clearly document how controls that manage EM Risks are operated.

Control descriptions explain the purpose of the control clearly enough for anyone to understand. When developing controls consider how they relate to the risk, and how the performance of the control will be assessed and measured to support control assessments. Control descriptions as minimum **should** answer the following six questions:

Why?	Why is this control in place? Include the specific element of the risk the control is mitigating.
What?	What needs to be done? Use control verbs to explain, like authorise, approve, monitor, and validate.
When?	How often is the control performed?
Who?	Who performs the control? Mention job title and business.
Where?	Where is the control performed? This could be a location, or an IT system, a third party or another part of the organisation.
How?	How is the control operated? Cover control steps, procedures, inputs, outputs, and what evidence is captured.

6.3 Resilience by Design (Change, Asset, and Investment Management)

Key Terms	
	'Resilience by design' is an approach that emphasises the proactive incorporation of strategies, principles, and features during the planning and development phase of systems, processes, and infrastructure to enhance an organisation's ability to withstand and recover from disruptions.

Provision 20 (Resilience by Design /Through Change)

Rail Entities **SHOULD** build and/or design operational resilience into their operating model, so that it is considered at the inception of any change, and the impact changes to the organisation may have upon the control of EM should be managed.

Resilience by design should play a crucial role in the Rail Entities approach to change and is recommended by the ORR: "*We urge the industry to consider during the design stage of infrastructure enhancements and renewals, system resilience and ease of system recovery from an incident. This should include consideration of the human factors that influence the ability of staff to take control of emergency situations, and where it is reasonably practicable, the design should facilitate emergency responses*."[27]

The Rail Entity should have a clear approach to managing EM, including periods of organisational change. It is good practice for the Rail Entity to proactively control risk, through continual improvement of its internal arrangements, including through periods of change. When implementing organisational changes, the following resilience implications should be carefully assessed:

- Implications to the assessment of risks: Understand how the proposed changes might impact the effectiveness of existing EM controls. Changes can sometimes weaken or even invalidate these controls. There may be changes to the interfaces with organisations and the way risks between different organisations. Risk assessments should be conducted to any newly introduced vulnerabilities and ensure that the Rail Entities resilience is not

[27] ORR (2017) Regulatory Guidance - Strategy for regulation of health and safety risks, Chapter 5 - interface system safety, V3.

compromised. Changes should be assessed and shared with relevant stakeholders (See Provision 28 Sharing and Cooperating), as they may also need to change their risk management strategies for the activity or asset affected by the change.

- Competency requirements for the technical aspects of change, as these may not exist within the end user or the Regulator.
- Implications for resilience integration: If the proposed changes offer an opportunity to enhance resilience, they should be designed and implemented to do so. **(**See Provision 22 Resilience Characteristics).
- Implications for testing and assurance: Changes should undergo thorough testing before acceptance into BAU operation, to ensure they do not have a detrimental effect on the Rail Entities ability to prevent and manage emergencies. Change assurance processes should confirm that the changes align with resilience requirements.
- Implications for transition to BAU: Any resilience characteristics or features of the change including maintenance requirements should be documented and communicated to the relevant asset/activity owner/s when a change is transitioned from a project/programme environment to the BAU management.

Following an incident Rail Entities may need to engage in restoration and recovery activities. Which in turn may present an opportunity to opportunity to enhance the resilience of the asset/activity.

Provision 21 (Investment Decisions)

Rail Entities **SHOULD** consider [EM] risk when managing resources, making investment decisions and business planning activities.

The Rail Entity should have a clear approach for incorporating consideration of [EM] risk when making key investment decisions and planning business activities. Investment decision-making should take systems level approach and the allocation of resources should be guided by resilience requirements:

- Investments should give due priority to projects and initiatives that enhance resilience. This may involve allocating funding to critical infrastructure upgrades, technology enhancements, or safety measures that mitigate risk.
- Cost-Benefit Analysis: Resilience-enhancing investments may involve higher upfront costs, but they should consider long-term benefits of high reliability, less direct and indirect costs arising out of disruptions and lessen the need for remedial works.
- Lifecycle Management: Resilience by design should be a fundamental aspect of asset lifecycle management. Assess the resilience of assets and plan for their maintenance and upgrades, allocating funds accordingly.
- Investment decisions should support a culture of continuous improvement. Allocate resources to ongoing initiatives that improve resilience, including training, testing.
- Contract and funding period: The timings of contracts and the investment timeline may not align.

Provision 22 (Resilience Characteristics)

Rail Entities **COULD** determine the resilience of assets/activities by considering robustness, adaptability, redundancy, and recovery.

A fundamental step in asset management is knowing what is available, where it is and what its current status is, which means having a good basis of data on assets from which to work from. Infrastructure resilience is the ability of assets and networks to anticipate, absorb, adapt to, and recover from disruption. Resilience is secured through a combination of the principal components shown in the table below.

Characteristics of Resilient Infrastructure	Examples of Rail EM Risk controls aligned with resilience characteristics
Robustness and Fault Tolerance: The ability of the infrastructure to maintain operational functionality and structural integrity under stress. It includes design-based engineering controls that ensure sufficient functional capacity and the capability to withstand shocks and extreme events with acceptable levels of damage, allowing for graceful degradation when necessary.	Rail Bridge Design: Its ability to maintain structural integrity and operational functionality under stress, especially extreme events e.g. floods or fires. Design-Based Components & Functional Capacity: Bridge is constructed with sufficient load-bearing capacity to accommodate heavy trains and stress during normal operations and potential additional loads during emergencies. Bridge design considers potential shocks, such as those caused by sudden braking or acceleration of trains. It's also engineered (materials chosen and structural design) to withstand extreme events, e.g. floods. In extreme stress the bridge should allow for graceful degradation. e.g. in a stress event such as flooding, if water levels rise to a critical point, the bridge may close to train traffic, avoiding catastrophic failure, remaining structurally intact and preventing further damage.
Adaptability, Awareness, and Resourcefulness: This refers to the infrastructures capacity to adapt and anticipate risks, thereby limiting threats & hazards. It includes automated real-time monitoring, decision-making capabilities, and situational awareness tooling. It demonstrates agility and flexibility to make real-time decisions for corrective actions, effectively averting impending risks.	Train Operations Management: The rail system adapts to unforeseen challenges, anticipates risks, and makes real-time decisions to limit hazards: Adaptability: Rail Entities use a real-time tracking system that monitors the location and status of trains. When an unexpected event like severe weather or a technical issue disrupts the schedule, the system can automatically re-route trains or adjust schedules to minimise delays and potential hazards. Awareness: Sensors and monitoring equipment are installed along the tracks to provide continuous data on conditions like temperature, track wear, and weather. This real-time data is fed into a central control system, enabling operators to be aware of potential risks or anomalies. For instance, if a track's temperature exceeds safety limits, the system can notify operators to act. Resourcefulness: In the event of an emergency the Rail Entity can rapidly deploy additional maintenance crews, emergency response units, or alternative transportation modes. This readiness ensures a quick and efficient response to minimise disruption and maintain safety standards.
Functional Flexibility and Redundancy: The ability to rapidly reorganise, shift resources, and provide substitutions to maintain an acceptable level of service/ functionality during disruptive events. It incorporates redundant system components / spare safeguards, ensuring operational flexibility and distributed functionalities. This allows system operators and users to substitute assets and modes, minimising single-point failures.	Rail Power Supply Systems Functional Flexibility: The railway's power supply system is designed with the capability to rapidly reorganise and adapt ensuring that no single-point failure can bring the entire system to a halt. In case of a disruption, such as a power outage or equipment failure, the system can switch to alternative power sources or redistribute power to critical components. Redundant System Components: Redundancy is built into the power supply system. This may include duplicate power sources, UPS, backup generators, and spare transformers. If one power source or component fails, the redundant systems can seamlessly take over to maintain uninterrupted operations.
Response and Recovery:	Station Emergency Response Plans

In situations where preventive measures prove inadequate, response and recovery plans are deployed to manage shock events as they unfold. This encompasses identifying options, prioritising actions to control damage and initiate mitigation, and efficient communication of decisions to the personnel responsible for implementation. Rapid recovery is a key objective, swiftly restoring normal operations after an emergency.	Pre-emptive Planning: Station managers regularly reviews and updates its emergency response plans and the potential for incidents. Response Arrangements: In anticipation of such incidents, the station has response arrangements in place. This includes an established emergency response team, equipped with necessary tools and resources to address various scenarios. Preparedness Measures: Station staff are trained and exercised in response procedures; they know how to identify the signs of an emergency and how to trigger response plans. Communication Protocols: Effective communication protocols are established to ensure that station personnel can efficiently coordinate their response efforts. This includes having clear channels to contact external emergency services if necessary. Recovery Actions: In the aftermath of an incident, the station team swiftly initiates recovery actions to repair damage and restore normal operations as soon as possible. By focusing on pre-emptive plans and arrangements, the station is better prepared to respond to incidents efficiently, ensuring the safety of rail users and staff and a swift return to normal operations after an emergency.

In addition to the core resilience characteristics outlined in the above table the broader concept of infrastructure resilience incorporates a strategic framework that ensures resilience is embedded in governance, operations, and emergency management planning. The following key principles reinforce and extend the resilience characteristics previously discussed:

- **Governance & Coordination** – Clear roles and responsibilities prevent overlaps and inefficiencies in managing resilience, ensuring accountability and transparency.
- **Information Flows & Learning** – Effective communication across agencies, infrastructure systems, and stakeholders supports adaptive risk management, enabling lessons learned from past emergencies to be embedded in future resilience strategies.
- **Flexibility & Resourcefulness** – The ability to evolve in response to changing risks, mobilising financial, technological, and human resources efficiently.
- **Reliability & Redundancy** – Designing systems to function under a range of conditions, with backup options available to maintain service continuity.
- **Safe Failure & Robustness** – Infrastructure should degrade gracefully in failure scenarios, minimising disruption and protecting overall network integrity.

These elements align with the resilient infrastructure principles outlined in Designing for Infrastructure Resilience, (2016) and reinforce the principles set out in this Code of Practice. They serve as a critical bridge between anticipation, assessment, and prevention of emergency management risk and the response and recovery phase, ensuring that resilience is considered proactively rather than reactively.

7 Monitoring & Reviewing

Monitoring refers to continual checking of EM Risks and attendant control effectiveness - as they are currently understood and managed. This is often done using risk indicators and real time data (See Provision 9 Process for Anticipating Risks). Reviewing refers to a periodic, but more in-depth assessment not only of the status of the risk, but its controls, indicators and environment the risk is operating in. Review helps identify if the risk has changed, if controls remain appropriate, or if the Rail Entities appetite has changed, which is vital because risk is not static.

7.1 Reviewing Arrangements

Provision 23 (Review)

Rail Entities **MUST** regularly review and maintain the currency of their risk assessments, controls, asset/activity vulnerability & criticality assessments, and retained risk. (MHSWR 1999)

Legally, businesses are required to review risk assessments (and associated controls and registers) regularly. Under the HSE's guidance, most businesses review them once a year, but it is up to the individual business to define, considering how regularly the organisation's business operations change, and the risk factor of business activities. Risk assessments for higher risk activities might need to be reviewed more regularly, and control measures will need to be continuously monitored to ensure people are always kept as safe as possible. **For example, depot activities or stations under construction or modification will require more regular risk assessment reviews than low-risk workplaces such as Rail Entity head quarter offices.**

Reviews help to answer the following questions:

- Have we identified the risks?
- For risks we have identified, have we evaluated them effectively?
- Do we have the right controls in place and are they operating effectively?

For most Rail Entities reviewing risks and control measures once a year is sufficient to achieve compliance with legislation, create a safe and secure workplace and to reduce the risks involved in business operations. Risk assessments will need to be reviewed and updated ahead of schedule in the following circumstances:

- Any major changes to the work environment, equipment, procedures or organisation structure. See Provision 3 (Context).
- When new threat/hazard information is identified. See Provision 9 (Process for Anticipating Risks).
- As a result of assurance/audit findings. See Provision 7 (Lines of Defence).
- A risk indicator exceeds its key risk indicator threshold. See Provision 26 (KRIs).
- Control testing indicates a control is not fully effective. See Provision 24 (Control Testing).
- After an incident, exercise or near miss highlights a new risk or a new understanding of what an existing risk entails (the incident might be internal or external).
- A change of legislation, statutory guidance or regulation. See RDG Guidance Note: Emergency Management Legal & Regulatory Register [RDG-GN-OPS=064].

7.2 EM Control Effectiveness

Provision 24 (Control Testing)

Rail Entities **SHOULD** demonstrate control effectiveness through regular testing of control design and control operation.

It is important to make sure that risk controls are designed and operating as intended.
Control Design Effectiveness is about determining how effective the control is and whether it achieves its objective to mitigate the risk effectively. Control design should be tested first (there is little point in assessing the operation of a badly designed control). The control tester should read the

description of all control activities and use their judgement to decide the extent to which the described control would mitigate the risks it is linked to (it may be in place to control multiple risks).

Testing involves the following considerations:

- Wherever possible preventive controls are preferable to detective and responsive controls as they prevent the risk from materialising. In practice an EM Risk is likely to have treated via a mix of controls and it is important to consider whether there is a sufficient mix of controls with a bias towards prevention wherever possible.
- The control should be applied at the optimum point, step or process (typically as early as possible) to prevent, eliminate or reduce the risk.
- Controls need to be performed often enough to mitigate the risk effectively.
- Could it be automated: This may be more efficient and reliable than multiple manual controls.
- Performed by the right person: Does the person responsible for performing the control have the right competence, knowledge, skills and authority?
- Suitable and scalable: Able to deal with an increase in activity as the business grows?
- Controls should be traceable to legal and regulatory obligations where appropriate.

Whenever possible, Rail Entities should consider control design at the time systems and processes are being developed, rather than having to retrofit controls later (See Provision 20 Resilience by Design/ Through Change).

Periodically reviewing incidents (e.g. a risk has occurred despite controls) to identify common root causes – in case these are occurring more frequently or haven't previously been identified - and whether controls really are operating as intended. If control weaknesses are identified, then a higher level of risk than expected is being taken. This activity can be seen as testing control effectiveness.

Control Operation Effectiveness is about whether the individual control has been performed effectively, consistently in line with control design, by the right people and on time.

The Control Owner should decide how often the operating effectiveness is assessed and what information and evidence they will require to support their assessment of operating effectiveness and how they will get it. It depends whether the control is automated, semi-automated or manual, the volume of activity assessed and the frequency of the activity.

Testing approaches may include:
Proactive monitoring: Proactive evidence to support the control assessment, for example:

- Proactive monitoring of the controls by exception reports from automated controls, evidence of occurrence and performance over a period for instance.
- Results and trends of KRI metrics that provide evidence of how well controls are performing (See Provision 26 KRIs).
- Results of emergency management tests and exercises.

Reactive monitoring and testing: Reactive testing is a reperformance or manual verification to check if a control has operated as intended. Reactive testing can only take place when proactive evidence does not exist.

Independent testing and other evidence: There may be other evidence available to support the control assessment. For example:

- Second-line risk oversight and audit or regulatory findings (See Provision 7 Lines of Defence).
- Risk events or regulatory breaches.

Each control activity needs to be assessed for operating effectiveness. Evidence should be reviewed where appropriate to support any verbal confirmations. When all control activities have been tested, the overall operating effectiveness for the control should be assessed based on the results.

Provision 25 (Automated Monitoring)

Rail Entities COULD consider implementing automation of monitoring and data gathering to support reporting and decision making.

Rail Entities could consider implementing automation solutions to increase the efficiency of EM Risks, assessments, tracking ownership of remediation activity or producing EM management information (MI) reporting. Automation is often a costly solution. The adopted solution should be proportional to the size and resourcing available for the organisation.

7.3 Monitoring using Key Risk Indicators (KRIs)

Key Terms

A ***key risk indicator (KRI)*** is a metric for measuring the likelihood that the combined probability of an event and its consequences will exceed the organisation's risk appetite and have a profoundly negative impact on an organisation's ability to be successful.

KRIs play an important role in enterprise risk management programs. This is because they:

- Provide advance notice of potential risks that could damage the organisation;
- Give insight into possible weaknesses in an organisation's monitoring and control tools; and
- Can be incorporated into ongoing risk monitoring between risk assessments.

KRIs are often confused with key performance indicators (KPIs), which are metrics that help an organisation assess progress toward declared goals. The two terms are functionally the inverse of each other. While they may be separate and distinct for some issues, the creation of one often results in the creation of the other as its complement.

Provision 26 (KRIs)

Rail Entities **SHOULD** define, establish, and regularly review quality KRIs for EM Risks.

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 indicators should be structured to allow for progressively deeper granularity to identify the root cause of poor performance to be understood and to align with individual, team and department-level performance assessment. KRIs and MI should contribute to ongoing and periodic assurance activities. Indicators can be developed to alert management to probable changes in a risk which:

- Confirms controls are having their intended effect;
- Could prevent it from exceeding previously agreed tolerance levels;
- Or prevent it from being managed to unnecessary levels beyond the optimal position.

The risk owner should work with the risk management team to develop appropriate quality KRIs for EM Risks. Doing so will enable the organisation to determine if the risk exceeds the organisation's risk appetite. KRIs can be used as a tool for the ongoing monitoring of risk within the organisation and may be incorporated into risk monitoring dashboards for use by top management. Good quality KRIs are:

- **Measurable and monitorable** (it is clear what will be measured/counted and how measurements will be tracked over time).
- **Defined and clearly written.**
- **Comparable** (can easily be compared with KRIs from other organisations).
- **Flexible within tolerance limits** (include an understanding of acceptable deviation).
- **Revealing** (highlight the area of focus rather than a description of the indicator itself).

- Accurate (should present a useful representation of the risk).
- Visual (KPIs are often presented in visual ways to make them appealing and insightful).

It is important to monitor and report about events that have occurred and their impacts, and making assessments of the risks that contribute to emergencies are elements of an overall approach to risk reduction and management.[28] Control owners should ensure that measures (tooling, alerting or manual processes) are in place to detect where processes or controls deviate from expected normal operation or where outputs are unexpected/abnormal.

Rail Entities should establish a regular monitor and review of any KRIs they are using for EM Risks (See 'Triggering a Review' for more detail on when this should take place). They should identify any changes to the situation/risks/threat levels identify and implement any remedial action that may be needed to the KRI metrics to ensure they remain fit for purpose.

The RRP suite of documents will also include one on KPIs and KRIs, which is forthcoming in 2025.

Provision 27 (Managing Corrective Actions)

Rail Entities **SHOULD** ensure that the findings of any reviews of risks are collated, recorded and any corrective actions are managed by the Rail Entity's standard process.

As with all reviews, assurance and audit 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 (see Provision 7 Lines of Defence and Provision 29 Common and Shared Risks).

[28] UNDRR (2020).

8 EM Risk Communication, Collaboration & Consultation

This section considers the requirements for communication and consultation about EM Risks and their management. This involves ongoing and iterative information exchange and discussing the management of EM Risks with relevant stakeholders.

Although this is the last section of the Code of Practice, it is important to note that stakeholder communication takes place throughout the risk management process not just the end.

8.1 Stakeholder engagement

The IEM CoP for Governance[29] already makes provisions for coordinated internal, industry and multi-agency activity therefore these are not repeated here where they establish requirements for general EM governance activity. This section provides further detail on how risk specifically may be managed within those groups.

Provision 28 (Sharing and cooperating)

Rail Entities **MUST** share information and cooperate with other LRF partners to enhance co-ordination and efficiency. (CCA, 2004)

Rail Entities **MUST** share information and cooperate with other relevant industry stakeholders to achieve the safe operation of the railway system and enhance co-ordination and efficiency. (ROGS, Reg 22).

No single entity is responsible for making the whole railway system safe. The various organisations, train operating companies, infrastructure managers, maintainers, contractors, suppliers, and the regulator each have important roles in ensuring that the overall combined system is safe.

Rail Entities should start all communication, collaboration & consultation from a position of considering the risks and harm if they do not share information. The duty of co-operation in ROGS (Regulation 22) requires companies to work together to manage risk by placing an obligation on transport operators to cooperate, so far as is necessary and reasonable, with other transport operators to achieve safe operation of the railway system.

The UK Government Resilience Framework (2022) established a fundamental principle that developing a shared understanding of the risks we (as individuals, organisationally and societally) face should underpin everything that we do to prepare for and recover from crises. With this in mind, Figure 7 depicts three broad categories of EM Risk management stakeholders for Rail Entities to consider within their collaboration and communication activities (non-exhaustive). It is good practice to map internal and external stakeholders regularly. Collaboration and information sharing is required at each level (internal, industry and multi-agency). A shared understanding of risks means:

- Risks can be aggregated and understood at a higher level.
- Interactions and boundaries between organisations (and shared controls) can be understood.
- Risks that are managed by controls outside the organisation can be better understood.
- Vulnerabilities and criticalities are understood in the context of a wider system.

Interdependencies and interconnectedness cannot be fully understood without incorporating their cross-jurisdictional dimension. Threats and hazards do not stop at jurisdictional or organisational borders. Some critical infrastructure systems cross borders, providing services in multiple regions, which makes it more compelling to integrate cross-organisational cooperation in critical infrastructure

[29] RDG Approved Code of Practice: Rail Emergency Management Code of Practice with Guidance Part A – Governance (RDG-OPS-ACOP-008)

resilience policies. Sharing good practices, adopting common approaches and developing joint standards in critical infrastructure resilience can foster cooperation in this area.

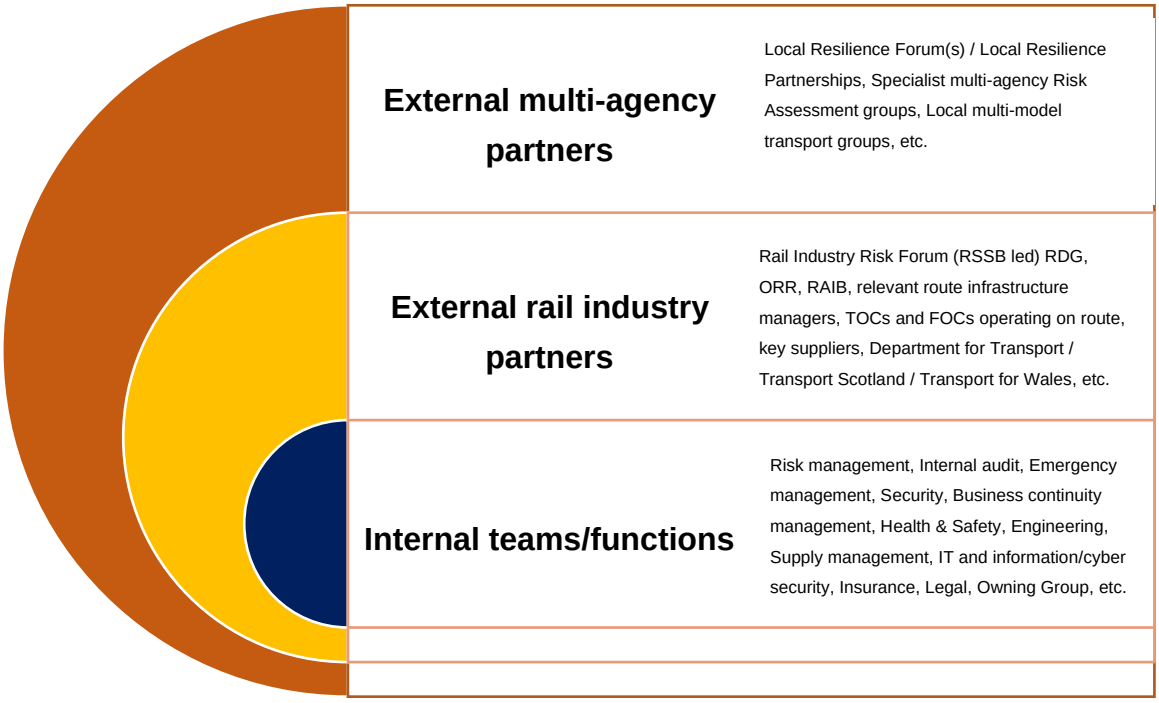


Figure 7: Diagram showing key resilience partners

IEM CoP for Governance (Requirement 6.1.1 and 6.1.2) already makes provisions for multi-agency collaboration and cooperation through LRFs and LRP to support duties listed under Section 2.1 of the 2004 Civil Contingencies Act. The CCA duties include the assessment risk of an emergency occurring and prevention and mitigation activities. **The general guidance supporting that requirement is not repeated here except those elements which relate to risk management**.

- Collaborate with CCA Category 1 and 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 outputs of horizon scanning, IEM Risk assessments, data gathering or real-time monitoring.
- 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 CCA 2004, including for planning, prevention, preparedness or exercising.
- Collaborate with the LRFs/LRPs in conducting local risk assessments, providing expertise and sector insight to allow the right resourcing, planning or mitigation measures are incorporated.
- Facilitate sharing lessons identified with relevant stakeholders in the LRF (e.g using the Joint Operational Learning – JOL – process and sharing documents on Resilience Direct) and enable collective learning and improvement across the industry and relevant communities when included in part of the review cycle.

Provision 29 (Common and Shared Risks)

Rail Entities **SHOULD** regularly collaborate with stakeholders to identify and manage shared risks and risk controls.

Rail Entity collaboration and consultation activity **should** include:

- Consulting with stakeholders to agree objectives, standards, processes, and arrangements for the management of shared and common risks.
- For shared and common risks:
    - Using industry knowledge effectively across direct and indirect interfaces to enable clear understanding and control of shared and common risks.
    - Sharing information and best practice between organisations with common/shared risks, to continually improve collaborative relationships and shared risk reduction.
    - Developing and using procedures/standards, jointly, effectively, and consistently to control common/shared and emerging risks.
    - Where risk controls cross organisational boundaries, all relevant organisations should possess the right information in the form of procedures and standards, factual data and intelligence, and instructions and reports relating to that risk.
    - Also taking into consideration shared interdependency (see Provision 8) and shared criticality (see Provision 9).
- Looking to other sectors and countries to identify EM Risks and using this insight to improve arrangements.
- Leaders searching within and outside the organisation for opportunities to improve risk control in their area of the organisation, to ensure it is as effective and efficient as possible.
- Regular reporting on risk information and joint learning about risks and their controls – in particular understanding the aggregate risk held by that particular risk community (as defined by owning group, geographic boundary, at industry level, at individual organisation level etc) and any retained risk outside of risk appetite.

The industry strategy 'Leading Health and Safety on Britain's railway' (RSSB, 2020) has been developed by leaders of the rail industry and is an example of an industry-wide agreed approach to voluntary collaboration. It focuses on those elements of health and safety risk management that can be improved by Rail Entities working together, both within and beyond legislative interface requirements.

Appendices

Appendix A: Table of Provisions

Section	Provision number and descriptor	Provision Wording	Functions involved
Chapter 3: Risk Environment	1 (Risk assessments inform EM and BCM)	Rail Entities MUST have in place arrangements for assessing the risk of emergencies occurring, (MHSWR 1999, HSWA 1974) and SHOULD use this to inform emergency and business continuity management.	Risk Management function Emergency Management (EM) / Business Continuity Management (BCM) functions Safety function
	2 (Business integration)	[EM] Risk management processes SHOULD be an integral part of management and decision-making and integrated into the management system governance, structure, operations, and processes of the Rail Entity.	Document Control function Top Management/ All Managers Governance/assurance function Risk Management function
	3 (Context)	[EM] Risk management SHOULD relate to the Rail Entity's purpose, governance, leadership and commitment, strategy, objectives, and operations. [ISO 31000]	Top Management Governance function Risk Management function
	4 (Risk Appetite)	Rail Entities SHOULD clearly articulate their risk appetite, so that this informs decisions about how EM Risks are managed and resource allocation.	Top Management Governance function Risk Management function
	5 (Leadership)	Rail Entity leaders SHOULD demonstrate leadership and commitment to the management of EM Risks. (ISO 45001, Clause 5.1 Leadership and Commitment)	Top Management
	6 (Framework)	The Rail Entity SHOULD have in place an overarching risk management framework with clearly articulate associated processes, roles, and responsibilities, for managing [EM] risks.	Risk Management function Supported by the EM & BCM functions
	7 (Lines of Defence)	Rail Entities SHOULD have in place a Three Lines of Defence model for the assurance and audit of EM Risks.	Risk Management / Governance function Audit function Supported by the EM & BCM functions
	8 (Asset/Activity Interdependency)	Rail Entities owners SHOULD understand systemic dependencies between their assets and activities. [OECD Policy toolkit on governance of critical infrastructure resilience]	Senior managers Asset/ Infrastructure owners Activity/Process owners Risk Management/ Governance function Performance board

	9 (Criticality Assessment)	Asset manager/activity owners SHOULD be accountable for assessing, documenting, and communicating the criticality of their assets/activities to stakeholders.	Risk Management/ Governance function - set the process Asset/Infrastructure owners - deliver Activity/Process owners - deliver
Chapter 4: EM Risk Identification (Anticipation)	10 (Process for Anticipating Risks)	Rail Entities should define, establish, and regularly review and improve a systematic process for data and intelligence gathering around EM Risks to allow them to be identified and understood - which then allows them to be assessed, evaluated, treated and monitored.	Risk Management/ Governance function Business assurance function Supported by the EM & BCM functions in delivery of this
	11 (Gathering Data)	Rail Entities SHOULD conduct a broad review of internal and external data sources to inform their identification and assessment of EM Risks. [ISO 31000]	Overall - Risk Management/ Governance function Specific risks according to risk owners EM & BCM functions for major EM Risks
	12 (Risk Identification & Terminology)	Rail Entities SHOULD use consistent terminology for identifying and defining risks and they COULD use a taxonomy as the basis for this. [OECD Policy toolkit on governance of critical infrastructure resilience and RSSB: Common Hazards for the Management of Industry Safety (CHAMOIS)]	RSSB to set tone nationally RAIB and RDG to feed in EM function Risk Management/ Governance function
Chapter 5: Risk Analysis and Evaluation (Assessment)	13 (Vulnerability Assessment)	Station emergency plans MUST address likely instances involving dangerous goods that pass through a station where this is relevant. [ORR's Strategy for regulation of health and safety risks, Ch 5 - interface system safety. V3 (Dec 2017)] Asset managers and/or activity owners SHOULD be accountable for ensuring the vulnerability their asset/activity is assessed, documented, and communicated to stakeholders.	Station managers Asset/Infrastructure owners Activity/Process owners EM function Safety and Security functions
	14 (Risk Analysis and Processes)	Rail Entities SHOULD analyse EM Risks using their own internal risk processes.	Risk Management function Governance function EM function
	15 (RWCS)	Rail Entities SHOULD regularly determine and assess the 'Reasonable worst-case scenario' for each EM Risk and document the criteria used to determine its plausibility.	Risk Management/ Governance function EM function
	16 (Diverse Perspectives)	Rail Entities SHOULD ensure that risk assessments are carried out by a diverse group of professionals and subject matter experts with a pragmatic mix of divergent of opinions, biases,	Risk Management/ Governance function EM function Subject matter experts

		perceptions of risk, and judgements. [ISO 31000]	
Chapter 6: Treatment (Prevention)	17 (Treatment)	Rail Entities MUST take all steps, so far as is reasonably practicable, to reduce safety related EM Risk. (Health & Safety at Work Act 1974) Rail Entities SHOULD formulate and select risk treatment options to reduce all EM Risk to within risk appetite. (ISO 31000)	Health and Safety function Risk Management/ Governance function
	18 (Residual Risk)	Rail Entities SHOULD ensure that residual risk that is outside of documented risk appetite is only retained by informed decision of Top Management, communicated to internal and external stakeholders, and subject to regular monitoring and review.	Risk Management/ Governance function Top Management Risk owners
	19 (Control Operation)	Rail Entities should clearly document how controls that manage EM Risks are operated.	Risk Management/ Governance function to determine process Risk Control owners to deliver
	20 (Resilience by Design/ Through change)	Rail Entities SHOULD build and/or design operational resilience into their operating model, so that it is considered at the inception of any change, and the impact changes to the organisation may have upon the control of EM should be managed.	Top Management Finance/business planning function Operations function EM/Resilience function
	21 (Investment Decisions)	Rail Entities SHOULD consider [EM] risk when managing resources, making investment decisions and business planning activities.	Top Management Finance/business planning function Procurement function
	22 (Resilience Characteristics)	Rail Entities COULD determine the resilience of assets/activities by considering robustness, adaptability, redundancy, and recovery.	Business Continuity function Asset/Infrastructure owners Activity/Process owners Performance function
Chapter 7: Monitoring and Reviewing	23 (Review)	Rail Entities MUST regularly review and maintain the currency of their risk assessments, controls, asset/activity vulnerability & criticality assessments, and retained risk. (MHSWR 1999)	Risk Management/ Governance function EM/BC function Performance Management function Audit/ Testing and exercising function
	24 (Control Testing)	Rail Entities SHOULD demonstrate control effectiveness through regular testing of control design and control operation.	Risk Management function Governance/Assurance function EM/BC function
	25 (Automated Monitoring)	Rail Entities COULD consider implementing automation of monitoring and data gathering to support reporting and decision making.	Control room function Business intelligence function

	26 (KRIs)	Rail Entities SHOULD define, establish, and regularly review quality KRIs for EM Risks.	Risk Management/ Governance function Business intelligence function
	27 (Managing Corrective Actions)	Rail Entities SHOULD ensure that the findings of any reviews of risks are collated, recorded and any corrective actions are managed by the Rail Entity's standard process.	Risk Management/ Governance function EM/BC function Risk owners Performance function
Chapter 8: Communication, Collaboration and Consultation	28 (Sharing and cooperating)	Rail Entities MUST share information and cooperate with other LRF partners to enhance co-ordination and efficiency. (CCA, 2004) Rail Entities MUST share information and cooperate with other relevant industry stakeholders to achieve the safe operation of the railway system and enhance co-ordination and efficiency. (ROGS, Reg 22).	EM/BC function Business c Risk owners / risk control owners
	29 (Common and Shared Risks)	Rail Entities SHOULD regularly collaborate with stakeholders to identify and manage shared risks and risk controls.	Risk Management function All risk owners / risk control owners

Appendix B: Definitions

Term	Definition in the context of this document
Business Continuity	Capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption (Business Continuity Institute)
Business Continuity Management (BCM)	Process of implementing and maintaining business continuity. (ISO 22313:2020). Holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response (CCS Civil Protection Lexicon, 2013)
Category 1 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)
Critical Control Point	Point, step or process at which controls can be applied and a threat or hazard can be prevented, eliminated or reduced to acceptable levels. (ISO 22300:2021)
Criticality Analysis	Process designed to systematically identify and evaluate an organisation's assets and activities based on the importance of its mission or function, and/or the significance of an emergency impacting the asset or activity effecting its ability to meet expectations and obligations. (adapted from ISO 22300:2021)
Control	Measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk. (ISO 31000). Note: Controls cannot always exert the intended or assumed modifying effect.
Emergency	An event or situation which threatens serious damage to human welfare, or to the environment; or war, or terrorism, which threatens serious damage to security. (UK Resilience Framework: December 2022)

	Note: For the purposes of this document the term Emergency has been used in relation to an emergency, business continuity event or similar event that triggers the activation of emergency, business continuity or similar arrangements.
Emergency Management (EM)	Overall approach for preventing emergencies and managing those that occur. (ISO 32200:2021) Note: In general, emergency management utilises a risk management approach to prevention, preparedness, response and recovery before, during and after emergencies.
Governance	Human-based system by which an organisation is directed, overseen and held accountable for achieving its defined purpose (ISO 37000:2021).
Governing Body	Person or group of people who have ultimate accountability for the whole organisation (ISO 37000:2021).
Hazard	Hazards are non-malicious risks such as extreme weather events, accidents, or the natural outbreak of disease. (UK Resilience Framework: December 2022)
Hazardous Event	A hazardous event is an event that has the potential to lead directly to death or injury. It is a central event lying between a threat/cause and a consequence, that corresponds to the moment when there is a loss of control of a hazard. (Taking Safe Decisions, Issue 3, and RSSB Rail Industry Bowtie Analysis: A Good Practice Guide, June 2021)
Human Factors	Human factors refer to the study of how people interact with their environment, technology, and systems. It focuses on understanding human capabilities, limitations, behaviours, and the psychological, cognitive, and social aspects of human interaction. The goal is to design systems, machines, and processes that improve performance, safety, and comfort by considering these human elements.
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. It entai six key activities – anticipation, assessment, prevention, preparation, response and recovery (Civil Protection Lexicon, 2013) 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 the voluntary sector, commerce and a wide range of communities. (Preparing Scotland – Scottish Guide on Resilience Chapter 3).
Major Incident	An event or situation with a range of serious consequences which requires special arrangements to be implemented by one or more emergency responder agency. (JESIP).
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)
Rail Users	Any person or persons that use the railway including, but not limited to, passengers, rail employees & contractors, and those accessing any services provided within stations. Note: This definition is broader than just rail passengers in order to include users of railway facilities such as retail and hospitality faculties in stations.
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 (ISO 22371:2022).

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 (ISO 31000:2018).
Risk Appetite	The amount of risk an individual, business, organisation or government is willing to tolerate. (UK Resilience Framework: December 2022)
Risk Treatment	Process to modify risk. Risk treatment can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the risk source; changing the likelihood; changing the consequences; sharing the risk with another party or parties (including contracts and risk financing); and retaining the risk by informed decision. (ISO Guide 73:2009) Note: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.
Risk Velocity	Refers to the rate at which a risk event develops from its onset to its peak impact. Understanding risk velocity can help to understand how quickly an organisation must respond to indicators the risk may be manifesting.
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).
So far as is reasonably practicable (SFAIRP)	Provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health (Health & Safety at Work Act 1974)
Stakeholder	Person or organisation that can affect, or be affected by, or perceive itself to be affected by a decision or activity (ISO 37000:2021).
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 (ISO 22371:2022).
Threat	Malicious risks such as acts of terrorism, hostile state activity and cyber-crime. (UK Resilience Framework: December 2022)
Top Management	Person or group of persons who leads and controls an organisation at the highest level. (ISO 22300:2021)
Vulnerability Assessment	Process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence. (ISO 22300:2021)

Readers are also directed to the list of definitions contained in:

- RDG Legal and Regulatory Register and accompanying Guidance Note (GN) (RDG-OPS-GN-064).
- RDG Governance Code of Practice – Approved Code of Practice: Rail Emergency Management Code of Practice with Guidance Part A – Governance (RDG-OPS-ACOP-008) [https://www.raildeliverygroup.com/about-us/publications/12981-rdg-ops-acop-008-rail-emergency-management-code-of-practice-with-guidance-part-a-guidance/file.html]
- UK Civil Protection Lexicon (2013) [LEXICON_v2_1_1-Feb-2013.xls (live.com)] includes a full glossary of definitions used in the context of UK Emergency Management and Resilience, however in many cases these have been updated using more modern references from UK resilience or from international standards.
- ISO Guide 73:2009(en) Risk management — Vocabulary
- ISO 22300:2021(en) Security and resilience — Vocabulary

Appendix C: Acronyms

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

Acronym	Full Form
ALARP	As Low as Reasonably Practicable
BAU	Business-as-Usual
BTP	British Transport Police
BCM	Business Continuity Management
BIA	Business Impact Analysis
BSI	British Standardisation Organisation
CCA	Civil Contingencies Act 2004
CIRAS	Confidential Incident Reporting & Analysis Service
COMAH	Control of Major Accident Hazards Regulations 2015
CoP	Code of Practice
CSM RA	Common Safety Method for Risk Evaluation and Assessment
DfT	Department for Transport
EM	Emergency Management
FOC	Freight Operating Company
GBRTT	Great British Railways Transition Team
GN	Guidance Note
IEM	Integrated Emergency Management
IRM	Institute of Risk Management
ISO	International Organisation for Standardisation
KRI	Key Risk Indicator
LRF	Local Resilience Forum
LRP	Local Resilience Partnerships
LoD	Lines of Defence (3LOD = Three Lines of Defence)
MI	Management Information
NARU	National Ambulance Resilience Unit
NFCC	National Fire Chiefs Council
OECD	Organisation for Economic Co-operation and Development
ORR	Office of the Rail Regulation
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations
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
SAIT	Safety Alerts IT Tool
SFAIRP	So far as is Reasonably Practicable
SMIS	Safety Management Intelligence System
SMS	Safety Management System
SPAD	Signal Passed at Danger toolkit
SRM	Safety Risk Model
TFW	Transport for Wales
TOC	Train Operating Company

Appendix D: References

For the purpose of developing this Code of Practice and associated guidance we have consulted a variety of national and international Standards, guidelines, and good practice documents, including:

Author	Year	Reference Name
Barami, B	2013	Infrastructure Resiliency: A Risk-Based Framework, US Department of Transportation, https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20Risk-Based%20Framework.pdf
BSI	2022	BS 65000 Organizational Resilience – Code of Practice https://knowledge.bsigroup.com/products/organizational-resilience-code-of-practice?version=tracked
Cabinet Office	2011	Keeping the Country Running: Natural hazards and infrastructure www.gov.uk/government/uploads/system/uploads/attachment_data/file/78901/natural-hazards-infrastructure.pdf
Cabinet Office	2012	Emergency Preparedness, Chapter 4: Local responder risk assessment duty (revised March 2012) https://www.gov.uk/government/publications/emergency-preparedness]
Cabinet Office	2015	National Business Resilience Planning Assumptions https://www.gov.uk/government/publications/business-resilience-planning-assumptions
Cabinet Office	2018	Public Summary of Sector Security and Resilience Plans https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
EU	2023	EU Critical Entities Resilience Directive (CER) https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en
Evidence on Demand	2016	Designing for infrastructure resilience, Gallego-Lopez, C.; Essex, J. (with input from DFID) https://assets.publishing.service.gov.uk/media/57d6bc5be5274a34fb00002e/Designing_for_Infrastructure_Resilience_July_2016_external.pdf
Government Finance Function	2021	Risk Appetite Guidance Note https://assets.publishing.service.gov.uk/media/61239758e90e0705481fc085/20210805_-_Risk_Appetite_Guidance_Note_v2.0.pdf
HM Government	2006	Railways and Other Guided Systems (Safety) Regulations 2006 https://www.legislation.gov.uk/uksi/2006/599/contents/made
HM Government	2022	UK Resilience Framework https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1131163/UKG_Resilience_Framework_FINAL_v2.pdf
HM Government	2023	UK National Risk Register https://www.gov.uk/government/publications/national-risk-register-2023
HM Government	2025	UK National Risk Register https://www.gov.uk/government/publications/national-risk-register-2025
HM Government	2023	The Orange Book Management of Risk – Principles and Concepts https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf
IRM		Practitioner Guides i.e., Standard Deviations, Cube to Rainbow https://www.theirm.org/news/from-the-cube-to-the-rainbow-double-helix-a-risk-practitioner-s-guide-to-the-coso-erm-frameworks/
IRM	2002	A Risk Management Standard https://www.theirm.org/media/4709/arms_2002_irm.pdf

IRM	2017	Risk Appetite Statements https://www.theirm.org/media/6878/0926-irm-risk-appetite-12-10-17-v2.pdf
ISO	2009	ISO Guide 73:2009(en) Risk management — Vocabulary, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en
ISO	2014	ISO 55001:2014(en) Asset management — Management systems — Requirements https://www.iso.org/obp/ui/#iso:std:iso:55001:ed-1:v1:en
ISO	2015	ISO 14001:2015(en) Environmental management systems – Requirements with guidance for use https://www.iso.org/obp/ui/#iso:std:iso:14001:ed-3:v1:en
ISO	2018	ISO 31000:2018(en) Risk management – Guidelines https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
ISO	2019	ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en
ISO	2020	ISO 22313:2020(en) Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301 https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-2:v1:en
ISO	2021	ISO 22300:2021 Security and resilience — Vocabulary https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:en
ISO	2021	ISO 37000:2021(en) Governance of organizations — Guidance https://www.iso.org/obp/ui/#iso:std:iso:37000:ed-1:v1:en
ISO	2022	ISO 22361:2017(en) Security and resilience — Organizational resilience — Principles and attributes [https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en]
JESIP	2024	Joint Doctrine: The Interoperability Framework, Version 3.1 https://www.jesip.org.uk/downloads/joint-doctrine-guide/
MI5		Threat Levels https://www.mi5.gov.uk/threat-levels
OECD	2014	Boosting Resilience through Innovative Risk Governance, OECD Reviews of Risk Management Policies https://dx.doi.org/10.1787/9789264209114-en
OECD	2019	Policy toolkit on governance of critical infrastructure resilience, in Good Governance for Critical Infrastructure Resilience https://www.oecd-ilibrary.org/sites/02f0e5a0-en/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book
ORR	2017	Regulatory Guidance - Strategy for regulation of health and safety risks https://www.orr.gov.uk/sites/default/files/2020-09/health-and-safety-regulatory-strategy.pdf
ORR	2020	Risk Management Maturity Model (RM3) https://www.orr.gov.uk/sites/default/files/2020-09/risk-management-maturity-model-rm3-2019.pdf
RAIB	2018	Roles of organisations in the UK's railways. https://www.gov.uk/government/publications/managing-the-uks-railways/roles-of-organisations-in-the-uks-railways#duty-holders
RDG	2021	Rail Resilience Project (RRP) Emergency Management Review: Findings and Recommendations Report https://www.raildeliverygroup.com/media-centre-docman/12968-rail-resilience-project-report-final-version/file.html
RDG	2023	Emergency Management Legal and Regulatory Register (RDG-OPS-GN-064) https://www.raildeliverygroup.com/media-centre-docman/acop/12969-rdg-ops-gn-064-emergency-management-legal-and-regulatory-register-final/file.html

RDG	2023	Approved Code of Practice: Rail Emergency Management Code of Practice with Guidance Part A – Governance (RDG-OPS-ACOP-008) https://www.raildeliverygroup.com/about-us/publications/12981-rdg-ops-acop-008-rail-emergency-management-code-of-practice-with-guidance-part-a-guidance/file.html
RSSB	2017	GEGN8646 - Guidance on the Common Safety Method for Risk Evaluation and Assessment https://www.rssb.co.uk/standards-catalogue/CatalogueItem/GEGN8646-Iss-1
RSSB	2019	Taking Safe Decision Framework https://www.rssb.co.uk/safety-and-health/guidance-and-good-practice/taking-safe-decisions
RSSB	2020	Leading Health and Safety on Britain's Railway Strategy https://www.rssb.co.uk/safety-and-health/leading-health-and-safety-on-britains-railway
RSSB	2023	T1194 - Common Hazards for the Management Of Industry Safety (CHAMOIS) https://www.rssb.co.uk/research-catalogue/CatalogueItem/T1194
UN	2020	UN Office for Disaster Risk Reduction. Hazard Definition and Classification Review: Technical Report, http://www.undrr.org/publication/hazard-definition-and-classification-review-technical-report

Note: For all legal and regulatory references please follow the link to the Legal and Regulatory Register
.

Appendix E: Taxonomy of Threats and Hazards

The following table provides a taxonomy of rail threats and hazards with the potential to disrupt or damage rail infrastructure and operations. Each Rail Entity can filter these threats and hazards (and those from alternative sources i.e., NRR) relative to their prioritised activities and critical assets. This taxonomy:

- Is based on the GB rail hazards classified within the RSSB Common Hazards for the Management of Industry Safety (CHAMOIS). The CHAMOIS project defined and structured both a threat and hazard taxonomy and a rail system ontology at three levels, each level including more detailed granularity.
- Each threat/hazard item represents potential challenges that may require specialised emergency response and recovery efforts to safeguard human welfare, environment and operational continuity.
- It is non-exhaustive and should be supplemented by additional threats and hazards identified through the review of internal and external data sources and information sources (see Provision 11).

The taxonomy should be used in combination with the supporting ontology list to identify and categorise all foreseeable and meaningful threat and hazard scenarios on the railway infrastructure. Both the threat and hazard taxonomy and the rail system ontology lists are structured in three levels, each level including more detailed granularity. There are eighteen (Level 1) threat and hazard categories, and these are:

1. Assault	10. Harmful contact with object
2. Collision between two trains	11. Asset failure
3. Derailment	12. Person struck by train
4. Train collision with buffer stop	13. Road traffic accident
5. Train collision with road vehicle	14. Slip, trip or fall
6. Electric shock	15. Trespass
7. Exposure to hazardous substance, condition or environment	16. Suicide
8. Extreme environmental / weather event or conditions	17. Terrorism / cyber-attack / unauthorised actions
9. Fire and explosion	18. Safety incident causes non-safety impact

The Railway System Ontology List contains elements that make up the rail system, including infrastructure, rolling stock, physical equipment, but also operational and organisational aspects, and the people operating and using or affected by the rail system. It attempts to contain a comprehensive list of all the elements of the railway which might be relevant to describing a threat or hazard scenario in context. There are six (Level 1) Ontology categories which include:

1. Infrastructure	4. Maintenance and Renewals
2. Railway Vehicles / Rolling Stock	5. People
3. Operations	6. Organisation

In combination, the hazard list and ontology list can be used to generate discussion and creative thought processes to identify and investigate potential threat and hazard scenarios in different contexts relating to different parts of the railway system (including interaction with different rolling stock/equipment/infrastructure, involvement of different people, in different environmental conditions/situations, etc.). The level 1 elements are broken down into further detail at level 2 and 3, resulting in approximately 500 detailed hazards and approximately 500 ontology elements (both lists contain a small number of duplications where an element is relevant to different categories of hazard/rail system).

Level	Threat and hazard list elements	Rail System Ontology list elements
Level 1	18	6
Level 2	84	64
Level 3	523	458

Further guidance is available on the RSSB website: https://www.rssb.co.uk/safety-and-health/risk-and-safety-intelligence/safety-management-resources/generic-hazard-list

Rail Delivery Group

National Rail

Rail Delivery Group Limited Registered Office, First Floor North, 1 Puddle Dock, London, EC4V 3DS
www.raildeliverygroup.com 020 7841 8000 Registered in England and Wales No. 08176197