Rail Delivery Group
National Rail

Guidance Note –
Station Incident Response Planning

Synopsis

This Guidance Note sets out good practice for operators to follow for Station Incident Response Planning, encompassing minor deviations from Business as Usual through to major emergencies.

Applicability

This Guidance Note has been prepared for passenger train operating companies, however, its content may also be of use to others.

Authorised by

James Burt
Chair, RDG Train Operators Emergency Planning Group

Issue record

Issue	Date	Comments
One	April 2016	Original version as an ATOC document.
Two	November 2019	Following periodic review and reformatted as an RDG document

Contents

Part 1   About this document

1.1   Responsibilities

1.1.1   Copies of this Guidance Note should be distributed by RDG members to persons within their respective organisations for whom its content is relevant.

1.2   Explanatory note

1.2.1   RDG produces RDG Guidance Notes for the information of its members. RDG is not a regulatory body and compliance with RDG Guidance Notes is not mandatory.

1.2.2   RDG Guidance Notes are intended to reflect good practice. RDG members are recommended to evaluate the guidance against their own arrangements in a structured and systematic way. Some or all 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 to adopt) elements of the guidance should be documented.

1.3   Guidance Note status

1.3.1   This document is not intended to create legally binding obligations between railway duty holders and should be binding in honour only.

1.4   Supply

1.4.1   Copies of this Guidance Note may be obtained from the RDG members' website.

Part 2 Introduction and purpose

2.1 Introduction

2.1.1 This guidance describes the components which make up a structured approach to Station Incident Response Planning. In the form of a template Station Incident Response Plan (SIRP), it sets out arrangements to enable railway undertakings to provide an effective response to accidents, incidents and other emergencies on or affecting a railway undertaking managed station (there is equivalent guidance in place for Network Rail Managed Stations).

2.1.2 Whilst this guidance is intended for use within railway undertakings, to certify effective co-ordination, the content herein has been consulted and harmonised with and reflects some of the emergency response arrangements of Network Rail and the emergency services. The guidance may be shared with third parties for their information only.

2.1.3 This guidance specifies generic approaches and actions to be implemented in the event of an incident on or affecting a railway undertaking managed station.

2.1.4 It does not seek to address station level response specific to disruption to train services.

2.1.5 Where additional or separate arrangements apply to a specific location, details should be provided within station specific plans. This guidance can also be used as an information source for a number of organisations, to allow them to understand the responsibilities of those who have a role in managing railway incidents.

2.1.6 Railway undertaking managed stations vary considerably in their size, physical and operational complexity, the frequency and type of train service operated, the numbers and types of passenger carried and the number of internal (i.e. other railway undertakings whose services call, Network Rail, the BTP) and external (e.g. local authorities, retail outlets, contractors) interfaces. Hence there can be no single definitive incident response plan appropriate to all stations and this Guidance Note does not attempt to provide one. Instead, it is intended to assist those responsible for individual stations in putting together response plans specific to their own circumstances by identifying the various factors, challenges and options that need to be considered when developing and implementing them.

2.2 Purpose

2.2.1 The purpose of this guidance is to identify and show the relationship to a number of plans which support the development of a SIRP. It also proposes a framework for developing SIRPs.

Part 3 Definitions

3.1 Definitions used within this document

3.1.1 For purpose of this guidance document the following definitions apply:

i) **Accident:** An unplanned, uncontrolled or unintended event, giving rise to death, ill health, and injury, damage to the environment or property, or other loss.

ii)   Cold debrief: A more comprehensive review of an incident and the response and recovery from same held within 28 days after the incident has concluded.

iii)   **Critical incident:** This is a police term and is defined as any incident where the effectiveness of the police response is likely to have a significant impact on the confidence of the victim, their family and/or the community. The corresponding rail terminology will be major incident.

iv)   **Emergency:** The Civil Contingencies Act (2004)[1] defines an emergency as:

   a)   An event or situation that threatens serious damage to human welfare in a place in the United Kingdom,
   b)   An event or situation that threatens serious damage to the environment in the United Kingdom, or
   c)   War, or terrorism, that threatens serious damage to the security of the United Kingdom.

v)   **Hot debrief:** A review of an incident and the response and recovery from same held immediately or shortly after the incident has concluded.

vi)   **Incident:** An unplanned or uncontrolled event which under different circumstances may have resulted in an accident. For the purposes of this document, the term "incident" includes "accident" and "emergency".

vii)   Major incident: An unplanned event that requires the implementation of special arrangements over and above normal operating procedures. A situation which constitutes a major incident for one organisation need not be a major incident for another.

Part 4 Background

4.1   Initial triggers

4.1.1   The initial trigger for developing this guidance was to take lessons learned from an incident within the North Terminal at Gatwick Airport on Christmas Eve 2013 in which a loss of power resulted in major and high profile disruption and consider how these could be applied in a rail context.

4.1.2   Its drafting was supported by the RDG (previously ATOC) Train Operators Operations Council which noted that it had been many years since the industry had faced the challenge of responding to a very major incident (Ladbroke Grove – the most recent to result in double figure fatalities was in 1998) and hence there was very little first-hand experience of handling such events at a senior level. This remains the case as at the date of issue of this version of the document.

---

[1] https://www.legislation.gov.uk/ukpga/2004/36/contents

4.2 Societal expectations

4.2.1 In addition, changes in societal expectations and the growth of social media mean that the manner in which a company responds is today subject to unprecedented levels of public scrutiny with consequent risks to reputation. A big part of the challenge to organisations – including railway undertakings – is to ensure that the public focus remains on the incident itself rather than the response to it. Operators might not be able to counter all threats and risks to the effective running of rail services but they can demonstrate a professional approach to response.

4.3 Update to the National Rail Security Programme

4.3.1 The National Rail Security Programme (NRSP) was re-issued in 2017 following an extensive review. This served to highlight the need to, if not fully integrate, then at least to more closely align station security and emergency response plans and arrangements which up hitherto been quite separate. The 2017 version of the NRSP places a greater emphasis on rail operators developing responses to a range of terrorist related threats. The likely responses will in the main cover most (if not all) of the risks associated with the day to day running of the railway.

Part 5 European requirements

5.1 Applicable European documents

5.1.1 European requirements for incident response planning and management are contained in a number of different documents, in particular:

i) Sections 4.2.3.6, 4.2.3.7 and 4.2.3.8 of Commission Regulation (EU) 2015/995 of 8 June 2015 amending Decision 2012/757/EU concerning the technical specification for interoperability relating to the 'operation and traffic management' subsystem of the rail system in the European Union (OPE TSI).
See https://op.europa.eu/en/publication-detail/-/publication/6a6e3ffc-1ef1-11e5-a342-01aa75ed71a1/language-en.

ii) Annex III(2)(i) to the Railway Safety Directive 2004/49/EC, on basic elements of the safety management system.
See https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:220:0016:0039:EN:PDF.

iii) Annex II(R) to the Common Safety Methods for assessing conformity (CSM CA), on criteria for assessing conformity with the requirements for obtaining safety authorisations / safety certificates.
See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1158&from=en and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1169&from=EN.

Part 6 UK requirements

6.1   RIS-3118-TOM and GOGN3518 current versions

6.1.1   UK requirements were originally set out in Railway Group Standard (RGS) GORT3118 - Incident Response Planning & Management. However, the content of this duplicated the European requirements listed above once these were published, hence rendering it redundant as a national standard. Notwithstanding this, the Standard contained much other information seen to remain of value and hence it was retained and re-issued, unchanged, in Rail Industry Standard (RIS) RIS-3118-TOM, issued in December 2016.

6.1.2   The difference in status between the two publications means that compliance with the content can no longer be mandated. However, it remains recognised good practice in respect of ~~identifying interface requirements for enabling a consistent, comprehensive and structured process for rail incident response planning and management and encourages~~. It requires duty holders to work together in a process of cooperation in order to produce plans for dealing with accidents and incidents.

6.1.3   GORT3118 was supported by GOGN3518 Guidance on Incident Response Planning & Management. GOGN3518 remains current and has been retained unchanged to support RIS-3118-TOM by ~~Associated RSSB guidance document GOGN3518 - Guidance on Incident Response Planning & Management, issued in 2008 (44 pages),~~ giving ~~es~~ guidance on interpreting the latter's ~~requirements content~~~~of GORT3118 but does not constitute a recommended method of meeting any set of mandatory requirements~~.

4.46.2   Review of RIS-3118-TOM

4.4.16.2.1   RSSB commenced a major review and updating of RIS-3118-TOM an GOGN3518 in the latter half of 2018 with formal consultation with industry on the revised draft taking place in July 2019.

4.4.26.2.2   The new version is intended to reflect changes to technology, emergency services' practices and responsibility arrangements within the industry since the document was first published. It has also been merged with GOGN3518 and rationale and other guidance has been added where appropriate.

6.2.3   RSSB does not envisage that the proposed revisions to the document will require any significant change on the part of industry as it will reflect present arrangements and therefore be more relevant to those staff who need to refer to it.

6.2.4   The revised version is expected to be published in December 2019.

6.2.5   Familiarity with taking due consideration of the content of the new version (when published) is strongly advocated.

~~Part 5~~ Part 7   What is a Station Incident Response Plan (SIRP)?

5.17.1   Station Incident Response Plan (SIRP)

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

7.1.2 The purpose of the SIRP is to set out the details of that response – what it is, how it is to be delivered and how and when it is to be activated.

7.1.3 Conceptually the SIRP comprises a number of different components (see part 12.1). This Guidance Note makes no recommendation as to whether these should be brought together in a single physical plan or maintained as separate documents. However, where two or more plans addressing these various components are in place, it is essential that they are fully aligned with each other and that there are no gaps in their collective coverage.

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

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

5.1.37.1.6 The SIRP is informed by:

  i) Variations to the Station Plan (SP) (see part 12.3) based on identifiable risks, e.g. loss of power, industrial action, flooding, overcrowding, terrorist attack, etc.

  ii) Identification of the risks and mitigation measures e.g. partial or part closure of the station, bringing in additional staff/security, emergency evacuation, etc.

  iii) The threats as set out in the National Rail Security Programme (NRSP) (see part 12.5).

5.1.47.1.7 There is no predefined structure for a SIRP. An outline for the content of a SIRP is shown as an Appendix. Please note that this is a guide only as local circumstances may dictate differences in approach.

5.1.57.1.8 The aviation experience is that there may be many risks but most can be covered by a generic response so there is no necessity to complete a different plan for every threat.

Part 6 Part 8   Alignment with Network Rail

6.18.1 Network Rail SIRPs

8.1.1 Network Rail has in place both a template and a Company standard for SIRPs which apply in respect of all its managed stations.

6.1.18.1.2   There has been cooperation between the (former) ATOC team developing this Guidance Note and the Network Rail team developing the standard. There is a high degree of alignment between the two and any differences reflect that Network Rail can mandate the adoption of the standard and that their business is structured differently from railway undertakings.

6.1.28.1.3   Network Rail undertook a major review of their arrangements and have moved away from a series of separate plans (covering emergencies, crowd control, fire precautions, security, special events, customer information and business continuity) in favour of a single holistic plan. Further details of how this is structured are provided in Appendix B.

~~Part 7~~ Part 9   Railway undertaking roles and responsibilities

~~7.1~~9.1   Categorisation under the Civil Contingencies Act

~~7.1.1~~9.1.1   Railway undertakings (and Network Rail) are defined as Category 2 responders within the Civil Contingencies Act. Their role at an incident is ensure safety, to support the emergency services during the initial response, consequence management and finally investigation and recovery.

~~7.2~~9.2   Alignment with JESIP

~~7.2.1~~9.2.1   As Network Rail has already done, railway undertakings should adopt the working ethos of the Joint Emergency Services Interoperability Programme (JESIP) – see part 17 below.

~~Part 8~~ Part 10   What does this guide do?

~~8.1~~10.1   Overview

~~8.1.1~~10.1.1 This document will give those tasked with creating and developing SIRPs guidance as to the process that should be adopted to complete this activity. It covers the following:

i)   What the suggested planning processes are and what they entail.

ii)   How to complete the components which support the planning process and what should be considered when producing/developing it.

iii) Who to consult with when producing and developing the plans.

iv)   How to test and validate the plans.

v)   How to publish the plans.

vi)   How to ensure staff are trained appropriately.

vii) How staff and stakeholders are briefed on the content of the plans.

Part 9 Part 11   Skills and competency for completing SIRPs

9.1 11.1   Overview

9.1.1 11.1.1 The task of completing a SIRP should not be taken lightly. Current practice shows that certain individuals are given the responsibility for completing station plans but few, if any, are qualified in plan writing, planning, exercising or validation. There are no training courses within Network Rail or the wider rail industry that are specifically designed to give those tasked with creating and developing station plans the necessary skills and competencies. Many have experience in completing plans but having a formal understanding of planning principles is considered an essential qualification.

9.2 11.2   Emergency Planning College

11.2.1   It is suggested that the courses provided by the Emergency Planning College (EPC) at Easingwold (or equivalent) should be considered as a pre-requisite to help those responsible for station plans to understand the principles of emergency planning. The EPC currently provides courses for civil protection, plan writing, exercising and testing, and business continuity management. There may be other providers who are able to offer similar courses.

11.3   Building on existing skills and knowledge

9.2.1 11.3.1 In practice, most SIRPs are not written from scratch but are updated versions of plans previously in place. It is recommended that those who are responsible for updating plans, particularly if new to the role and relatively inexperienced, are supported by and the resulting plans reviewed by those with greater skill sets.

Part 10 Part 12   Recommended composition to Station Incident Response Planning

10.1 12.1   Components

10.1.1 12.1.1 Research has identified that there are a number of components which together make up a comprehensive approach to Planning. The components are:

    i)   Station Plan.

    ii)   Station Security Plan.

    iii) Station Incident Response Plan.

    iv)   Evacuation Plan.

    v)   Operational Continuity Plan.

10.1.2 12.1.2 Irrespective of the degree to which these various components are combined together - if at all - they are mutually interdependent and link as per the diagram on the next page:
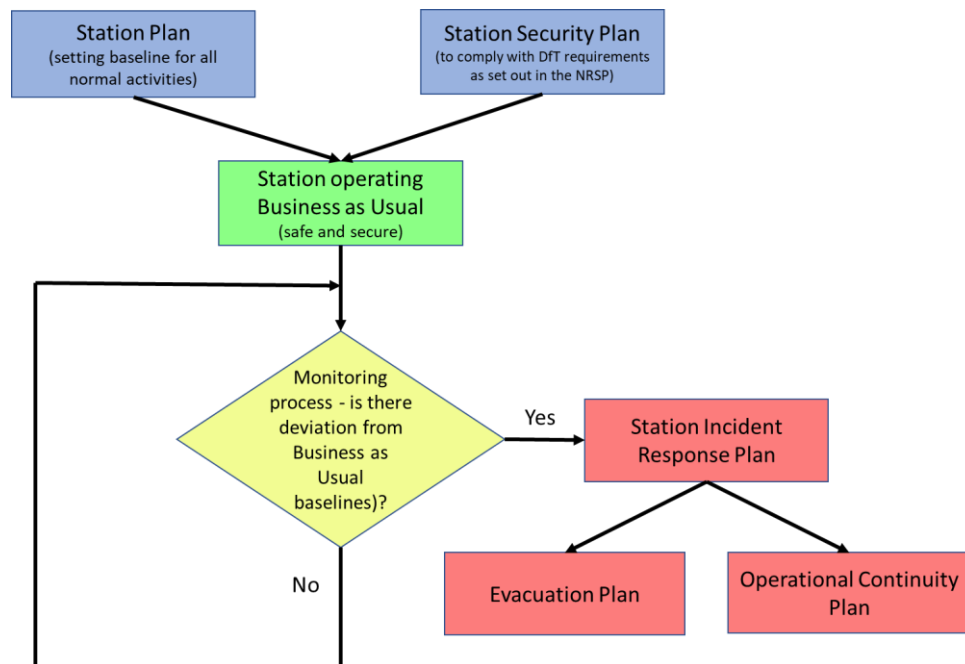
~~10.2~~12.2   **Processes**

~~10.2.1~~12.2.1 There are a number of common processes which support all of the above. These are:

  i) Communication.

  ii) Training.

  iii) Exercising.

  iv) Post incident review.

~~10.2.2~~12.2.2 Each of these components and the common processes are defined in more detail below.

~~10.3~~12.3   **Station Plan[2]**

~~10.3.1~~12.3.1 The SP sets out what business as usual looks like across all of the activities undertaken. It should state its purpose and scope.

~~10.3.2~~12.3.2 This sets the baseline for the activities and enable the operator to identify any deviations from the state of normality.

~~10.3.3~~12.3.3 The range of business activities covered by the SP would include:

  i) Crowd management.

  ii) Automated announcements.

[2] Within Network Rail, the information listed in this section is generally provided within the Business as Usual (BAU) / Station Information part of the station's SIRP.

      iii)   Catering outlets.

      iv)   Customer information screens / display boards.

      v)   Data links.

      vi)   Electricity supply.

      vii)   Evacuation.

      viii)   Fire alarms and other alerting systems.

      ix)   Heating.

      x)   Information points.

      xi)   Lighting.

      xii)   Phone lines.

      xiii)   Public address systems announcements.

      xiv)   Public information messages.

      xv)   Retail outlets.

      xvi)   Security checks.

      xvii)   Ticket gates.

      xviii)   Ticket sales.

      xix)   Toilets and washing facilities (both public and staff).

      xx)   Train dispatch.

      xxi)   Water supply.

      xxii)   Others as identified.

~~10.3.4~~12.3.4 The SP should also identify the triggers which show that the activity has or is moving away from the state of normality. These triggers should be used by the operator to consider if any response or change in response is required.

~~10.4~~12.4   Triggers, thresholds and escalation

~~10.4.1~~12.4.1 A process should be put in place to identify any deviation from the defined "business as usual" baseline, e.g. failure of electricity supply, an unusual degree of overcrowding, emergency incident. This should include monitoring to ensure tolerable thresholds are not exceeded and recording where appropriate decisions to implement or not implement the SIRP.
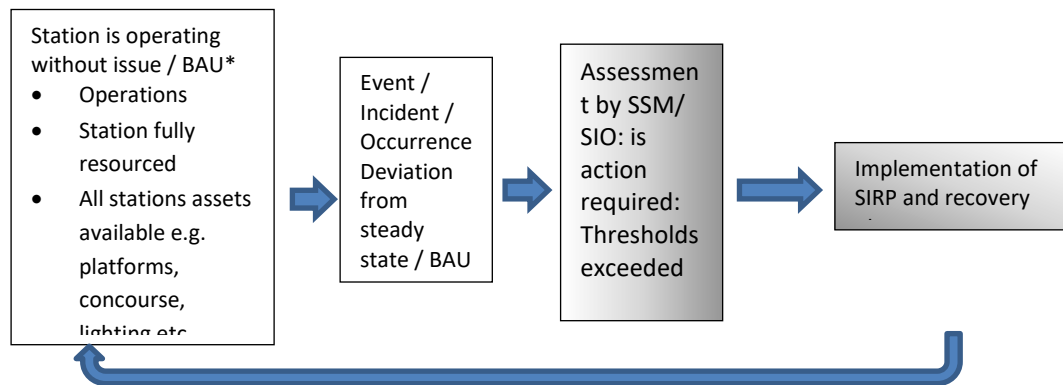
* BAU: Business as usual

~~10.5~~12.5   Station Security Plan (SSP)[3]

~~10.5.1~~12.5.1 A SSP is required to be produced in order that railway undertakings comply with the requirements set by the DfT under the auspices of the NRSP.·

~~10.5.2~~12.5.2 The SSP is a classified document (Official Sensitive) which means that it cannot be made available to railway undertaking staff who do not have Counter Terrorist Check (CTC) clearance. It is issued to:

   i)   National Security Contacts (and deputies).

   ii)   Directors with Responsibility for Security.

   iii)   Cyber Security Contacts.

~~10.5.3~~12.5.3 In most cases, Station Managers will not have direct access to the NRSP because they will not have security clearance. Railway undertakings will have to ensure that the requirements of the NRSP are communicated to Station Managers to ensure they are carried out as required.

~~10.5.4~~12.5.4 The content of the SSP has to be agreed with the DfT and railway undertakings are inspected on a regular basis to ensure compliance. Advice as to the content of a SSP can be obtained from the DfT.

~~10.5.5~~12.5.5 The measures outlined in the NRSP apply to Station Facility Owners (SFOs) of those stations in Categories A, B and C (but not D). The list of stations with their categorisation is set out in an Appendix to the NRSP.

~~10.5.6~~12.5.6 The measures specified in the Security Response Level (SRL) tables in the NRSP must be applied to a relevant location in accordance with the current SRL, as notified to the SFO or operator in writing by the Secretary of State.

---

[3] The Station Plan and Station Security Plan could be the same document but there will need to be consideration given to whether some of the content of the latter contains restricted information (Official and/or Official Sensitive) which would limit access.

~~10.6~~12.6 Evacuation, invacuation and lockdown plans

~~10.6.1~~12.6.1 Railway undertakings should already have in place a plan to evacuate a station for an actual or suspected fire. The threat/risk assessments should identify a range of new circumstances when a full or partial evacuation of the station is required. They should also determine the speed in which the evacuation should take place, i.e. immediate, controlled over a short time frame, controlled over a longer period.

~~10.6.2~~12.6.2 Research has shown that it is likely that a generic "base plan" should be sufficient to cover the majority of eventualities identified in the threat/risk assessments. For some of the threats/risks an evacuation might not be necessary. Evacuation should only be used as a viable and appropriate response to a threat/risk.

12.6.3 Railway undertaking should note that there may be circumstances when either invacuation or lockdown may be a more appropriate response than evacuation, either for public, staff or both.

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

    ~~i)~~ii) Lockdown involves the securing of external entry points and members of the public and/or staff being instructed to take immediate shelter in a secure location such as a store room or office until such time as the all clear signal has been given. Lockdown would typically be invoked as a response to a security incident/threat.

~~10.6.3~~12.6.4 In order to facilitate an invacuation or lockdown, railway undertakings should seek to identify potential 'safe havens' within the station to which members of the public and/or staff can be directed.

~~10.6.4~~12.6.5 Railway undertakings might wish to consider whether some of their plans for dealing with specific threats may be restricted.

~~10.7~~12.7 Operational Continuity Plan (OCP)

~~10.7.1~~12.7.1 The time to return to business as usual (or a revised business as usual) will depend on the nature of the incident/event. For some eventualities the return to normality will be quick but for others it might be days, months and in a few cases even longer (in which case railway undertakings should have in place business continuity plans which show how services will continue if, for example, a station needs to be rebuilt following a building collapse).

~~10.7.2~~12.7.2 Railway undertakings will need to demonstrate how the business operation (as shown in the SP) will continue after the emergency response and before return to normality. If the event has been significant then business as usual might be very difficult to achieve for many days, weeks or even longer.

~~10.7.3~~12.7.3 Examples of where an OCP might be required include the following (the list is not intended to be exhaustive):

    i) Long term loss of an external supply, e.g. water, electricity or gas.

ii)   Loss of an external service, e.g. refuse collection, cover by a security company, etc.

iii)   Insufficient staff to continue a safe operation, e.g. following a critical incident in the vicinity of a station, a health emergency which has affected staff, strike, etc.

iv)   Waiting for a response by the emergency services to be completed - this may be to allow for a forensic examination of a scene or check for a suspicious device or behaviour.

v)   A critical piece of station infrastructure has failed which cannot quickly be repaired or replaced.

vi)   A structural failure has occurred which requires extended remedial work.

~~v)~~vii)   Decontamination is required.

~~Part 11~~ Part 13   Post Incident Review (PIR)

~~11.1~~13.1   Introduction

~~11.1.1~~13.1.1 Incidents will differ in their complexity and the time it takes to return to normality. They may be undertaken in addition to or alongside Hot and Cold Debriefs.

~~11.2~~13.2   When to undertake a Post Incident Review

~~11.2.1~~13.2.1 A PIR should be undertaken after every major/critical incident.

~~11.2.2~~13.2.2 A PIR should be considered in the following circumstances:

i)   An aspect of the response was not as effective as it could have been.

ii)   It is a company requirement to under a review following an incident.

iii)   There has been significant public/government scrutiny as to how the incident was handled.

~~11.3~~13.3   Who should lead a Post Incident Review?

~~11.3.1~~13.3.1 There is no hard and fast rule about who should lead the PIR. It is presumed that this will be the railway undertaking. Depending on the nature of the incident, consideration might be given to the lead organisation being the BTP or, because of confidentiality issues, it might be necessary to hold two separate (but coordinated) reviews.

~~11.3.2~~13.3.2 A PIR is, simply, an evaluation of the response to an incident. The evaluation can be aimed at the entire company, selected departments or groups, and/or the external responders to the incident. The review identifies weaknesses while emphasising the strengths within the company which will serve to reinforce improved planning.

11.3.313.3.3 PIRs are critical to the long-term success of the company. While the event is fresh in everybody's memory, it is important to document, organise, and prioritise what everyone in the company has learned and convert these lessons learned into real changes in policies, plans, procedures, personnel, and budget priorities. The companies that identify and accept these lessons and change the way they do business are those that will respond more effectively during the next incident.

11.3.413.3.4 Keys questions to consider as part of the PIR are:

i) What should be learned from the incident?

ii) What can be done to avoid repeating the same mistakes?

iii) How to determine which policies and procedures worked and which didn't work?

iv) What are the implications of the incident on customers, staff, third parties using railway undertaking facilities and the wider rail industry?

v) What changes need to be made? What worked well?

vi) How do these questions get answered? Who has the authority to address the findings?

vii) Should an expert, third-party be invited in to facilitate this process?

11.3.513.3.5 Key considerations in terms of the PIR itself are:

i) Who will conduct the PIR?

ii) Who will be on the review team?

iii) What expertise will be needed?

iv) What level of management should be involved?

v) What functional areas of the company need to be represented?

vi) What locations need to be involved?

~~Part 12~~ Part 14   Communication

~~12.1~~14.1   Introduction

~~12.1.1~~14.1.1 Where a Station Committee exists[4], it is expected that all Plans (except those which are restricted) will be developed with the membership. It will be the responsibility of the lead representatives from each partner to make sure that the Plans are promulgated as necessary.

~~12.2~~14.2   Sharing of plans

---

[4] There is already a requirement under the NRSP for a Station Security Committee to exist at Cat A and B Stations. The Station Security Committee and a Station Committee as not necessarily the same thing. It is for operators to decide if they wish to keep them separate.

12.2.1 14.2.1 It is recommended that Plans be shared with the following:

> i) The BTP (both representatives of the local policing team and specialist policing team).
>
> ii) Other companies and organisations which operate at the station where this is considered appropriate.
>
> iii) Tenants.
>
> iv) The local Home Office Police force.
>
> v) The Local Authority.
>
> vi) Other transport operators that operate outside the station.
>
> vii) Other emergency services.
>
> viii) Other relevant organisations.

12.2.2 14.2.2 All Station Managers should ensure that all their staff are made aware of the existence and location of the Plans referred to in this guidance and the key responsibilities contained within them.

12.2.3 14.2.3 Consideration should be given to how the Plans can be made available to a wider group of people. Options include:

> i) Hard copies which should be kept at locations where they are accessible at the time an incident is taking place. A copy should be kept off-site in the event of a critical incident which requires the closure of a station.
>
> ii) Use of an Extranet so that authorised partners may access the Plans on line.
>
> iii) Intranet so that staff may access the Plans on line.

12.2.4 14.2.4 Railway undertakings and the BTP are moving into a position where information is made available to them on PDAs and smart phones. The provision of digital versions is therefore recommended.

12.2.5 14.2.5 One of the key challenges is version control so that staff and partners have access to the most up to date set of plans. It should be the responsibility of the Station Manager to ensure that all hard copies of Plans held at stations are up to date and accessible. They should also ensure that any digital versions are aligned with hard copies.

Part 13 Part 15 Training

13.1 15.1 Overview

13.1.1 15.1.1 Railway undertakings should put in place a comprehensive approach to training to make sure that the objectives and contents of Plans are understood by staff.

13.1.2 15.1.2 There are a variety of ways of achieving this including:

i) Awareness.

ii) Briefing.

iii) Training.

~~13.1.3~~15.1.3 Railway undertakings already have to comply with the training requirements of the NRSP[5] and there are a lot of synergies between what is covered in respect of the SSP and the other plans referred to in this guidance.

~~13.1.4~~15.1.4 It is proposed that railway undertakings compile a document which shows the approach to ensuring the effective delivery of the Plans set out in this guidance.

~~13.1.5~~15.1.5 The document should include:

i) The roles for which awareness/briefing/training is required.

ii) What jobholders will be trained in.

iii) How the awareness/briefing/training will be delivered, assessed and refreshed.

iv) How learning from training will feed back.

v) How training records are going to be compiled and maintained.

~~Part 14~~ Part 16 Exercising and drilling

~~14.1~~16.1 Overview

~~14.1.1~~16.1.1 Railway undertakings should have a risk based exercise programme in place to test their response to all incidents, based on current awareness of key plans/arrangements and the consequences of getting it wrong.[6] The objective of exercising is to identify vulnerabilities in the current arrangements - either because they are untested, complex or involve multiple organisations. The type of exercising to be undertaken may be influenced by cost, practicality, number of available participants, impact on business or other factors.

~~14.1.2~~16.1.2 The table on the next page provides a guide to railway undertakings to determine their approach to exercising:

---

[5] A Security Training Plan has to be produced for DfT and compliance is inspected.
[6] As a minimum, Cat A and B stations must exercise their security response plans/arrangements on an annual basis.

Proportionate use of exercising

14.1.316.1.3 Lessons learnt through exercising should be captured, shared, and fed back into response plans/arrangements, as appropriate, by the railway undertaking.

14.1.416.1.4 Drilling – the repetitive practice of specific skills, ultimately to the point at which they become second nature and can be applied without the need for significant direction – can be an effective training method for situations or staff where the priority is to act rather than think.

Part 15 Part 17 Joint Emergency Service Interoperability Programme (JESIP)[7]

15.117.1 IntroductionOverview

15.1.117.1.1 JESIP was established in 2012 to address the recommendations and findings from a number of major incident reports.

15.1.217.1.2 When police, fire and ambulance services respond together to incidents, along with other agencies, each organisation brings its own expertise to that situation. JESIP has recognised this and developed and published the JESIP Joint Doctrine – the interoperability framework. This guidance has been designed to help clarify the roles and responsibilities of emergency services in the early stages of response to a multi-agency incident.

---

[7] There is a dedicated site – please see http://www.jesip.org.uk/home.

APPENDIX A

Station Incident Response Plan (SIRP) Proposed Structure

A.1   Structure

A.1.1 The proposed structure for a SIRP is:

i)   Contents.
ii)   Introduction.
iii)   Roles and responsibilities.
iv)   Definitions.
v)   Command.
vi)   Role of the Station Incident Officer (SIO).
vii)   Command post.
viii)   Multi-Agency Threat and Risk Assessment (MATRA).
ix)   Resources.
x)   Triggers, thresholds and escalation.
xi)   Business continuity/desired end state.
xii)   Working strategy.
xiii)   Record keeping.
xiv)   Business as usual – what does the station look like when operating normally.
xv)   Station specific information (maps, diagrams, how the fire alarm works, etc.).
xvi)   Specific Incident Response Plans covering:
    a) Evacuation.
    b) Crowd management.
    c) Event plan.
    d) Terrorist incidents (covering all the threats identified in the Identified Threats Scenarios within the NRSP).
    e) Public protest on station.
    f) Fire alarm activation.
    g) Rendezvous points for emergency services. and
    h) Other 'What If's' (such as flood in station, fire, public disorder/public protest, gas leak, loss of key access routes/disabled access, loss of escalators, loss of communication systems, loss of power, loss of water, building collapse, crime scene, loss of waste facilities (and toilets), external non-rail incident, incident on London Underground (applicable to London only)

A.2   Contents

A.2.1   Insert a contents page

A.3   Introduction

A.3.1   Explain how the Plan was put together, its purpose and what other documents are referred to and where they can be located.

A.4   Role and responsibilities

A.4.1   Identify the roles and responsibilities for your company and the partners you have worked with on developing the Plan. Include partners who will be involved in any response arrangements.

A.5   Definitions

A.5.1   Insert the list of definitions used in the SIRP.

A.6   Command

A.6.1   Railway undertakings should comply with the standard UK three-tier command structure for the management of the response to an incident affecting the railway. These tiers are defined as Strategic (Gold), Tactical (Silver) and Operational (Bronze). The detailed response depends on the circumstances, in liaison, if appropriate, with the emergency services.

A.6.2   Having a command structure provides a framework for delivering a strategic, tactical and operational response to an incident. It also allows processes to be established that facilitate the flow of information, and makes sure that decisions are communicated effectively and documented as part of an audit trail.

A.6.3   In the event of a major incident, a command and control structure will be put in place to provide overall management and coordination of the response. This comprises Gold (strategic), Silver (tactical) and Bronze (operational) levels. Rail industry involvement in this involves the appointment of a Rail Incident Officer by Network Rail and the appointment of a Train Operator Liaison Officer (TOLO) or Station Incident Officer (SIO) by the Train Operator(s)[8] to support the RIO. See below for an explanation of the differences between the three command levels.

Strategic (Gold)

   i)   This is the strategic level of command and will be located away from the scene. It does not exercise operational control of the incident but it will establish policy within which Tactical Commander(s) will work. It will provide resources, make executive decisions, prioritise demands, consider long-term incident handling and decide plans to return to normality.
   ii)   Strategic Co-ordinating Group (SCG).
   iii)   Rail – British Transport Police (BTP).

Tactical (Silver)

   i)   This is the tactical level of command and may be located at or near the scene. The Silver Commander is the Incident Officer responsible for the operational management of the incident. Silver will prioritise resource allocation, plan and co-ordinate tasks to be undertaken, hold meetings and deal with inter-agency communications.
   ii)   STAC (Scientific Technical Advice Cell).
   iii)   Rail - Engineering staff, Rail Incident Commander (RIC) if appointed, otherwise RIO.

---

[8] For Network Rail managed stations, Network Rail will appoint the SIO

Operational (Bronze)

    i)   This is the operational level of command that is located at the scene or associated areas. There may be several Bronze Controls. Bronze level will assess the extent of the incident and determine specific tasks e.g. scene security, cordons, victim recovery etc.

    ii)   Rail – RIO (if RIC appointed), TOLO, SIO, Engineering staff.

A.7   Role of the Station Incident Officer (SIO)

A.7.1   The SIO is the person charged with the role of Tactical (on-site) command for incidents that occur on or within the confines of a station. The role of the SIO shall be undertaken by a railway undertaking or Network Rail member of staff depending on whether the station is managed by Network Rail or the railway undertaking. The role of the SIO should usually be undertaken, at railway undertaking /Network Rail stations, by a Shift Station Manager who has the relevant competencies.

A.7.2   For an incident that affects both the route and a station, the RIO will assume command of the incident and the SIO will report to that RIO.

A.7.3   The SIO will be appointed locally and will be of an appropriate level of seniority according to the severity of the incident, i.e. this could be a supervisory member of staff, shift station manager or station manager.

A.7.4   The Station will never determine the Strategic or Tactical levels of an incident. That should come from Route Control.

A.8   Command post

A.8.1   Good practice suggests that an incident command post is established from which the incident can be managed. This would normally be the Station Control Room, however, alternatives should be considered in case this is unable to be used. The purpose of the command post is to conduct and direct on-scene control of tactical operations.

A.8.2   The Incident Command Post will typically comprise the SIO and immediate staff and may include other designated incident management representatives.

A.9   Resources

A.9.1   The starting point for business continuity plans is that normal business cannot be achieved in extraordinary circumstances. It is therefore important that station resources can be deployed and reallocated to critical functions during an incident.

A.9.2   Station Plans should list the minimum resources and staffing levels required to fulfil those functions.

A.9.3   The SIRP should consider the number of staff required in order to isolate, contain and deal with the incident.

A.10   Triggers, thresholds and escalation

A.10.1   Please see the reference in the main text (para 11.8).

A.10.2   The level of any response will depend on a structured approach looking at indicators e.g. Green, Amber, Red type assessments and associated actions. Taking pedestrian flow in a key subway as an example this might be:

i)   Green = full body of individuals visible on CCTV images – BAU and no action needed.
ii)   Amber = only upper half of bodies of individuals visible – overcrowding apparent – appropriate action needed (e.g. direction of staff to area, closer monitoring).
iii) Red = only heads of individuals visible – serious overcrowding apparent – appropriate action needed (e.g. redirect passengers to alternative routes, alert station manager).

A.10.3   Each response element follows a set format which hopefully sets out the initial actions that should be undertaken when an incident occurs. These are:

i)   What information do I have and what information do I need?
ii)   What are the threats and risks to the station from this incident?
iii) What policies are available that I can use to resolve this incident?
iv)   What are my options for resolving this incident?
v)   What do I need to put in place to respond to this incident?

A.10.4   It is proposed that operators construct a table using the following format:

Threat/Risk	Indicators G, A & R	Response (policies/procedures)	Options - Mitigation Measures	Responding agencies and lead
Loss of water supply	Green – water supply working as normal at all locations Amber – water supply not present at some location and/or intermittent supply. Red – no water supply at all locations.	Amber – Establish what is causing the problem then consider if the temporary loss affects operations and if so what measures have to be introduced. Red – consider what services have to shut and the effect on operations.	a) Partial closure of the affected facility. b) Total closure of the affected facility. c) Partial closure of the station. d) Total closure of the station.	Lead: TOC Water Board
Loss of electricity supply				
Etc.				

A.11 Business continuity/desired end state

A.11.1 Plans should cater for dealing with the incident as well as managing business as usual activities. The OCP needs to be aligned with the SIRP.

A.11.2 It is considered good practice that whilst responding to the incident, any recovery plan is implemented at the same time as the SIRP is implemented.

A.12 Working strategy

A.12.1 A strategy is a plan of action designed to achieve a series of objectives or a particular goal and sets out the principles that responders to the incident are expected to uphold and the standards of behaviour they are expected to meet. It sets out the high-level overview of the incident response and, as such, does not get drawn into tactical or operational detail. Many organisations have their own values statements which are complementary to the working strategy.

A.12.2 Throughout an incident, decision makers should ask themselves:

   i)   Is what I am considering consistent with the working strategy?
   ii)   What would the victim or community affected expect of us in this situation?
   iii) What does my organisation expect of me in this situation?
   iv)   Is this action or decision likely to reflect positively on my professionalism and response generally?
   v)   Could I explain my action or decision in public?
   vi)   In lieu of any strategic intention or working strategy from the Network Rail Strategic Commander (Rail Incident Commander), the following 'default' working strategy should be adopted:

A.12.3 Operators, by working in partnership with the emergency services, rail industry colleagues and other stakeholders, will endeavour to:

   i)   Preserve life and reduce the risk of serious injury to those affected by the incident.
   ii)   Utilise process and procedures that maximise the safety and welfare of the public, emergency services and rail industry staff.
   iii) Support the return to normality by implementing service recovery plans at the earliest opportunity to minimise delay to the travelling public.
   iv)   Provide a prompt and professional response to the incident and adopt a partnership approach to enable a return to normality at the earliest opportunity.
   v)   Provide clear, consistent information (one truth) to customers to assist the travelling public to make informed decisions by having the right information at the right time.

A.13 Record keeping (decisions and log books)

A.13.1 The following benefits should be considered when making and keeping records:

   i)   They provide a record of all planning, strategic, tactical and operational decisions made and actions taken during an incident.
   ii)   They ensure an accurate record is available in the event of any subsequent investigation, Public Enquiry or litigation.
   iii) They allow the Incident Officer to record their justifications for a course of action or decision in a contemporaneous written record of the thought process supporting this action.

    iv)   Remember - records are for YOUR protection:
        a)   They provide a note (aide mémoire) from which to justify your reasoning and decisions later.
        b)   They assist in promoting coherent reasoning in the exercise of your discretion.
        c)   Honestly held beliefs and actions taken in good faith at the time should be recorded and rationalised.

A.13.2   When making a log:

    i)   Entries should be made accurately and in chronological order.
    ii)   Entries should be made at the time the information is received or at the earliest opportunity afterwards.
    iii) Entries should be made in ink or ballpoint pen.
    iv) No pages may be removed or inserted.
    v)   No entry may be erased or obliterated.
    vi) There must be no overwriting or double entries.
    vii) There must be no blank pages or spaces.
    viii) Pages must not be torn out.
    ix) When an alteration is necessary, a single line must be drawn through the error, correction entered and the alteration initialled.
    x)   The log must be maintained until such time as the incident is concluded or responsibility passes over.
    xi) A loggist should be used if possible.

A.14   Business as Usual – what does the station look like when operating normally?

A.14.1   This will be identified in the Station Plan.

A.15   Station specific information

A.15.1   The Plan should include the following information:

    i)   Maps.
    ii)   Diagrams.
    iii) How the fire and any other similar alarm systems work.
    iv) Predetermined messages.
    v)   Where plans are located.
    vi) Anything of use to staff and those responding to an incident.

A.16   Specific incident response plans covering:

A.16.1   In many cases a generic response plan will be able to cover for the majority of the threats/risks. However, this will not be the case for all eventualities. The following additional response plans may need to be developed:

    i)   Evacuation.
    ii)   Crowd management.
    iii) Event plan.
    iv) Terrorist related incidents ~~(suspect package, bomb threat, mtfa, cbrn)~~[9].
    v)   Public protest on station.
    vi) Fire alarm activation.

---

[9] See NRSP for guidance in response to a terrorist related threat.

vii) Rendezvous points for emergency services (noting that these may need to be different for non-security and security related incidents).

viii) Other 'what if's' (such as flood in station, fire, public disorder/public protest, gas leak, loss of key access routes/disabled access, loss of escalators, loss of communication systems, loss of power, loss of water, building collapse, crime scene, loss of waste facilities (and toilets), external non-rail incident, incident on London Underground (applicable to London only).

A.16.2 It should be noted that some of the Counter Terrorist (CT) response plans are classified and the detail is not widely circulated. BTP has specific response plans for many of the CT threats which are also classified.

APPENDIX B

Summary of Network Rail Station Incident Response Plan (SIRP) Structure

B.1   Overall structure

B1.1   The overall structure adopted is as shown below:
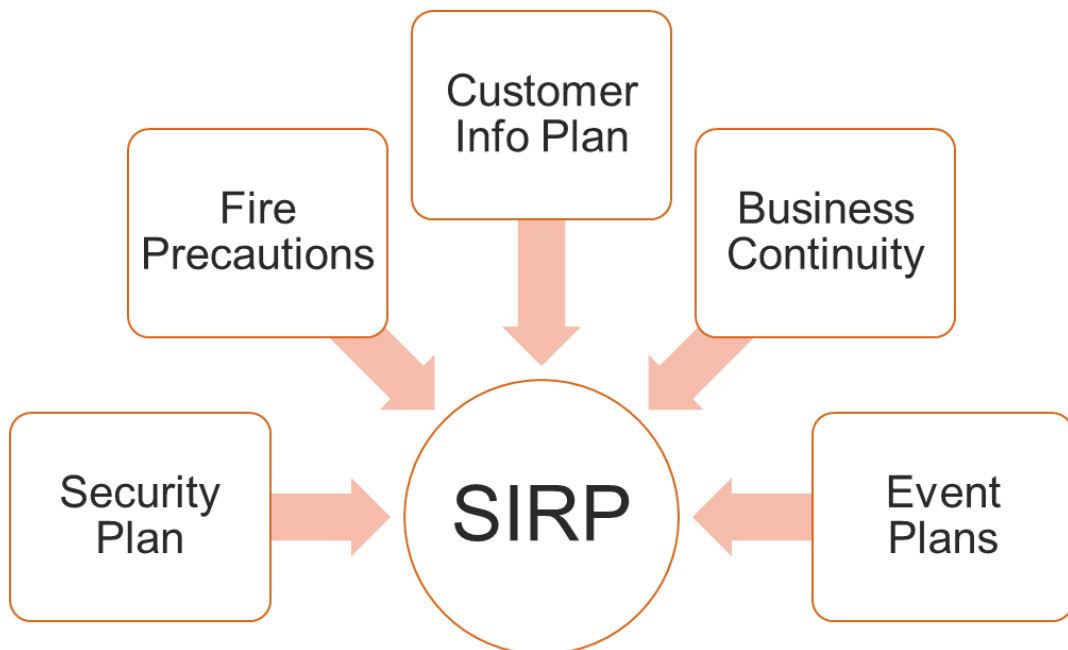
B.2   Core main template

B2.1   Core Main template, comprising:

i)   Introduction.
ii)   Station Incident Response Plan structure overview.
iii)   Application.
iv)   Strategic intent of working strategy for an incident.
v)   Planning process.
vi)   Exercise and testing.
vii)   Consultation matrix.
viii) Definitions.

B.3   Station information template

B3.1   Station Information template, comprising:

i)   Station key emergency and comms info.
ii)   Station asset info.
iii)   Station operations Business as Usual snapshot.
iv)   Tenants info.
v)   Train service and customer information.
vi)   Supporting maps.

B.4 Incident response template

B4.1 Incident Response template, comprising:

    i) Incident triggers, thresholds and escalations.
    ii) Incident management.
    iii) Command.
    iv) Working with the emergency services.
    v) Record keeping.
    vi) Incident response.
    vii) Sabotage / cyber attack.
    viii) Threats by phone, email etc.

B.5 Crowd management template

B5.1 Crowd Management template, comprising:

    i) Key principles.
    ii) Method of management.

B.6 Evacuation template

B6.1 Evacuation template, comprising:

    i) Principles of evacuation.
    ii) Evacuation options.
    iii) Maps.

B.7 Service disruption and customer information template

B7.1 Service Disruption and Customer Information template, comprising:

    i) Passenger information.
    ii) Provision of customer information to the station.
    iii) Triggers for implementation.
    iv) Response.

B.8 Customer welfare template

B8.1 Customer Welfare template, comprising:

    i) Triggers for implementation.
    ~~ix)~~ii) Response.