HIGHWAYS AGENCY

Safe roads, reliable journeys, informed travellers

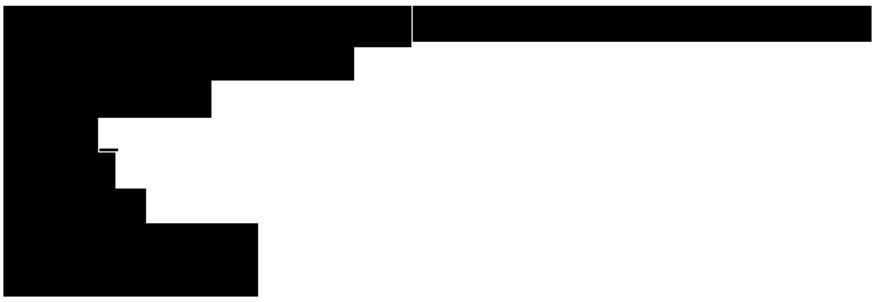
Area 13 Service Provider Contingency Plan Version 2.40

31st May 2013

If you receive a copy of this Plan, you must:

Read and understand it
Identify the role you have to play

and be prepared to undertake the actions ascribed to you



Page blank for pagination

Area 13

Service Provider Contingency Plan Version 2.40

Issue and Revision Record

Rev	Date	Originator	Checker	Approver	Description
2.40	31/05/2013	[redacted]	[redacted]	[redacted]	Annual Review (no major changes)
2.30	31/05/2012	[redacted]	[redacted]	[redacted]	Changes due to ASC Retrofit
2.20	31/10/2011	[redacted]	[redacted]	[redacted]	Various contact details amended. 6 monthly review
2.10	31/03/2011	[redacted]	[redacted]	[redacted]	Plan Holders and box of Reference updated
2.00	30/11/2010	[redacted]	[redacted]	[redacted]	New template Version 2.11 – AMM132_10

Blank page for pagination

List of Contents Page

Executive Summary

This is the Contingency Plan for Area 13.

It explains how the Area will escalate its Standard Incident Response from Operational Command (Bronze) to Tactical (Silver) and Strategic (Gold) Command when that is necessary.

This will ensure the most robust response possible to any severity of emergency or disruption to network operations.

The Plan has been written in accordance with the Highways Agency's (HA) Template for Area Service Provider Contingency Plans and has been approved by the HA's NW Service Delivery Manager. This version (June 2012) has been amended to incorporate the retrofit of Part 3 "Incident Response Operational Requirement" of the Asset Maintenance and Operational Requirements" in Area 13.

The Plan is reviewed & updated where required at 6-month intervals.

Where sections are not used, a brief description as to why has been included.

Any questions about this Plan or the related documents should in the first instance be referred to the Plan Manager.

Blank page for pagination

1 Purpose of the Plan

1.1 Introduction

This Plan explains how the Service Provider will escalate an incident response from Operational **(Bronze)** to Tactical **(Silver)** and Strategic **(Gold)** Command on occasions when needed.

The Plan refers to the Highway network shown in **Figure 1.2.** It refers to incidents affecting that network, whether occurring on or off it.

1.2 Structure of the Plan

The Plan has three components:

- This Contingency Plan setting out the escalated response of the Area 13 Service Provider to a Major or Critical Incident and is supported by:
- Emergency Diversion Route Document (EDRD)
- A Box of Reference which contains a wide range of information that may be needed by the Tactical Management Team managing an incident

1.2.1 Emergency Diversion Route Document (EDRD)

The Emergency Diversion Route Document (EDRD) contains details of Emergency Diversion Routes to be used in the event of an incident on or off the Strategic Network closing a section of HA road, along with other information required and identified by the guidance in AMM 71/06. This is a stand alone document that is stored either electronically or can be produced in a hard copy and issued to the relevant parties that require a copy.

1.2.2 Box of Reference

This Box contains major stakeholder contingency plans and other detailed reference information that the Tactical Management Team may require to manage an incident.

The contents of the box of reference are specified in Section 10.

It will be utilised in the event that the Tactical Management Room (TMR) is unavailable and redeployment of the facility to another site is required.

1.3 Glossary of Terms within the Plan

A list of terms which are used throughout the Plan is stored in **Appendix E** for reference.

1.4 Scope of the Contingency Plan

The Plan covers the actions to be taken by the Service Provider in escalating response to an incident, and interfaces between the Service Provider and other organisations.

In general, the emergency services will take control of any serious incident. This Plan is designed to ensure that the Service Provider is able to make a proper response to the situation in order to:

- Support the actions and requests of the emergency services
- Ensure that proper interfaces are achieved with other organisations
- Ensure that nuisance to HA's customers and Major Stakeholders is minimised
- Escalate management of the response to a higher level if necessary

The Plan is designed to ensure that:

- In such circumstances, the right members of the Service Provider are in the right place at the right time
- They are aware of their individual responsibilities, decisions and actions they have to take
- They have the information and resources necessary to make these decisions and undertake these actions in a timely and efficient way.

1.5 Escalation of Incident Response

There are separate but related Contingency Plans for:

- Service Providers
- Regional Control Centres

These Plans allow for the management of incident response to be escalated from the Service Provider to the RCC when circumstances require it. Each plan explains how the organisation will escalate and manage its response to an incident when it has that responsibility, and the functions it will perform when that responsibility lies elsewhere.

- Management of the response is escalated when any of the Common Incident Objectives (see below) are threatened at the current level of Command and Control.

1.6 Highways Agency Objectives

The Highways Agency (including the Service Provider) will give full support to the Emergency Services in attaining all the Common Incident Objectives, but will have a particular focus on objectives relating to its Customers First agenda:

- Avoid undue impact on surrounding area
- Minimise the impact of the incident on the travelling public
- Collate information for onward transmission to road users, Major Stakeholders, and other interested parties e.g. Government
- Restore the network to normal conditions as quickly as possible

1.7 Multi Agency Common Incident Objectives

The Incident Objectives listed below are common objectives for all agencies involved in managing an incident. All involved in implementing the Plan must be aware of the objectives set out in this section and strive to maximise support for them.

INCIDENT OBJECTIVES

Saving and protecting life
Relieving suffering

Protecting property
Providing the public with timely information

Containing the emergency
Limiting its spread
Maintaining critical services
Maintaining normal services at an appropriate level

Protecting the health and safety of personnel
Safeguarding the environment

Promoting self help and recovery
Restoring normality as soon as possible

These objectives embrace more than simply dealing with the incident itself and of particular importance in the context of this plan is the need to repair damaged infrastructure and reopen the road.

In addition, there are two further common objectives which are essential in managing an incident, but which are not considered critical to the implementation of the Contingency Plan:

Facilitating investigations and inquiries

Evaluating the response and identifying the lessons to be learned

1.8 Contingency Plan Escalation Procedure

The Contingency Plan is implemented when the Service Provider's Standard Incident Response Procedures are unable to contain an incident, to the extent that any of the Multi Agency **Common Incident Objectives** are threatened and the situation is likely to deteriorate further and become out of control without tactical or strategic intervention.

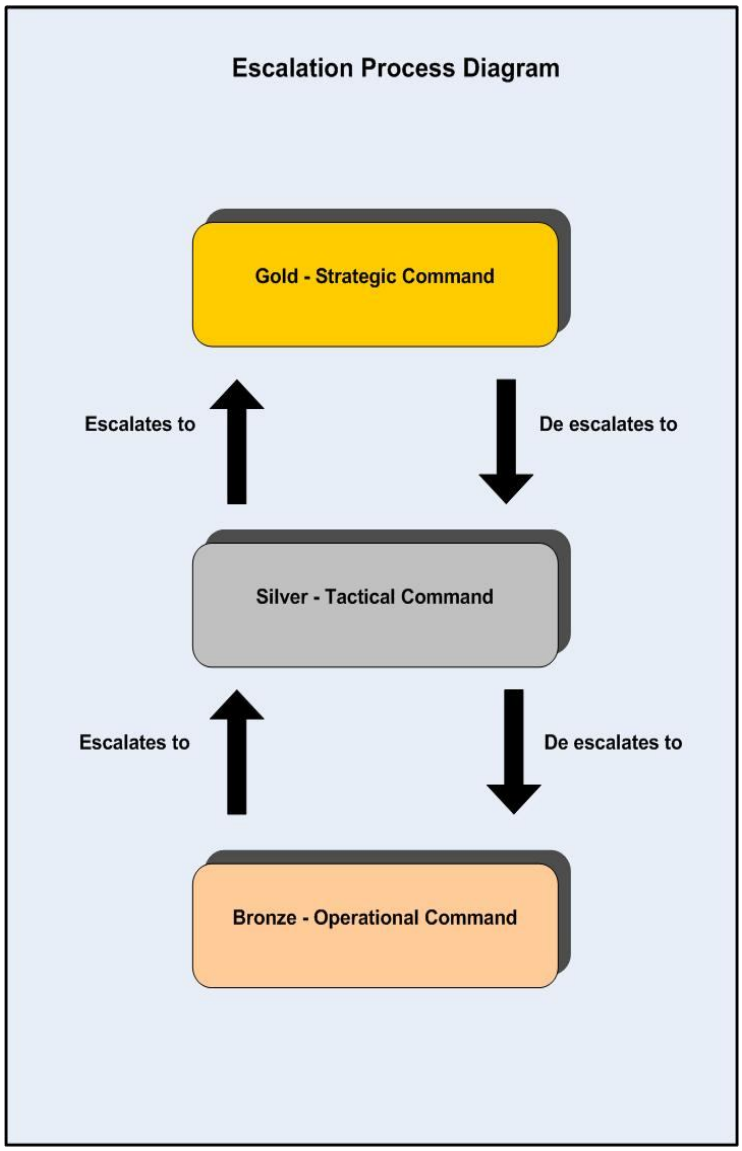
Figure 1.1 The Gold Silver Bronze (GSB) Command structure provides a system for escalating incident command to higher levels of command authority when required. Similarly, when these higher authority levels are no longer required the system allows for de-escalation to the most appropriate level of command.

In broad terms, command should be escalated to the next higher level of command authority (Bronze, to Silver to Gold) when:

- The incident Commander can no longer manage the response with the resources available to them
    - And/or
- They require support/authority to activate additional resources or authorise decisions
    - And/or
- The incident Commander believes that the incident is of such significance that a higher level of command authority is required to manage the response.

Incident Commanders should consider early escalation if they believe that any of the above criteria may be met. It is better to escalate early than to wait so long such that the incident response becomes compromised.

Figure 1.1: Escalation Process Diagram



1.9 Strategic Management by the HA Traffic Officer Service (RCC)

When the Service Provider is unable to manage the incident at Gold Command then Strategic management of the incident passes to the Traffic Officer Service (RCC). Details of how they operate can be found in their Regional Emergency Plan and the wider actions to be taken within the HA at this level are set out in HA's Standard Incident Management Framework Document (SIMF).

However, there are parts of the HA network where the on road TOS do not operate and in these instances the Service Provider will liaise directly with the Emergency Services at the scene and keep the RCC informed of the situation.

1.10 Interface with Regional Emergency Plans

This Plan will be consistent with the HA's NW Region – Regional Emergency Plan. The Regional Emergency Plan adopts the same procedures and terminology, and embodies the actions specified for the TOS in this Plan.

1.11 Plan Manager

[redacted]

[redacted]

1.12 Plan Updates

The Plan is a live document that is to be updated every six months. The Plan will be subject to a continuous flow of new information received. This information has to be managed and a document called the "Guidance and Management of Service Provider Contingency Plans" has been produced to assist the Plan Manager with the task of updating the Contingency Plan and associated documents.

Any significant changes needed for the Contingency Plan must be forwarded to the HA Network Resilience Team via the Area Performance Team, this information shall then be entered into the Forward Improvement Plan (FIP), which will then be discussed at the Network Resilience Team contingency planning forum.

1.13 Plan Holders

Plan holders are the relevant persons who may be involved in some part of the incident management process or may be affected by the incident. Plan holders' name and contact details are given in **Appendix A** of this Plan.

1.14 Statement of Robustness

This Plan complies with the following robustness criteria:

- The Plan has been reviewed by the HA's NW Service Delivery Manager
- The Plan demonstrates an understanding of the roles and capabilities of the Emergency Services, the Local Highway Authorities, HA Service Delivery Team, TOS (RCC) and the Service Provider interfaces with them.

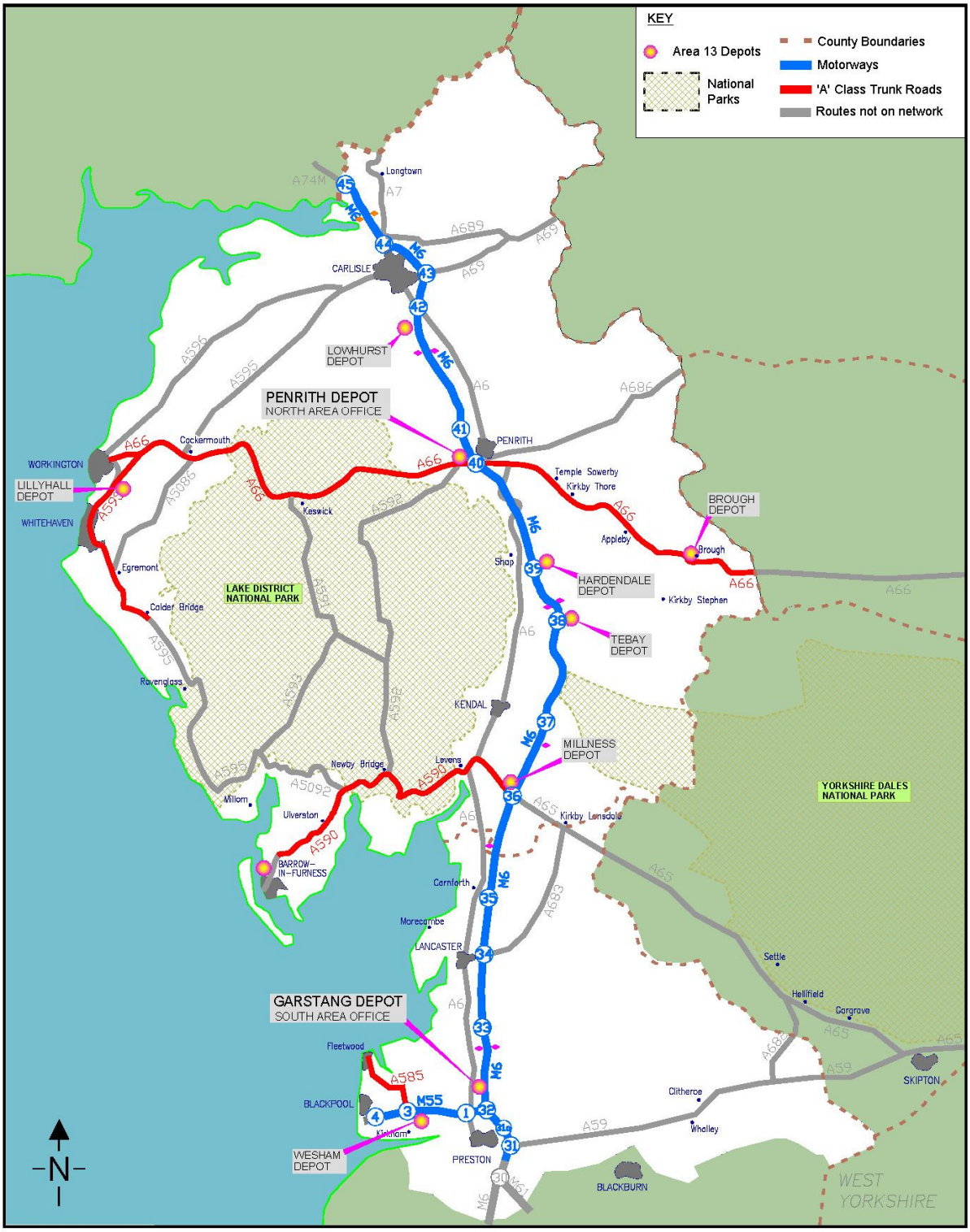
- Contact has been made with each Local Authority, Emergency Service and Stakeholder listed in the Box of Reference.

- The Plan has been tested through a progressive exercise programme and all staff involved in the implementation of the Plan have been trained and briefed about their specific roles.

1.15 Incident Definitions

The HA have established definitions of Major and Critical incidents. These are in **Appendices C** and **D** of this Plan.

Figure 1.2: Service Provider Area Map



1.16 Network Area Description

Area 13 is one of 13 Highways Agency areas in England. It covers Cumbria and North Lancashire.

The Area 13 Network covers sections of the following All Purpose Trunk Roads (APTR's) and Motorways:

M6 from boundary with Area 10 (Higher Walton Viaduct) to Jct 45
A74 (M) from M6 Jct 45 to Scottish Border (Sark Bridge)
M55 from M6 Jct 32 to M55 Jct 4 (A583)
A590 from Barrow in Furness to M6 Jct 36
A66 from A596 Workington to boundary with Area 14 (Cumbria/Durham border)
A595 from A66 Jct Chapel Brow to Calder Bridge
A585 from M55 Jct 3 to Albert St, Fleetwood (non-core)

Also the following partial routes:
Roundabout on A7 (M6 Jct 44)
Roundabout on A69 (M6 Jct 43)

The total network length listed in the documents is approx. 414 route km.

1.16.1 Incident Response Performance Measures

Incident response performance measures and performance level requirements are in accordance with Table 3.1 of Part 3: incident Response Operational requirement of the Asset Maintenance and Operational Requirements (see below).

Incident Response Performance Measures and Performance Level Requirements

Road type*0	Emergency Services present	Time of day	Road Traffic levels	Performance Metric 1 From Provider Incident identification / notification from TOS/Emergency Services through to production of Provider Tactical Incident Response Plan*1 100% compliance	Performance Metric 2 Monthly mean: For all Provider attended HA*8 led Incidents from Lane Closure*2 through to Lane Opening*3 100% compliance	Performance Metric 3 Monthly mean: From Incident command handover from the Emergency Services to the HA, through to Lane Opening 100% compliance
Motorway*4	No	Day*5	Heavy*7	30 minutes	70 minutes	n/a
Motorway	No	Day	Light*7	45 minutes	90 minutes	n/a
Motorway	No	Night*6	All	60 minutes	120 minutes	n/a
Motorway	Yes	Day	Heavy	30 minutes	n/a	70 minutes
Motorway	Yes	Day	Light	45 minutes	n/a	90 minutes
Motorway	Yes	Night	All	60 minutes	n/a	120 minutes
APTR – dual	No	Day	Heavy	30 minutes	70 minutes	n/a

Road type*0	Emergency Services present	Time of day	Road Traffic levels	Performance Metric 1 From Provider Incident identification / notification from TOS/Emergency Services through to production of Provider Tactical Incident Response Plan*1 100% compliance	Performance Metric 2 Monthly mean: For all Provider attended HA*8 led Incidents from Lane Closure*2 through to Lane Opening*3 100% compliance	Performance Metric 3 Monthly mean: From Incident command handover from the Emergency Services to the HA, through to Lane Opening 100% compliance
APTR – dual	No	Day	Light	45 minutes	90 minutes	n/a
APTR – dual	No	Night	All	60 minutes	120 minutes	n/a
APTR – single	No	Day	Heavy	30 minutes	50 minutes	n/a
APTR – single	No	Day	Light	45 minutes	70 minutes	n/a
APTR – single	No	Night	All	60 minutes	100 minutes	n/a
APTR – dual	Yes	Day	Heavy	30 minutes	n/a	70 minutes
APTR – dual	Yes	Day	Light	45 minutes	n/a	90 minutes
APTR – dual	Yes	Night	All	60 minutes	n/a	120 minutes
APTR – single	Yes	Day	Heavy	30 minutes	n/a	50 minutes
APTR – single	Yes	Day	Light	45 minutes	n/a	70 minutes
APTR – single	Yes	Night	All	60 minutes	n/a	100 minutes

Note: The M6 from the boundary with Area 10 (Higher Walton Viaduct) to Junction 32 is classified as “Heavy” road traffic levels during the day (04:00 to 20:00). All other routes including the APTRs are classified as “Light” road traffic levels during the day (04:00 to 20:00).

All Area 13 routes are classified as “Light” road traffic levels during the night (20:00 to 04:00).

2 Roles and Responsibilities

The following briefly explains the roles and responsibilities of the organisations who may be involved in an incident.

- Service Provider
- TOS (RCC) (See Appendix B for contact details)
- HA Service Delivery Team (See Appendix B for contact details)
- Police (See Contacts List in Box of Reference (4 of 4) – Reference Information Documents)
- Fire Service (See Contacts List in Box of Reference (4 of 4) – Reference Information Documents)
- Ambulance (See Contacts List in Box of Reference (4 of 4) – Reference Information Documents)
- Local Highway Authority (See Contacts List in Box of Reference (4 of 4) – Reference Information Documents)
- Environment Agency (See Contacts List in Box of Reference (4 of 4) – Reference Information Documents)

The roles of other parties (e.g. Police, are explained in further detail in the HA document named Standard Incident Management Framework (SIMF). A copy of the SIMF and SIMG is included in the Box of Reference.

2.1 The Service Provider

2.1.1 Role

The role of the Service Provider is to respond to incidents at an Operational (Bronze), Tactical Management (Silver) and Strategic Command (Gold) levels when required on a 24/7 basis.

2.1.2 Responsibility

The responsibilities of the Service Provider are as follows:

- Provide and use the necessary operational expertise
- Escalate incident management to a Tactical (Silver) level when required
- Keep other parties informed of the situation
- Trigger escalation of incident management to Strategic (Gold) level when required
- Manage Service Provider operations and ensure that the right resources are provided
- Direct operational vehicles to incidents

- Provide a 24/7 response service to the RCC
- Provide other on-road support requested by the Emergency Services or the Traffic Officers

2.2 HA Traffic Officer Service Regional Control Centre (RCC)

2.2.1 Role

The TOS (RCC) are the centres for all communications regarding incidents on the HA's strategic road network including roads that are not patrolled by the Traffic Officer Service. They manage Traffic Officer Involvement in incidents, liaise with the Emergency Services and Service Providers, and manage the HA's response to the incident at operational, tactical and strategic levels.

2.2.2 Responsibility

Specific responsibilities of the TOS (RCC) include:

- Managing Traffic Officer involvement in incidents
- Co-ordinating the responses of emergency services and other service providers
- Monitoring and managing traffic on the strategic network

2.3 Highways Agency Area Team

2.3.1 Role

The HA Area Team's role in the Contingency Plan is to safeguard the Agency's interests at an Area level. This may involve providing specialist advice to the TOS, Service Provider and other agencies involved in the incident. This may require the HA advising the Police on certain aspects regarding the network or any other Emergency Services involved in the Incident.

2.3.2 Responsibility

- Authorise temporary variations in the Service Provider's contract to facilitate their response to the incident
- Give specialist advice to the TOS (RCC) if requested.

2.4 Police

2.4.1 Role

The role of the Police is to assume overall command at all injury, critical and major incidents to coordinate the response and actions of others in attendance plus those summoned to provide additional support.

2.4.2 Responsibility

- To provide operational, tactical and strategic levels of scene/incident management.
- Process and record all casualty information the identification/removal of those fatally injured.
- Preserve the scene, safeguard property, gather/collate and secure evidence to support any judicial proceedings/hearings.

2.5 Fire Service

2.5.1 Role

The role of the fire service is to attend incident scenes and provide specialist operational assistance in support of other emergency services.

2.5.2 Responsibility

- Rescue people trapped by fire or in wreckage.
- Deal with any released chemicals or other contaminants liaising with specialist database providers.
- Prevent any further escalation by extinguishing fires and undertaking any preventative measures to contain the incident.
- Ensure Health and safety of all those involved at the scene.
- To provide an operational level of management.

2.6 Ambulance Service

2.6.1 Role

The role of the ambulance service is to attend the incident and provide a first line medical response to those in need of treatment.

2.6.2 Responsibility

- To coordinate the response of the NHS resources as required.
- Triage the walking wounded.
- Work with the fire service and determine the priority for persons trapped in wreckage.
- Administer emergency treatment.
- Determine to which hospitals the injured are taken.

- Work with the Air Ambulance regarding the evacuation of those with critical injuries.
- To provide an operational level of incident management.

2.7 Local Highway Authority

2.7.1 Role

The role of a Local Highway Authority via the Emergency Planning officer is to provide a measured level of assistance relative to an incident and coordinate any help and resources provided by outside non-emergency groups or bodies.

2.7.2 Responsibility

- To support the emergency services with aspects of traffic management and resource provision relative to their network.
- Provide any additional signing as agreed on designated diversion routes to facilitate their operational use.
- Provide emergency rest/welfare centres for those in need and/or if possible assist with on site provisions where evacuation is not possible or practical when the HA ECW facility is not available.
- Provide emergency transport between the incident and rest centres.
- Work with the police and the HA providing practical help and an operational response.

2.8 Environment Agency

2.8.1 Role

The role of the Environment Agency is wide ranging being both proactive and reactive to situations relative to the management of flooding and dealing with contaminants/emissions that are harmful to land, water or air being detrimental to public well being and wildlife.

2.8.2 Responsibility

- To advise the emergency services and others at incident scenes on the impact a substance may have on the environment and of any preventative measures necessary to remove or minimise the risk or harm to the environment or the general public.
- Provide early notification of potential watercourses or Pluvial flood warnings and predictions of intensity, peak levels and relevant duration times.
- Manage flood defences and appropriate control measures.
- In relation to the HA network ensure that the SP manages and works to prevent any spillage of pollutants entering and contaminating adjacent watercourses, the land or affecting air quality.

- Taking legal action against those who don't take their environmental responsibilities seriously.

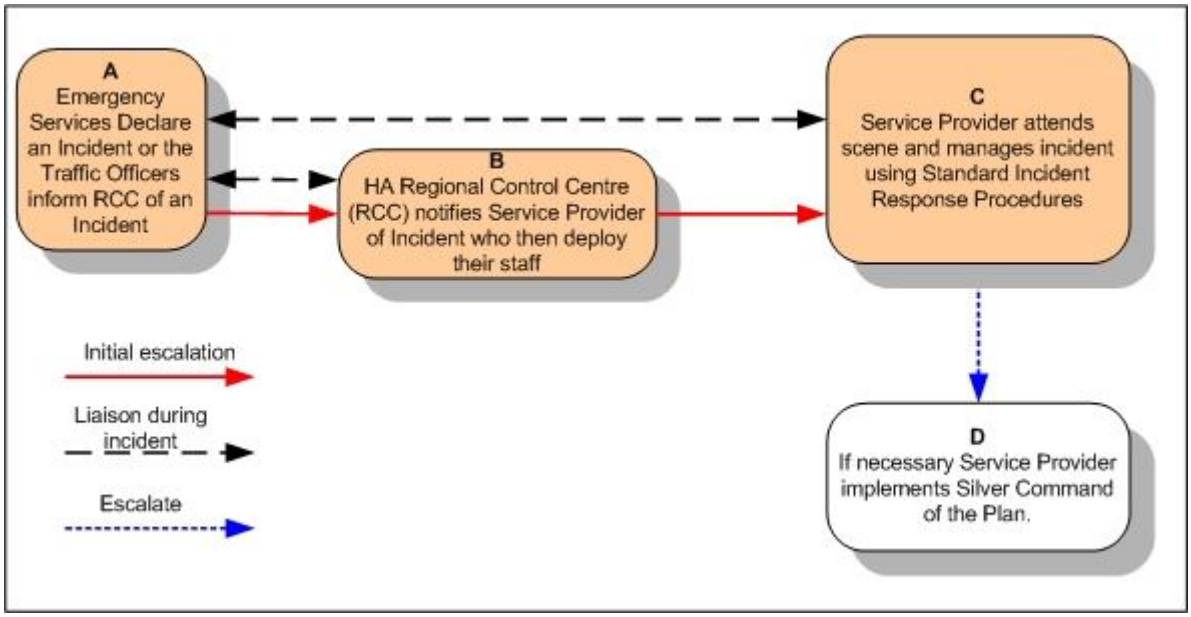
3 Service Provider's Standard Incident Management (Bronze)

3.1 Introduction

Most incidents that occur on the Highway Agency's Strategic Network can be dealt with under the Service Provider's established Standard Incident Management Procedures.

These responses precede the implementation of the Contingency Plan as such. The Contingency Plan will be implemented when the Service Provider's Standard Incident Response Procedures are unable to contain an incident or its effects, to the extent that the Incident Objectives set out in **Section 1.7** are threatened.

Figure 3.1: Service Provider's Standard Incident Response Procedures



3.2 Box A

The RCC is informed of an incident on the Strategic Road Network by the Emergency Services, the on road Traffic Officer Service or alternative source such as the Service Provider, Emergency Phones etc

3.3 Box B

The RCC contacts the Service Provider and informs them that there is an incident on the network and assistance is required.

3.4 Box C

The Service Provider's 24/7 Control Room completes a Tactical Incident Response Plan (TIRP) and arranges for the deployment of the necessary resources to the scene of the incident and makes the necessary response (e.g. temporary signing, repairs to the infrastructure, etc). The Service Provider liaises with the Traffic Officer and assesses whether the incident can be managed under Standard Incident Management Procedures and whether any of the incident objectives are threatened.

3.5 Box D

If any of the Incident Objectives are threatened, the Service Provider will escalate the incident management.

4 Service Provider Tactical Command (Silver Command)

4.1 Introduction

Mobilisation of the Media Management Team (MMT) is a function which may be carried out by a team or an individual and may be needed where incident objectives are threatened but the operational response is straightforward and does not require tactical management. In these circumstances the MMT will closely monitor how the incident is developing and this will enable an informed decision to be made about the need for further escalation.

4.2 The MMT will attend the Tactical Management Room (TMR) and carry out the following duties:

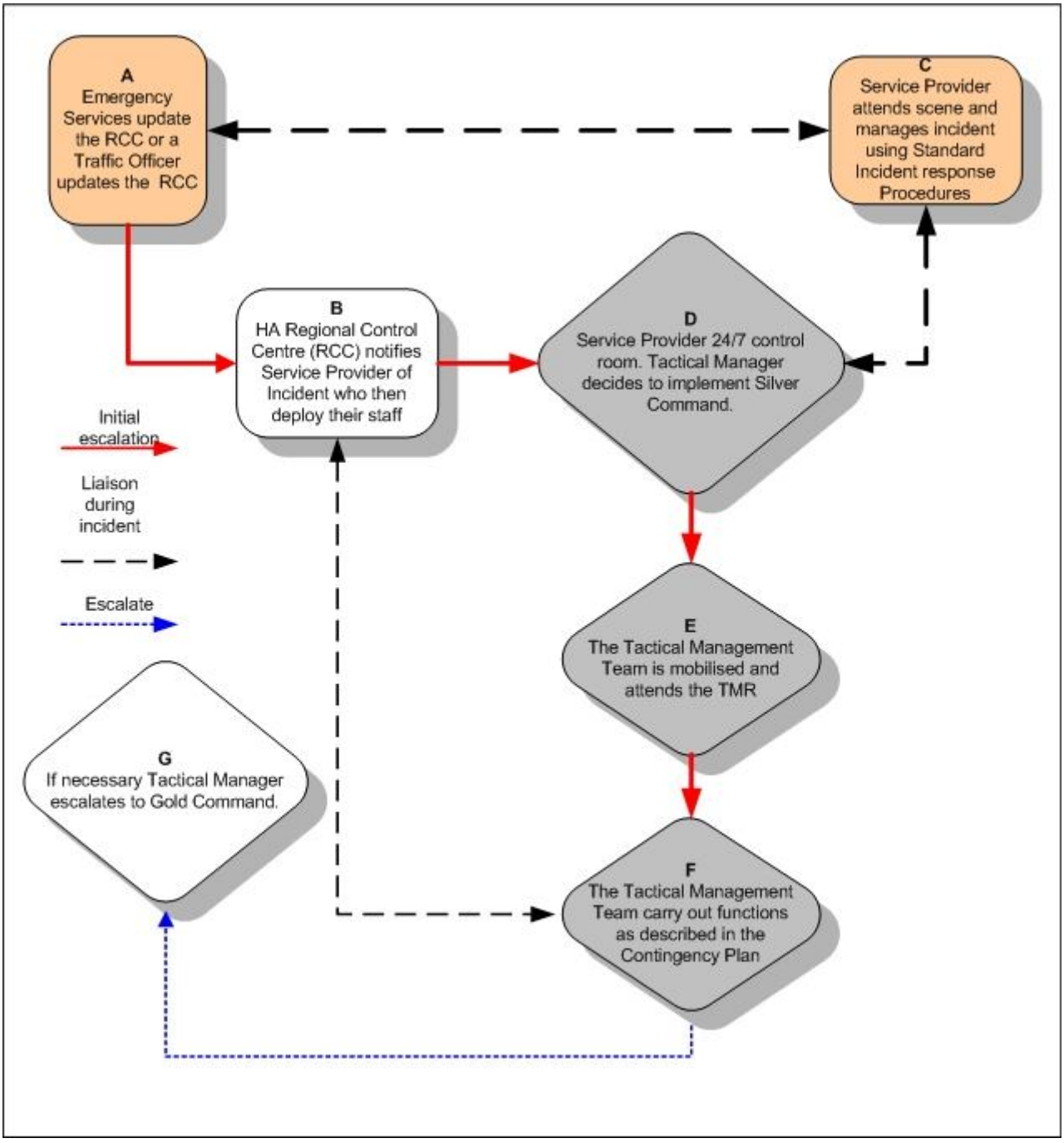
- Liaise with the Service Provider staff on site
- Inform Major Stakeholders affected by the incident
- Inform Senior Management and regularly update
- Keep the RCC informed
- Monitor media broadcasts concerning the incident (TV, websites, radio)
- If a media message is incorrect, inform the RCC

If the MMT deem the incident to be escalating then they will inform the Tactical Manager who will then mobilise the full Tactical Management Team.

Full mobilisation of the Service Provider's Tactical Management Team (TMT) in the Tactical Management Room (TMR) allows the Service Provider to provide tactical management of the situation remote from the incident(s) itself.

Figure 4.1 shows how Silver Command is mobilised, key actions, and lines of liaison during. The key actions are explained in the succeeding sections.

Figure 4.1 : Full Mobilisation of the Plan (Silver Command)



4.3 Escalation to Silver Command

Escalation from Bronze to Silver is described in **Section 3**. This Section describes key actions in boxes E through to F.

4.4 Box E

The Tactical Manager mobilises the full TMT in the TMR. This team consists of personnel who have the experience and knowledge to tactically manage an incident on the network.

Their role is to give tactical advice to the teams on the ground and also to look at the whole network to assess the wider effects of the incident. In liaison with the Service Provider staff on site they make decisions on operational matters to minimise the impact of the incident.

The TMT will be mobilised following an instruction from the Tactical Manager (Silver Command).

The TMT will involve employees from across the business that can make a positive contribution in delivering the incident objectives. Team members will either have expert geographical knowledge or will be specialist professionals. Some of the key TMT members are detailed in B.5.

In addition the TMT will comprise a number of sub-teams:

- Media Management Team (MMT)
- Administration Team
- Senior Management Team

The TMT will be mobilised via telephone by the NCC and asked to attend the TMR.

4.5 Box F Silver Command

4.5.1 Tactical Management Team and Tactical Management Room

Tactical Management of an incident by the Service Provider is core to the successful implementation of the Plan. Further explanation of the TMT and TMR are given below.

4.5.2 TMT Key Functions

The key functions of the TMT are to:

- Relieve the Service Provider's 24/7 Control Centre of the burden of having to deal with a Major Incident while continuing to fulfil all its other functions
- Insert a tactical planning capability into incident response, to take full account of network wide events, events in neighbouring Areas, and incoming HA and Government advice or instructions and requests for information
- Be a forum within which tactical decisions can be made, in conjunction with the Emergency Services, Local Authorities, TOS (RCC), HA Area teams and Government as necessary
- Enable complex situations to be managed in such a way that the Incident Objectives are achieved, when they might otherwise be threatened
- Be proactive in safeguarding the comfort and wellbeing of drivers trapped in stationary vehicles on the network, including liaising with the Police/TOS (RCC) over procurement of Local Authority support services

- Be a centre for “enhanced” communications with HA and network stakeholders, (i.e. above the level of communication required in established Incident Management Procedures and suited to a serious situation which may be of significant media interest or political concern)

- Liaise with TOS (RCC)

- Formulate a recovery plan, close the incident down, and pass control of the site back to the Service Provider’s 24/7 Control Room

- Send a representative to Police/HA Silver Command if requested to act as a Tactical Adviser

4.5.3 TMT Key Characteristics

The TMT will be **aware, in control, proactive and tactical**.

Key characteristics of the team will be:

- Up-to-date knowledge of the state of the whole network and incident, at all times
- Proactive management of the situation, to achieve the Incident Objectives
- Proactive communication of information, to those who need to know
- Tactical thinking and tactical decision making, but tactics which are capable of timely implementation within available resources
- Proactive outreach to other organisations when their assistance is required

4.5.4 TMT Structure

The Tactical Management Team comprises a number of sub-teams:

- Tactical Decision Team

- Media Management Team (MMT)

- Administration Team

- Senior Management Team

Members of staff available to form each team are listed in Appendix B, together with their contact details. In addition, Appendix B lists other persons who may be called upon by the TMT (e.g. technical specialists).

The minimum number of staff from each team that will be included in the TMT will depend on the nature and scale of the incident. However, for all HA Critical and Major Incidents at least one member of each team will be either involved or made aware of the incident.

The functions of each team are explained below.

4.5.5 Tactical Decision Team

This team is formed of staff that are responsible for the day-to-day running of the network. They have sound experience and knowledge of the network and current Standard Incident Response procedures. All members of the team are qualified to approve escalation to Silver Command, and then to act as the Tactical Manager in the TMR.

4.5.6 Media Management Team

The functions of the Media Management Team (MMT) are set out in 4.2 of this section. In a full mobilisation, they will be assisted by Admin staff with communicating with the HA and local authorities on operational matters as required. The Media Management Team will be composed of individuals qualified to undertake these functions.

4.5.7 Administration Team

The Administration Team will:

- Ensure that communications, decisions and actions by all staff are recorded
- Use the HA website to view VMS settings on the network
- Monitor traffic congestion from websites and other sources
- Keep incident overview board up to date
- Advise the Tactical Decision Team members of other events on the network (e.g. road works)
- Provide admin support to all other members of the TMT including attending to the smooth running of IT and other facilities in the TMR

4.5.8 Senior Management Team

A nominated Senior Manager will be kept informed of the situation at all times so that they will be in a position to respond to queries from Board level within the HA or from Central Government. They may choose to be located within the TMR, or they may arrange to remain in contact elsewhere.

If the Tactical Management Team is required to give advice or authorisation for Service Provider activities that are out of their jurisdiction, then they would escalate the incident to Gold Command. This would require the Senior Management being briefed to take appropriate action.

4.5.9 Organisation

The TMT will be led by a Tactical Manger (Silver Command).

It may be necessary for the Tactical Manager to deploy another member of the Tactical Decision Team to an alternative location such as Multi Agency Silver Command, NW RCC or to act as support to the HA at a Multi Agency Strategic Coordinating Group.

The Tactical Manager will be responsible for ensuring that both the HA and members of the Senior Management Team are kept updated via telephone if not present in the TMR.

Rotas exist for Gold, Silver and Structures Engineer. The rotas are contained in the box of reference – reference information document. Contact details for all rotas are also available via the NCC Incident Management Tool. The Rotas run from mid day on Friday to mid day on Friday. The NCC contacts members of staff on a Friday morning to remind them that they are on duty.

Other Team members who are not on a rota system have been briefed into this Plan and will either attend the TMR when required to do so or will provide the Tactical Manager with advice and support remotely.

4.5.10 Tactical Management Room (TMR)

The TMT will operate in the Tactical Management Room. This room contains the equipment and resources needed to support the TMT.

4.5.11 Location

The TMR is located within the Network Delivery Office at EM Highway Services Ltd's Penrith office.

4.5.12 Facilities

The TMR offers the following facilities:

- Computers
- Phone lines
- White boards
- Contingency Plan & Box of Reference (hard copy)
- Digital radio
- Video conferencing

4.5.13 Setup

The TMR is a turn key facility that is permanently set up. Any meetings scheduled to take place in the meeting room during the operation of the TMR will be relocated to suit.

In addition to the TMR there are a number of small offices on the ground floor together with the Helvelyn Meeting Room located within the Penrith Depot supervisor's office building. All rooms have telephony and network connection points.

If required the TMR and other facilities at Agricultural Hall will be available for use by other agencies at part of a Multi Agency response.

4.5.14 Interface with other Tactical Teams

There may be occasions where a Severe Weather Desk is in operation / when the decision is made to mobilise the TMT (or vice versa). The Severe Weather Desk will operate as a tactical team within the TMT and report to Silver Command.

Resources such as the Media Team and Administration Team will support both the Severe Weather Desk and Silver as appropriate.

4.6 Box G

The Tactical Manager will continually monitor the situation and if necessary, will escalate the response to Gold Command.

The Tactical Manager will escalate to Gold Command if the incident objectives are threatened.

Factors that would influence this decision may include / but not be limited to:

- Death or serious injury to Service Provider employee
- Threats to Service Provider business continuity / loss of facilities and/or resources
- Assistance required from Parent Companies
- Assistance required from other adjacent Service Providers
- Decision needed to commit considerable financial or / other resource

The Tactical Manager is authorised to approve the escalation and will contact Gold Command via telephone to handover responsibility.

The Tactical Manager will continue to lead the TMT and will report directly to Gold Command.

4.7 Emergency Service Interfaces

Generally, communication between the Service Provider and the Emergency Services at the scene of an incident will be relayed back to the Service Providers NCC unless the Service Provider has relocated this resource within the RCC. Otherwise all communications should go through the relevant RCC.

Blank page for repagination

5 Service Provider Gold Command

5.1 Introduction

The Service Provider will escalate the response to the Gold Command if the incident objectives are still threatened and the situation cannot be managed at a Tactical level of Command. For example, an incident might require:

- The need to re-allocate resources within the Service Provider's own organisation beyond the powers of the TMT
- The need to request mutual aid from adjacent Areas

Strategic decisions and command of the incident are passed to the Service Provider's Senior Management Team. The Senior Management Team will then make the strategic decisions concerning the incident whilst keeping the TMT and the TOS (RCC) informed of the situation.

5.1.1 Service Provider Gold Command

If following a full implementation of the TMR, the TMT is unable to manage the incident with its current resource level, the TMT will liaise with the Service Provider Senior Management Team and request that Gold Command is set up to provide additional powers such as:

- Transfer of resources (personnel and equipment) from other Service Provider's activities to deal with the incident
- Release of office or depot space needed to deal with the incident
- Authorisation of the TMT to take actions or decisions above their normal level of authority
- Authorisation of expenditure at a level above the authority of the TMT

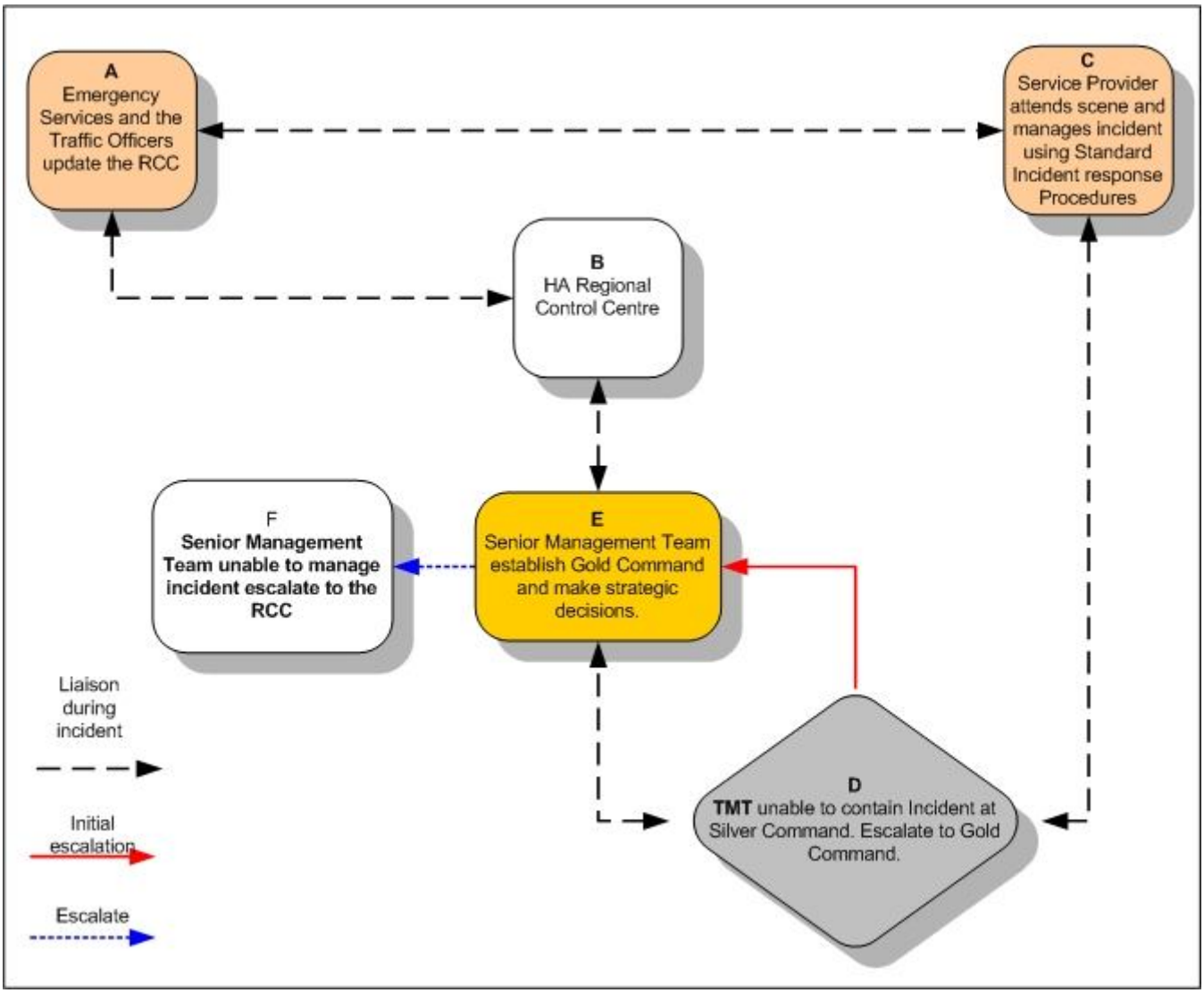
The Service Provider Senior Management Team may also set up Gold Command following liaison with the TMT if:

- Reputation is at risk
- There is public interest at a regional or national level
- Legal action may ensue

It is important to note that management of the incident itself shall remain with the TMT, but all strategic decisions concerning the Service Provider will be made by the Senior Management Team and all communications relayed through the TMR to the TOS (RCC).

Figure 5.1 shows how Gold Command is mobilised, key actions, and lines of liaison. The key actions are explained in the following sections.

Figure 5.1: Service Provider Gold Command



5.2 Service Provider Gold Command

5.2.1 Box E

Gold Command is formed up of representatives from the Service Provider Senior Management Team and will make strategic decisions to minimise the impact of the incident.

Tactical Command of the incident will remain with the TMT. Actions or decisions taken by Gold Command will be in support of that tactical management, and will be agreed between Gold Command and the TMT.

Gold Command will be established at a location to be determined by the Senior Management involved. It may be established by:

- Telephone or e-mail communication from the locations where Senior Management are already positioned

- Senior Management co-locating at a convenient location, which could be the TMR but not necessarily so

Once established, Gold Command will remain established as long as incident objectives remain threatened. Once the situation is under control, the TMT will inform Senior Management that the incident can be managed at tactical level.

5.2.2 Box F

Senior Management Team in conjunction with the Tactical Management Team is unable to contain the impact of the incident and therefore decide to escalate command of the incident to the TOS (RCC).

The Service Provider will maintain Tactical command of the incident but Strategic decisions will now be taken by the TOS (RCC).

Blank page for repagination

6 Key Stages of Plan

6.1 Introduction

Implementation of the Contingency Plan comprises a number of levels of Command (Bronze, Silver and Gold). The process of escalating and de-escalating between these levels is key to the successful management of incidents and ensuring that the incident objectives are met.

This section describes the two different ways in which the Plan can be implemented:

- Bottom Up Plan implementation is triggered by events within the Service Provider's area of responsibility.

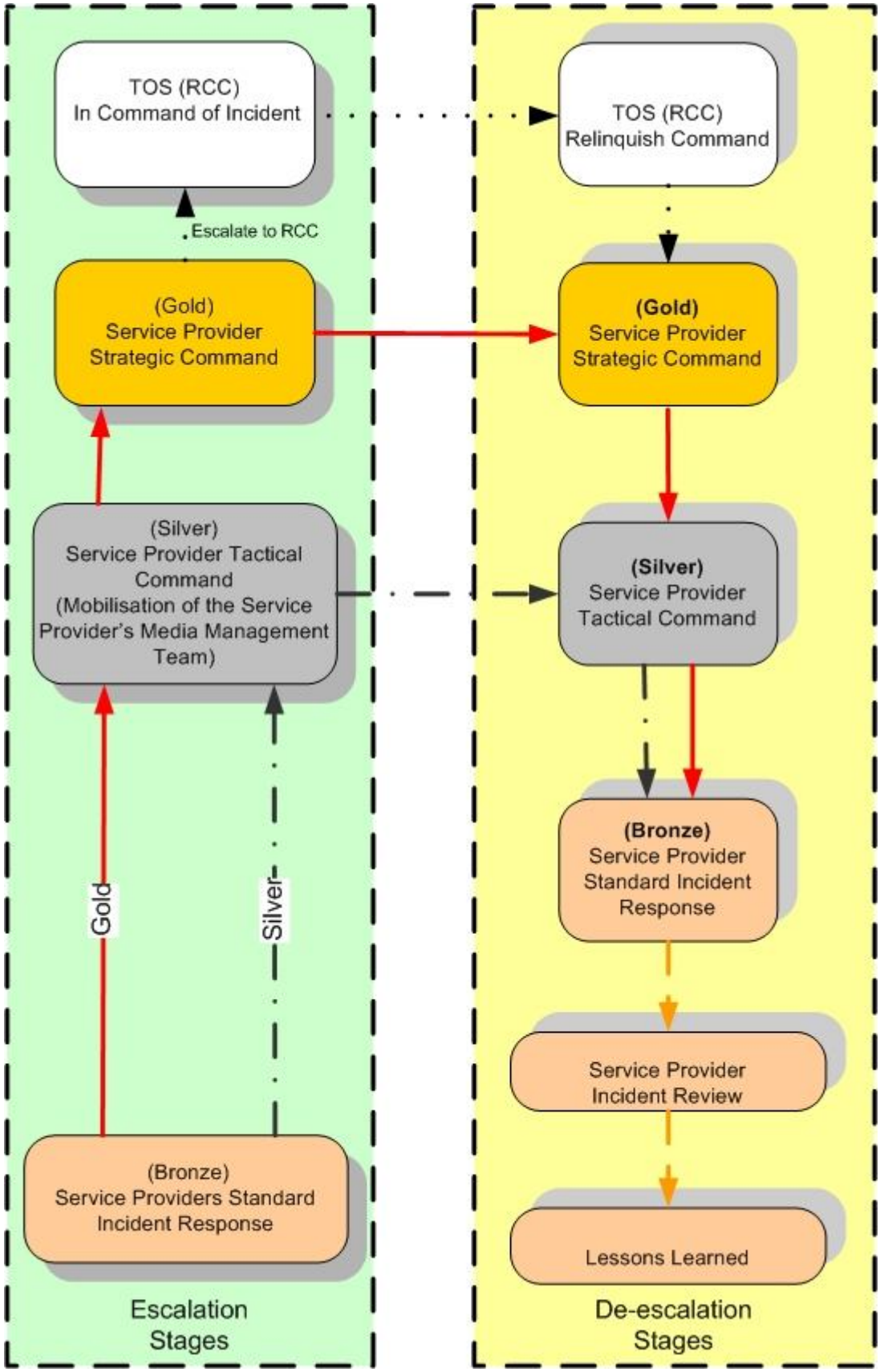
- Top Down Plan implementation is triggered by external events imposed on the Service Provider from the HA regionally or nationally.

6.2 "Bottom-Up" Plan Implementation

Figure 6.1 shows the key levels of Contingency Plan implementation.

There are 3 escalation levels and 3 de-escalation levels, although some levels appear in both procedures. The decision to escalate or de-escalate (at each level) depends on whether the incident objectives (**Section 1.7**) are being threatened.

Figure 6.1: High Level diagram showing the different levels of mobilisation and de-escalation



6.3 "Bottom-Up" Plan Escalation and De-escalation

The levels of Plan implementation below refer to "Bottom-Up" Plan escalation triggered by events within the Service Provider's Area. Depending on the level of escalation needed or how the escalation is triggered, there are four alternative sequences to implementing the Contingency Plan. In each case, the corresponding de-escalation levels are also included.

Service Provider Tactical Control (TMT) Silver Command

This shows the incident escalating to Service Provider Tactical Control as the situation deteriorates further. The Service Providers Media Management Team (MMT) will be mobilised and can alert others of the need to mobilise and keep the HA and other relevant stakeholders up to date with enhanced information from the incident scene.

Service Provider Gold Command

The sequence shows escalation to the Service Provider Gold Command. When the Service Provider decides that Strategic Command of the incident is no longer required, the Service Provider returns to Silver Command.

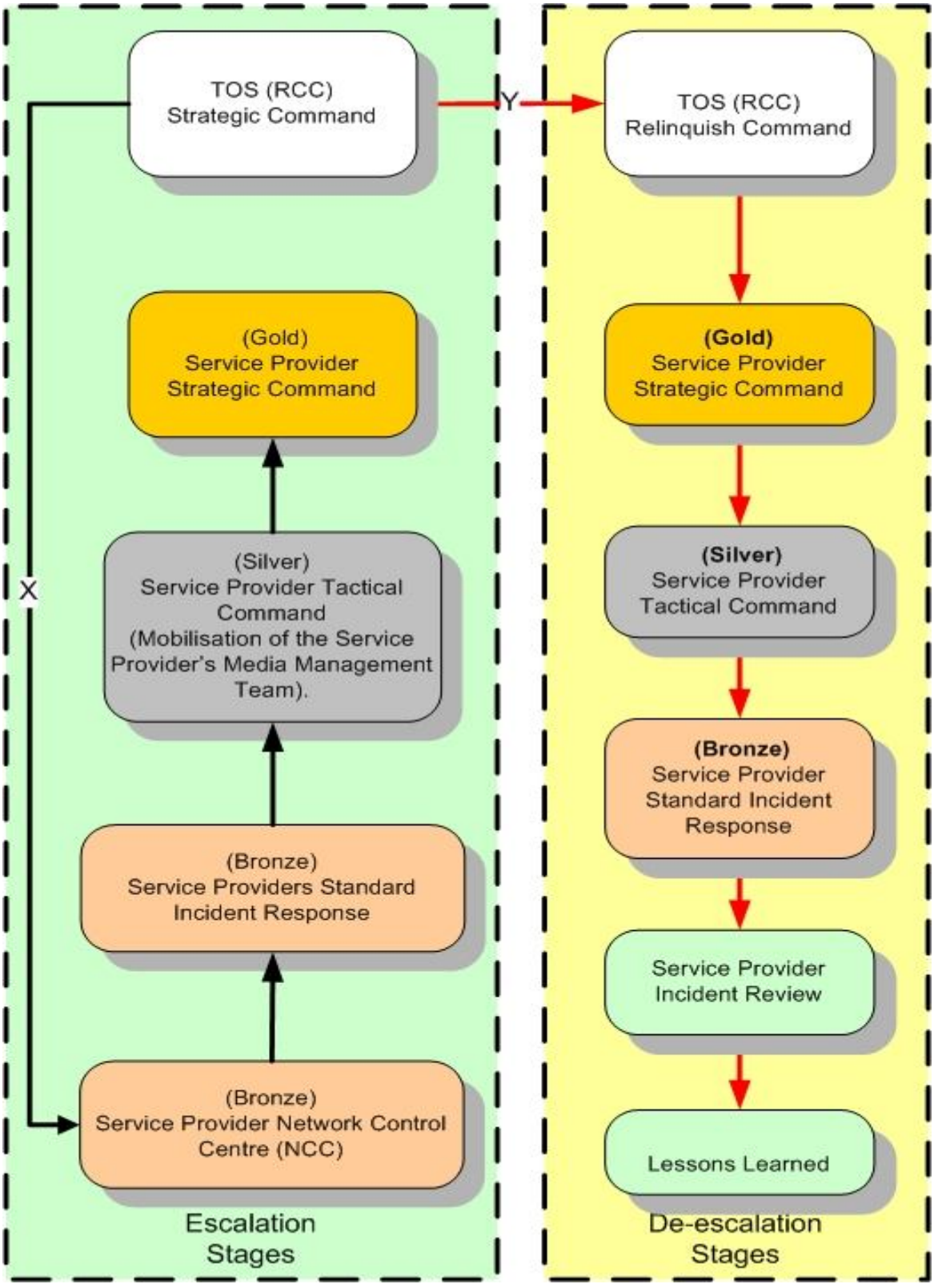
Highways Agency TOS (RCC) Strategic Command

This sequence shows escalation up to the HA RCC Command. When the HA RCC Team relinquishes Command of the incident, the Service Provider regains Strategic Command.

6.4 "Top-Down" Plan Implementation by TOS (RCC)

The stages of Plan implementation below refer to "Top-Down" Plan escalation triggered by events outside of the Service Provider's control. Depending on the level of escalation needed or how the escalation is triggered, there are two sequences to implementing the Contingency Plan. In each case, the corresponding de-escalation stages are also included.

Figure 6.2: Top down Implementation by the TOS (RCC)



Implementation of the Service Provider's Contingency Plan may be triggered or instructed by HA, in response to events outside the Service Provider's Area.

6.4.1 Escalation: Sequence X: TOS (RCC) Silver

This sequence shows how the TOS (RCC) implements the Area Contingency Plan and instructs the Service Provider to set up Gold Command. Contact with the Service providers will be made through the normal communication channels i.e. through the Service providers NCC. The incident will then be dealt with using their Standard Operating Procedures and the appropriate level of response will be made.

Should the TOS (RCC) instruct the Service Provider to set up Gold Command the NCC will contact the Gold Commander using the Gold Commander Rota. The Gold Commander may well instruct the Silver Commander to mobilise the TMT.

6.4.2 De-escalation: Sequence Y: TOS (RCC) stands down Gold

As the threat from the incident recedes, command is successively passed back down from the TOS (RCC), Service Provider Gold and Silver Commands and finally to Service Provider Bronze Command.

Blank page for repagination

7 Traffic Officer Service (TOS) Management of the Incident

7.1 Introduction

The Highways Agency TOS (RCC) will already be aware of an incident on the strategic network through liaison with the Service Provider (s) via the Regional Control Centre (RCC) and will know that the situation is either in control or is reaching a point where TOS Strategic Management is required to mitigate any further impacts on to the strategic network.

7.2 Implementation of the TOS (RCC) Command of the Incident

7.2.1 Bottom up escalation

A bottom up incident (Service Provider managing the incident through the command sequence Bronze, Silver, Gold), the decision to escalate the incident to TOS (RCC) command is up to the Service Provider. The reason for escalation will be that the impact of the incident cannot be mitigated within the Service Provider's existing contract or resources.

7.2.2 TOS (RCC) Management of the Incident

The TOS (RCC) will manage the incident using the following HA documents:

- Standard Incident Management Guidance (SIMG)
- Standard Incident Management Framework (SIMF)
- Regional Emergency Plans

By following the guidance in the above documents they will take Strategic command of the incident and assist the Service Provider with reducing the impact of the incident by carrying out the following:

- Co-ordinate an approach towards resolution
- Disseminate information to all stakeholders
- Contact the Highways Agency Area Performance Manager
- Make strategic decisions for the regional strategic road network

7.2.3 Top Down Implementation of the Service Provider Contingency Plan

A top down implementation of the Service Provider Contingency Plan could take place if the Highways Agency deems an incident or an event to be severe enough to have a major impact on the strategic road network.

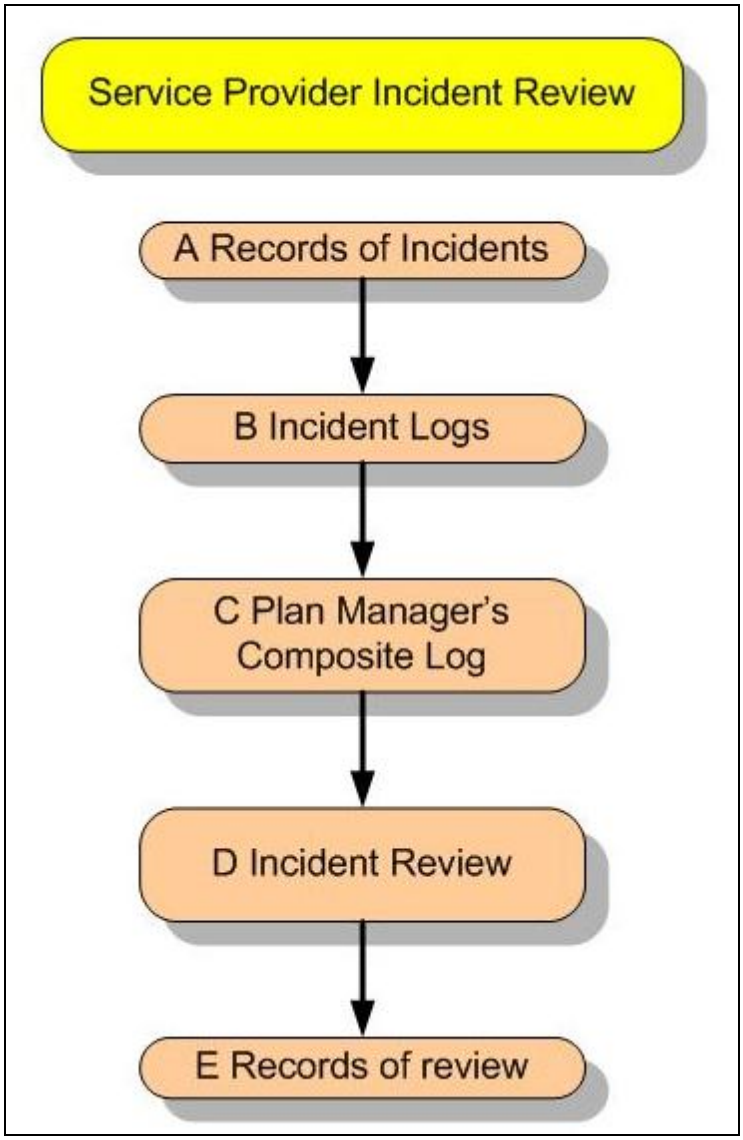
The TOS via the RCC would contact the Service Provider via their NCC and inform them that their services are required. It is then up to the Service provider to determine what level of the plan that they escalate to so that they can provide the assistance that the RCC require.

8 Service Provider Incident Review

8.1 Introduction (HA Review)

The Plan's content needs to be reviewed after an incident requiring any stages of the Plan (above Bronze Command) to be mobilised. The Service Provider's incident review should be in line the HA AMM 70/06 which offers guidance on Post Incident Cold Debrief Process and the internal and external distribution of learning points and good practice.

Figure 8.1: Walk through agenda that the Service Provider should use as a guide



8.2 Box A – Records of Incidents

When a partial or full implementation of the Contingency Plan has occurred, records must be kept of:

- Communications
- Actions
- Decisions

Throughout the incident, records must be kept as described in this section of the Plan. These should be recorded in the manner most convenient for each person involved (e.g. on purpose-prepared forms, in a diary or notebook, on a Dictaphone or on a computer, etc).

8.2.1 Records of Communications

All communications involving the relay of information and decisions made must be recorded. Records of Communication must be made by both parties involved and must include:

- Date and time
- Person initiating communication
- Person receiving communication
- Summary of information passed (including location of the incident)
- Summary of response (if any)
- Next actions (if any) as a result of the communication
- Who will take these actions (if any)

If decision making is involved, the following additional information must be recorded:

- Decision to be made
- Options considered
- Decision made
- Reasons for decision made

Please note that it is vital to record decision making processes to permit a full review of the handling of the incident afterwards.

8.2.2 Records of Actions

Records of key actions must be kept to include:

- Location of incident
- Name of person taking action
- Date and time
- Action taken
- Outcomes

8.2.3 Records of Decisions

Unless recorded within a Record of Communication, all key decisions must be recorded to include:

- Location of incident
- Name of person(s) making decision
- Date and Time
- Nature of decision to be made
- Options considered
- Decision made
- Reasons for decision

8.3 Box B – Incident Logs

Incident logs are summaries of the Records above, and must be completed by:

For the purposes of the Service Provider Incident Review the following people or teams should prepare Incident Logs.

- NCC complete TIRP on Causeway
- Incident Record Sheet completed by team attending the incident
- Administration team to assist with:
- Decision Log
- Action Log
- Bronze, Silver and Gold Commanders should maintain there own records / logs.

Each log should contain the following information:

- Times and dates of specific communications, actions or decisions made
- Information relayed
- Actions taken
- Decisions made

8.4 Box C – Plan Manager's Composite Log

The Service Provider's Plan Manager will then combine all logs and:

- Seek clarification of inconsistencies between individual logs
- Seek any missing information
- Produce a composite log of the whole incident covering all actions

8.5 Box D – Internal Incident Review

The Service Provider will arrange an internal Incident Review adopting the following procedure:

The review should include:

- Actions taken and assessment of their appropriateness
- Actions not taken and assessment of whether they were not needed or whether they should have been taken
- Communication links that were implemented and assessment of whether they worked efficiently
- Communication links that were not established and assessment of whether they were not needed or whether they should have been made
- The timing of actions, including establishment of communications links
- Liaisons with third parties, particularly the emergency services, other Service Providers and Local Authorities
- Whether the right parties were involved in dealing with the incident
- The mobilisation of key staff
- Stakeholder communications, with particular regard to the parties contacted and the usefulness (to them) of the information received
- The usefulness and accuracy of information contained within the Plan and the need for any additional information (or less information).
- The overall structure and function of the Service Provider response (would an altogether different approach have been more effective?)

All persons involved in the incident must submit their logs to the Plan Manager within two working days of the incident. The Plan Manager is then to produce a composite log and an Incident Review within ten working days of the incident.

8.6 Box E – Records of Review

Where an internal review is undertaken, copies of the minutes of the meeting and other relevant papers will be provided to the HA NW Service Delivery Team.

It should be emphasised that the review has the sole aim of strengthening the Service Provider's response or confirming that existing response procedures are appropriate. It is not concerned with allocating blame to any individual or organisation.

Should legal proceedings be pending as a result of the incident, the circumstances under which the Incident Review takes place will be subject to a further review to ensure that individuals are not compromised in any way.

It should be noted that any notes taken or documents produced as a result of any review may become subject to relevant disclosure rules at subsequent legal hearings, whether criminal or otherwise. In particular if there is suspicion of any professional negligence being evident in such a review, advice should be sought.

9 Lessons Identified

9.1 Future Plans

Revisions of future Plans should incorporate points arising from the Incident review with the aim of ensuring a more effective response by the Service Provider when the next incident occurs.

If immediately after an incident it is the view of the Service Provider that significant improvements can be made to the HA or other operational procedures, then immediate feedback should be given to the HA NW Service Delivery Manager, so that they can share this with other HA Areas.

Information regarding any lessons identified should be included in the Service Providers Forward Improvement Plan (FIP) and forwarded to the Network Resilience Team for inclusion in the Service Provider National FIP.

9.2 Personal Incident Debriefing

If any member of the Staff from the Service Provider requires a personal incident debrief for stress or trauma reasons, then they should contact their line manager or confidential counselling services supplied by their employers.

EM offer all employees a confidential counselling service through the Bupa Employee Assistance scheme. This is a free call 24/7 hours a service in complete confidence.

Bupa Employee Assistance Contact Details

[redacted]

[redacted]

Blank page for repagination

10 Box of Reference

10.1 Introduction

The Box of Reference contains comprehensive information about the network for use during the Tactical and Strategic Management of incidents.

There are 5 files:

- Area 13 Emergency Diversion Routes
- Area 13 Service Provider Plans (1 of 4)
- Area 13 Stakeholder Plans (2 of 4)
- Area 13 Adjacent Area Plans (3 of 4)
- Area 13 Reference Information Document (4 of 4)

There are 2 Hard Copies:

- One stored in the Tactical Management Room
- One stored with the Service Provider Contingency Plan Manager

The Contingency Plan including the Box of Reference is available to all Service Provider employees on the S drive:

See link S:/Network Delivery/Incident Management/Contingency Plan

All Plan Holders detailed in Appendix A receive a DVD copy of the Contingency Plan which includes Box of Reference.

The box contains a list of contents and instructions as to when these have to be checked and updated. The Service Provider Contingency Plan Manager will check and update all contents on a regular basis in accordance with the instructions.

10.2 Information in Box

There are four types of documents stored in the box of reference:

- Emergency Diversion Route Document (EDRD)
- Major Stakeholder Emergency Plans
- Service Provider Operational Plans
- Reference Information Document (RID)

10.3 Suggested Contents of the RID

Below is an example of the contents identified in the RID. This information can be inserted within the document as text or can be referenced to another location within the Service Provider's office. This data may also be stored electronically and therefore file paths to their locations would be required within the RID.

- Schematic Diagrams and Key Location Features of the Network
- Emergency Crossover Points
- Vulnerable Nodes
- Emergency Access Points on Network
- Area Depot Locations
- Stakeholder Contact Details
- Sign Bin Inventory
- Location of CCTV Cameras
- Business Continuity Plan
- Network Lighting
- Location of Traffic Signals
- VMS Locations
- Major Works on or off Network
- External Events
- Police Boundaries and contact details
- Emergency Services contact details
- Traffic Officer Service Boundaries
- High Risk Weather Sites
- Hazardous Sites Adjacent to the Strategic Network
- Network Rail Bridges over the Strategic Network
- Contact details for Service Provider Welfare
- Plant and Equipment
- Specialist Contractors to assist the Service Provider
- Types of Communication Systems for liaison with all stakeholders
- Liaison with Adjacent Areas