HIGHWAYS AGENCY

Area 4

Network Contingency Plan

June 2013

Version 3.4

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

Highways Agency Area 4
Federated House
London Road
Dorking
Surrey RH4 1SZ
Tel: 0845 955 575
Fax: 01306 878 491

Page blank for pagination

Balfour Beatty Mott MacDonald

HIGHWAYS AGENCY

Area 4
Service Provider
Network Contingency Plan
Version 3.4

Issue and Revision Record

Rev	Date	Originator	Checker	Approver	Description
3.0					1st Issue of new document
3.1					Half yearly revision
3.2					Half yearly revision
3.3					Half yearly review
3.4					Half yearly review

Blank page for pagination

List of Contents

Executive Summary

This is the Contingency Plan for Area 4.

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 Area Performance Manager. All copies of the plan will be provided in electronic format only, on a CD also containing the Incident Response Plan, Resource Information Document, Emergency Diversion Route Document and the Hospital Guide.

The Plan is updated at 6-month intervals.

Sections of the plan in blue italic type are sections inserted into the framework document by the Service Provider. Those sections of the framework document that are not used remain, but are struck out, and an explanation appended to them.

Since the introduction of the AMOR contract version 1.7 to Area 4 this plan should be read in conjunction with the Area 4 Incident Response Plan, which is a requirement of the AMOR contract. Nothing in this document will clash with anything in the Incident Response Plan.

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 four components:

- This Contingency Plan setting out the escalated response of the Area 4
- Service Provider to a Major or Critical Incident and is supported by:
- Area 4 Incident Response Plan (required under AMOR)
- 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 standalone 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.

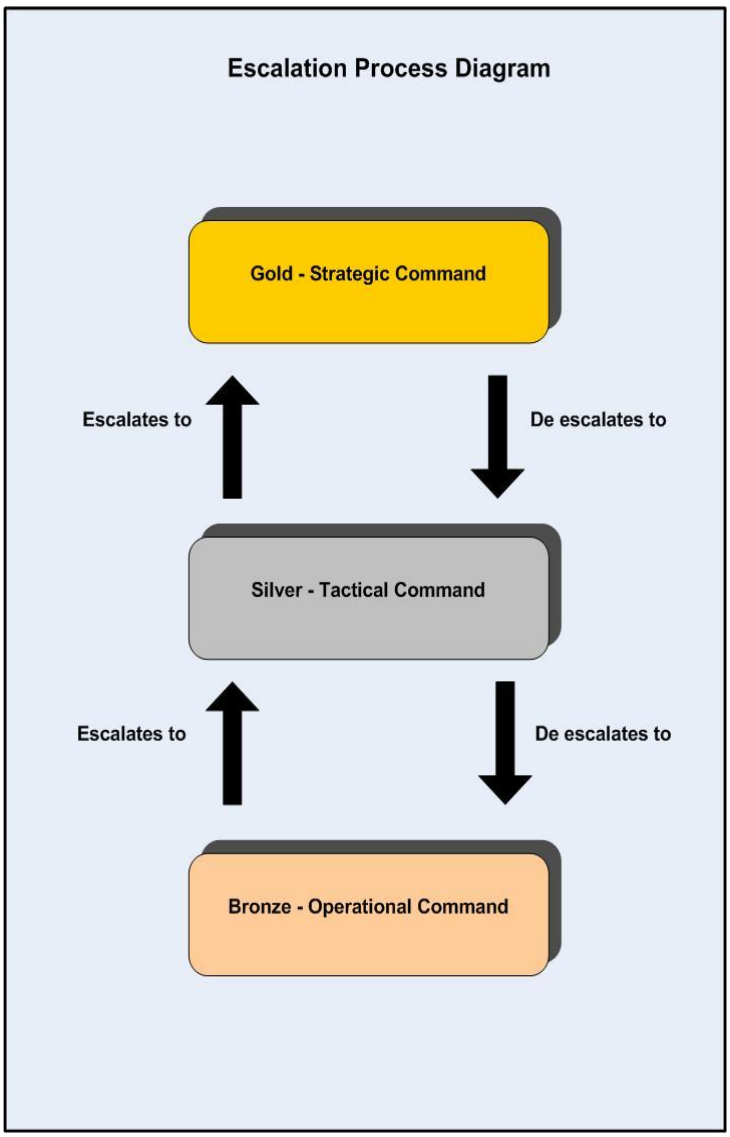
Figure 1.1 The Gold Silver Bronze (GSB) Command structure provides a system for escalating incident command to higher levels of command authority when required. Similarly, when these higher authority levels are no longer required the system allows for de-escalation to the most appropriate level of command.

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 South Eastern 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. (This plan is currently either under development or does not exist)

Plan Manager

1.11 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.

1.12 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.

1.13 Statement of Robustness

This Plan complies with the following robustness criteria:

- The Plan has been reviewed by the HA's Severe Weather and Network Resilience Manager
- The Plan demonstrates an understanding of the roles and capabilities of the Emergency Services, the Local Highway Authorities, HA Area 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.

1.14 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

1.15 Network Area Description

Area 4 is a mixture of motorways (M2, M20 J3 to J13 and M23) and All Purpose Trunk Roads which include dual carriageway with hard shoulder (A2 west), dual carriageways without hard shoulder (A2 east, A20 east of M20 J13, A21, A23, A27 and A2070) rural single carriageway roads (A2 east, A21, A26, A27 A259 and A2070) and residential single carriageway roads (A20 A259 A27) in Kent, part of Surrey, Sussex and part of Hampshire. The roads are split into two categories

Simplified AMOR Contract Incident clearance times based on Table 3.1 of version 1.7

Motorway & APTR Dual – Heavy Routes – Day = 70 minutes
Motorway & APTR Dual – Light Routes – Day = 90 minutes
Motorway & APTR Dual – Night = 120 minutes

APTR Single – Light Routes – Day = 50 minutes
APTR Single – Heavy Routes – Day = 70 minutes
APTR Single – Night = 100 minutes

For more detailed information refer to Table 3.1 in the contract document.

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 Area Team (See Appendix B for contact details)

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
- Coordinating the removal of vehicles from the 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.

3 Service Provider's Standard Incident Response (Bronze)

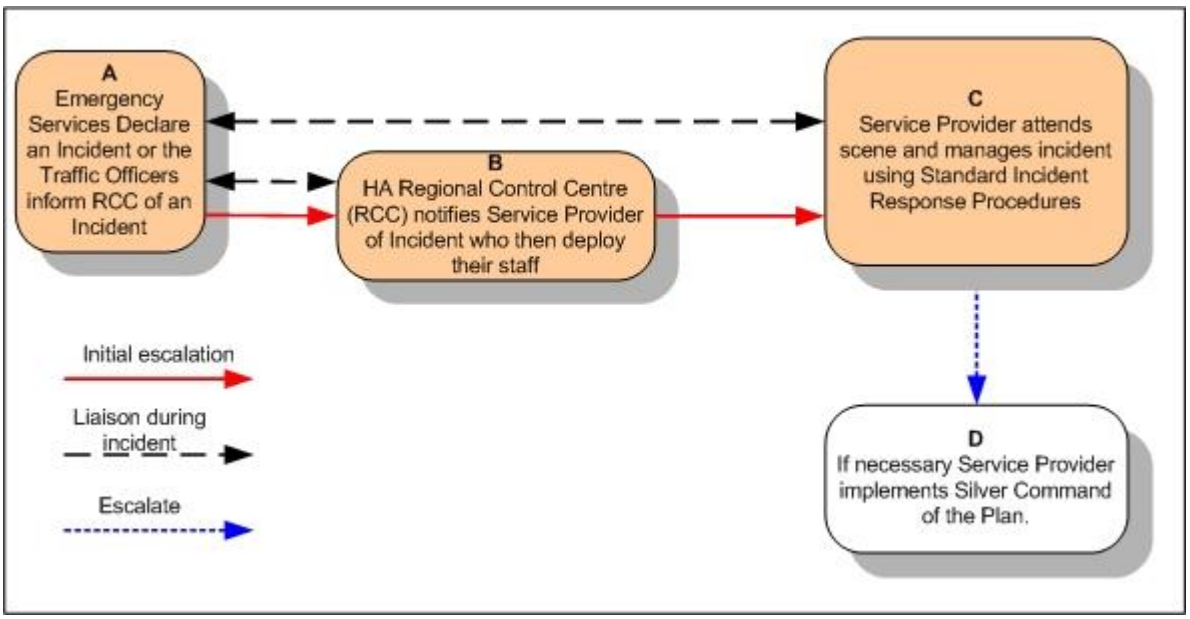
3.1 Introduction

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

Following the introduction of the AMOR contract version 1.7, the Service Provider's "Standard Incident Response Procedures" have changed. There are no longer Incident Support Units ready to respond at a moment's notice to an incident as the Service Provider is no longer required to respond immediately. The Service Provider on notification of an incident will provide a Tactical Incident Response Plan (TIRP) explaining how the incident will be cleared up and the network returned to normality. They will deploy the most appropriate response for the clear up of the incident. This will not however conflict with the escalation of this plan, as the basis of the plan is to demonstrate how the Service Provider and other organisations move forward when the standard response is not enough.

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 MRT, 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 Produce a Tactical Incident Response Plan (TIRP)and sends an Maintenance Response Team (MRT) and/or 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 Response 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 response.

4 Service Provider Tactical Command (Silver Command)

4.1 Introduction

This is not part of the Area 4 standard incident response, see box below.~~Mobilisation of the Media Management Team (MMT) is a function which may be carried out by a team or an individual and is only is 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 If a media message is incorrect, inform the RCC~~

Thisis a partial escalation to Silver which is NOT part of the Area 4 escalation process.This section is dealt with by the Network Control Centre (NCC) in its normal function. It is also part of the role of the National Incident Liaison Officer (NILO)

~~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.~~

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.

AREA 4 escalation to Silver

A complete explanation of the Area 4 escalation process is found in the Area 4 Incident Response Plan.

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 Response 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)~~See 4.2
- Administration Team
- ~~Senior Management Team~~

The Senior Management Team **isGOLD** and not part of the TMT. However the TMT may be in contact with the senior manager on call prior to GOLD being called.

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 Tactical Management Team will be made up by the Tactical Manager using whoever the TM feels best suited to the needs of the particular incident. This may include outside specialists from companies assisting the Service Provider in their response to the incident.

The Area 4 incident response model is based around one team working for and with the TM, not separate groups. This team will carry out communications and admin functions for the TM. There will also be specialists (pavement engineers, Street lighting etc.) available and called in to assist the TM with decision making in relation to 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~~ *See Section 4.2*

~~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~~ (This is a GOLD response not Silver)

~~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

Structure of the TMT

- The TMT will comprise those specialist staff the TM deems necessary to make decisions relating to the particular incident and sufficient admin support to assist with:-
- Ensuring that communications, decisions and actions by all staff are recorded
- Keeping the RCC updated with the current situation.
- Keeping Stakeholders and NILO updated with incident reports
- Monitoring media broadcasts concerning the incident if there are any.

Lines of communication

With the implementation of Airwave radio the TMT will have available, direct contact with the incident and the RCC all communications for the incident should be via an incident channel and this will be monitored by the TMT. Airwave will be the primary method of communication for the incident.

The TMT will take full responsibility for the running of the incident for the service provider. The TMT will maintain close contact with the incident Manager/Supervisor on site (Bronze) via Airwave radio. If radio is not available or if sensitive or confidential information has to be passed then phone will be used.

The TMT will be in contact with the RCC via phone or radio throughout the incident.

The TMT will if necessary be in close contact with the Senior Manager on call (Gold)

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

Kings Hill Office, Meeting Room three. Access out of office hours is via contact with the Network Control Centre

4.5.12 Facilities

The TMR offers the following facilities:

- Computers
- Phone lines
- Display board
- Printer
- Box of Reference
- Airwave Radio base station
- Video conferencing facilities
- Network CCTV

4.5.13 Setup

All equipment required for the TMR will be available in the room. The Airwave Base Station (obtainable from the Traka Cabinet located in the NCC) will require plugging in.

If the meeting room is in use when the TMR needs to be set up the meeting will be moved out immediately the room is required.

IT support is available during office hours.

4.5.14 Interface with other Tactical Teams

The TMT shall expand to encompass any specialised specific role that is needed for a response under any of the operational plans. Additional staff may be required.

It is fundamentally important that there is no blurring of roles between Bronze, Silver and Gold. There is a danger that Silver may become too cantered on the operational issues that are Bronze's remit. Silver should retain a tactical over view at all times. Likewise Gold should avoid losing sight of their Strategic role by becoming too tactical.

4.6 Box G

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

- If the incident is likely to have a severe impact on the network or the ability of the service provider to continue his day to day business or requires mutual aid assistance from neighbouring areas, (see section 5) then the TM will contact the Senior Manager on call (the SM may already be aware of the incident via SMS text messages or incident updates or will have been appraised of the incident by the TM at an earlier stage).
- The TM will call the duty SM from the current rota
- All TM's will be approved to escalate the incident to the SM on call.
- With the introduction of the Senior Manager on call and any team he feels necessary to assist him; the TMT will continue in their tactical control role and assist the SMT where necessary.

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.

With the introduction of Airwave Radio to the service provider the RCC must inform the NCC which incident channel will be used to run the incident. The NCC will change one of its radios to this channel and inform the MRT and Incident Manager/supervisor to do the same. All communications will then be directed through the RCC. When the TMR is set up they will also set their Airwave radio to the incident channel. Airwave will be the primary communications platform.

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

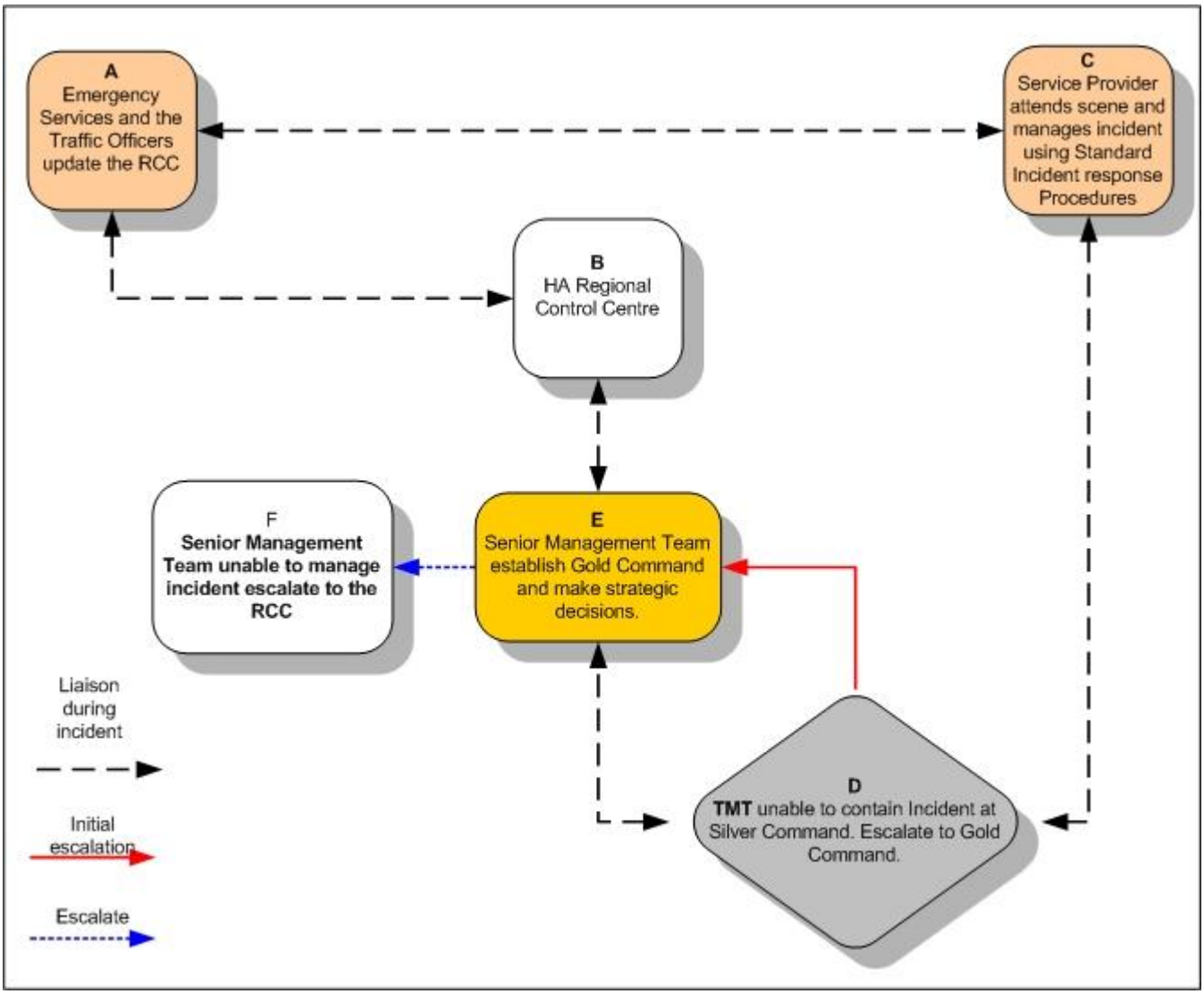
The Service Provider Senior Management Team may also set up Gold Command following liaison with the TMT if:

- Reputation is at risk
- There is public interest at a regional or national level
- Legal action may ensue
- The incident involves death or injury to Service Provider staff or contractors working on the Service Providers behalf.

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:

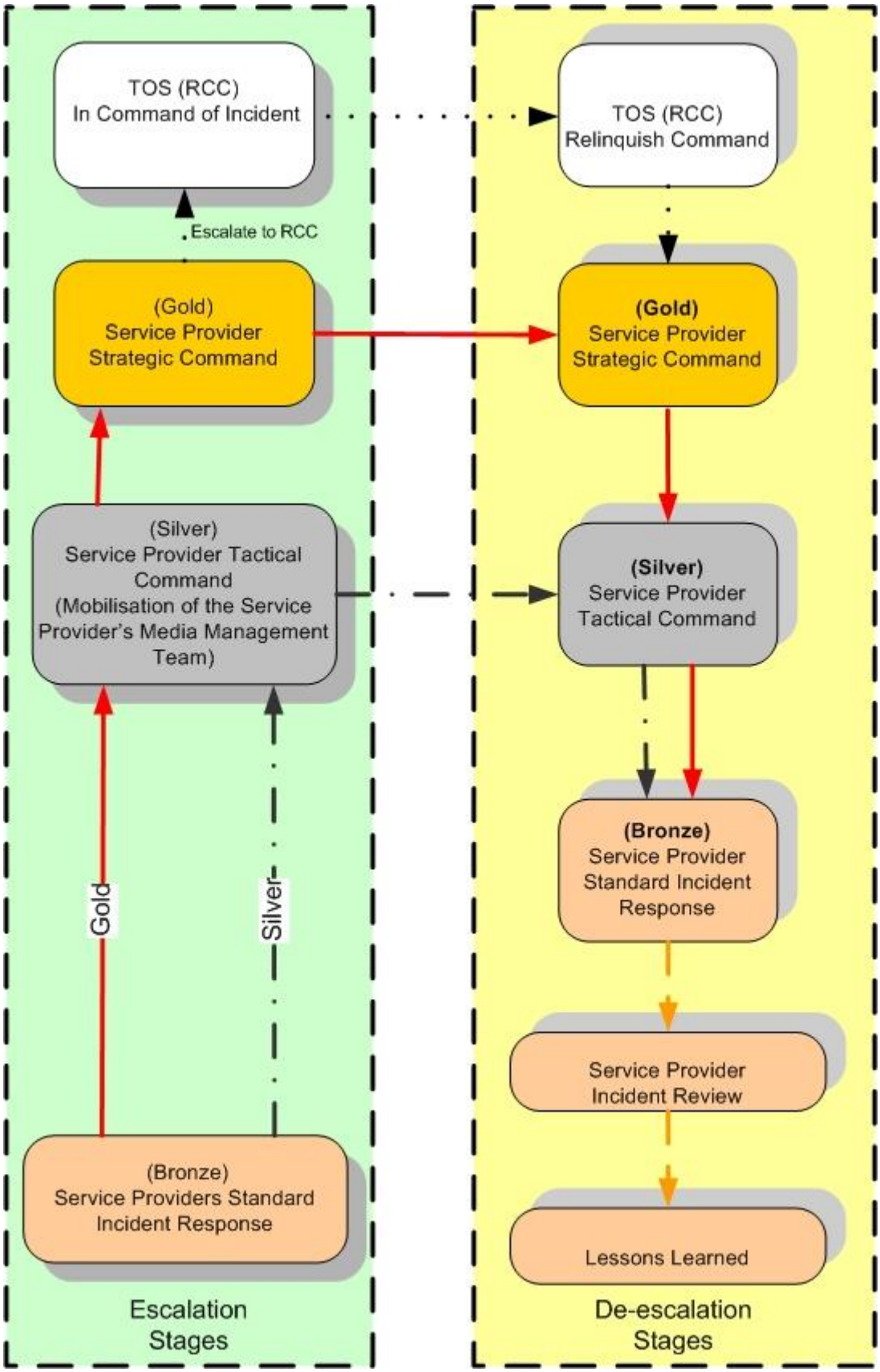
- Bottom up Plan implementation is triggered by events within the Service Provider's area of responsibility.
- Top down Plan implementation is triggered by external events imposed on the Service Provider from the HA regionally or nationally.

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.

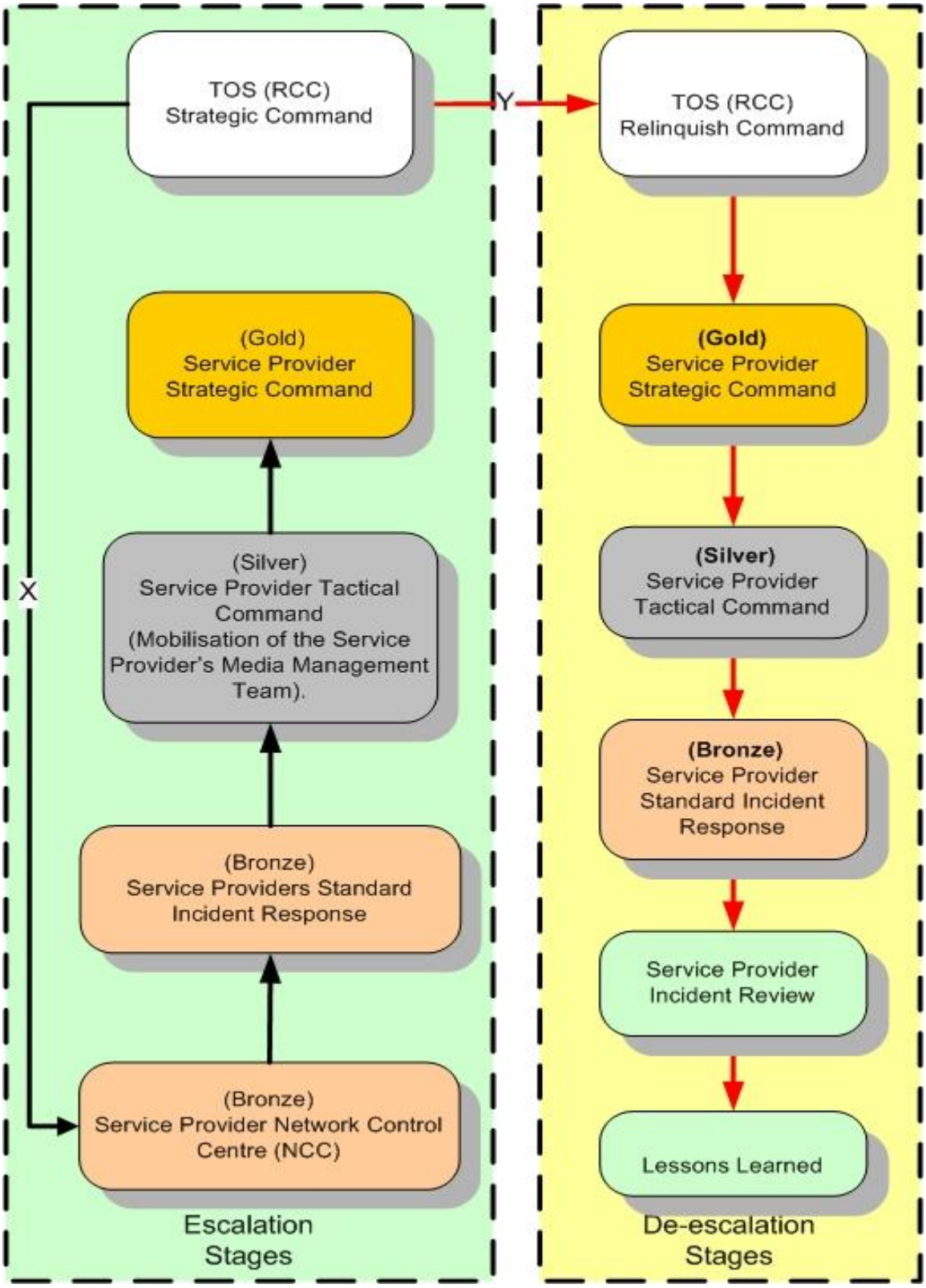
Highways Agency TOS (RCC) Silver Command

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.

Normal channels of communication between the SERCC and Area 4 are via the NCC. The SERCC will contact the NCC requesting the implementation of the network contingency plan. The NCC will contact either the Senior Manager on call (GOLD) or the tactical Manager on call (SILVER) as directed by the RCC. The appropriate manager will then make contact with the RCC to establish what is required of the Area. The Area will then implement a response as required.

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.

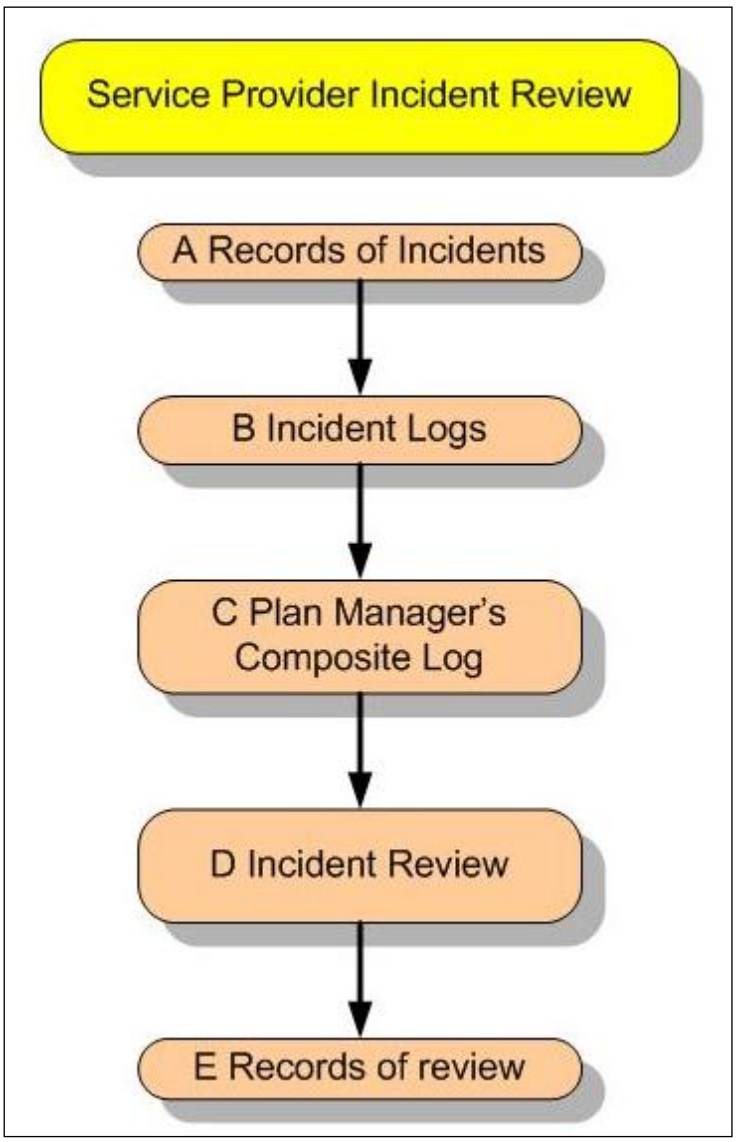
The TOS via the RCC would contact the Service Provider via their NCC and inform them that their services are required. It is then up to the Service provider to determine what level of the plan that they escalate to so that they can provide the assistance that the RCC require.

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 with 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)
- *Remember that if the incident has been managed using an incident channel on the Airwave Radio network then all communications will be recorded at the RCC. Copies of these communications should be available to service providers.
- Records to be kept for a period of years (according to Service Provider's contractual arrangements)

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:

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 Area Performance 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 Area Performance 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.

9.2.1 Balfour Beatty Major Civil Engineering Staff

If a member of staff employed by BBMCE suffers stress as a result of dealing with an incident, a free and confidential counselling service is available from CiC under the Employee Assistance Programme. The service is available 24 hours a day 365 days of the year through the contact number

9.2.2 Mott MacDonald Staff

If a member of staff employed by Mott MacDonald suffers stress as a result of dealing with an incident, a free and confidential counselling service is available from the Employee Assistance Programme. The service is available 24 hours a day 365 days of the year through the contact number. Further details are found in the Mott MacDonald conditions of employment

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 five Boxes:

- One stored in the Network Control Centre, Kings Hill.
- One stored in the Tactical Management Room, Kings Hill.
- One stored at Coldharbour Depot, Junction 5 M20.
- One stored at the SE RCC, Godstone.
- One stored at the Highways Agency Federated House, Dorking.

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) Due to the size of the document it is stored in pdf. format on a CD
- Major Stakeholder Emergency Plans
  Where these plans are marked "restricted" or higher, they will NOT form part of the boxes sent to the SERCC, Highways Agency Federated House unless permission to do so is obtained from the plan owner.
- Service Provider Operational Plans
- Resource 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

Appendix A Plan Holders

Copy Number	Name	Organisation	Position	E-mail address
1				
2				
3				
4				
5				
6				
7				
8				
9				

10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				

34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				

46				
47				
48				
49				
50				
51				
52				
53				
54				
55				
56				
57				

58				
59				
60				
61				
62				
63				
64				
65				
66				
67				
68				
69				

70				
71				
72				
73				
74				
75				
76				
77				
78				
79				

Blank page for pagination

Appendix B Contact Details

B.1 Tactical Decision Team (Silver Command)

There is a rota system in place. The rota is held by the Network Control Centre who will be responsible for calling the on call Silver.

Name	Position	Contact information
Tactical Decision Team		

B.2 Senior Management Team (Gold Command)

There is a rota system in place. The rota is held by the Network Control Centre who will be responsible for calling the on call Gold.

Name	Position	Contact information
Senior Management Team		

B.3 ~~Media Management team~~NOT PART OF AREA 4 ESCALATION PLAN

B.4 ~~Administration Team~~NO ON CALL STAFF FOR THIS ROLE

B.5 Service Provider other resources that may be required

Name	Position	Contact information
Other Resources		
Other resources provided by the Service Provider are on an on-call rota; updated weekly. The weekly on-call rota is emailed to all interested parties and is also held by the Network Control Centre. This includes on call structures team, street lighting and engineering support. The NCC also has contact details for all contracted in services. All communication will only be via the NCC. A list of contracted in services can be found in the RID section 15.		

B.6 Service Provider Area Offices and Locations

Name	Address	Access Arrangements / Available Facilities

Name	Address	Access Arrangements / Available Facilities

B.7 HA Area and Regional Contacts

Name	Position	Contact information

Page blank for pagination

Appendix C Definition of Major Incidents

Major Incidents are any emergencies that require the implementation of special arrangements by one or more of the emergency services, the NHS or local authorities for:

- The rescue and transport of a large number of casualties
- The involvement either directly or indirectly of large numbers of people
- The handling of a large number of enquiries likely to be generated both from the public and the news media usually to the Police
- The large scale deployment of the combined resources of the emergency services.
- The mobilisation and organisation of the emergency services and supporting organisations, e.g. Local Authority, to cater for the threat of death, serious injury or homelessness to a large number of people

The police or other emergency services will usually declare a major incident and notify the Highways Agency through service providers network control centres or similar.

Blank page for pagination

Appendix D Definition of Critical Incidents

Critical Incidents are unforeseen events that seriously impact upon the Highways Agency and its ability to deliver its 'safe roads, reliable journeys, informed travellers' objective. Importantly, the police, other emergency services or local authorities may not consider these types of incident as important as the Highways Agency.

Critical Incidents also include incidents of which ministers wish to be informed.

It should be noted that Critical Incidents might be, or become, major incidents.

Service Providers declare Critical Incidents for their own and the Highways Agency management purposes. If Service Providers believe that Critical Incidents are or may become major then they should notify the police immediately.

The following are deemed to be Critical Incidents:

1. Multiple collisions involving fatalities, serious injuries or vehicles disabled on a carriageway

2. Partial or full closure of motorways or trunk roads due to weather or road conditions. This will also include minor incidents occurring at differing locations aggravated by other circumstances, which taken as a whole fall into this category

3. Collisions involving crossover of a vehicle from one carriageway to another

4. Collisions involving passenger coaches, school minibuses, trains, or public service vehicles resulting in fatalities or injuries

5. Fatal collisions involving fire

6. Serious collisions involving a vehicle carrying dangerous substances (e.g. hazardous chemicals, flammable liquids such as petrol, radioactive materials, etc.)

7. Collisions on motorways or trunk roads resulting in serious/potentially serious structural damage (e.g. to a bridge) necessitating road closures

8. Fatal collisions on motorways or trunk roads where road works are in progress

9. Any significant event impacting partial or full closure of motorways or trunk roads due to collisions, security alerts or criminal/terrorist acts. (NILO must ensure that TRANSEC is advised of security alerts)

10. Any incident off or adjacent to the network that may meet any of the above criteria, and affects the network.

11. Any incident or event off the HA network which results in stationary vehicles, on the HA network, for a period of 1 hour or more.

12. Suicide or attempted suicide resulting in the closure of lanes or carriageways.

13. Roadwork's over running by 30 minutes or more, and likely to have an impact on the network.

14. Any instances of 50% of the 'reserve' winter maintenance fleet being utilized within any area.

15. Any instance where the Highways Agency or Managing Agents provide welfare support or are aware of support being provided to road users on the Highways Agency's network by other organisations.

Criteria for reporting an incident to the Minister

The Minister only needs to be informed about the most serious incidents on our network, such as the Selby train crash or the Kegworth air disaster, where there are multiple fatalities or issues of national significance.

The Ministers office also wants to be informed about the following:

- Significant accidents involving a school minibus whether resulting in fatalities or not
- Any serious accident involving a vehicle carrying dangerous substances e.g. chemicals, inflammable liquids such as petrol or radioactive materials
- Major closure of motorways or trunk roads due to accidents, weather or road conditions and other incidents, where serious congestion is likely or has occurred
- Death or serious injury of an HA employee or contractor

HA officials also need to be told about the most serious incidents. However, where there is significant damage to roadside furniture or, where there are emergency closures causing significant delays, the relevant Divisional Director should be informed only when the HA Duty Officer is unobtainable.

Appendix E Glossary

ACPO	Association of Chief Police Officers
AMM	Highways Agency "Area Management Memo"
AMOR	Asset Maintenance and Operational Requirements
APM	Highways Agency Area Performance Manager
Bronze Level Command	On-site incident management by Emergency Services Officer in Charge/Traffic Officer/Service Provider
Box of Reference	A box that contains reference information about the network and also Operational and Major Stakeholder Emergency Plans.
Contingency Plan Response	The highest level of Area response to incidents
Network Control Centre (NCC)	May be called by another name on other Areas, but is essentially a 24/7 communication service which deploys the Service Providers MRT's
CP	Service Providers Contingency Plan
Emergency Diversion Route	A pre-planned route to take traffic away from an incident site
ECP	Highways Agency "Emergency Contact Procedures"
EDRD	Emergency Diversion Route Document
Standard Incident Response Procedures	Service Provider established plans for dealing with routine Network incidents
Gold Level Command	Strategic Management of the incident
HA Area Team	Highways Agency Area Performance Manager's Team
Implementation Criteria	The circumstances in which the Contingency Plan will be implemented
IRP	Incident Response Plan: Contractually required under AMOR V1.7 sets out how Service Provider will deal with incidents on their network. This is a separate document to the NCP
MRT	Service Providers Maintenance Response Team. These will attend the scene of an incident if required.
MMT	Service Providers Media Management Team
NCP	Network Contingency Plan

NILO	HA National Incident Liaison Officer
NRT	Highways Agency Network Resilience Team
NTCC	National Traffic Control Centre
Process Flow Chart	A diagram showing the procedures to be followed in the event of an incident
RCC	Highways Agency Regional Control Centre (RCC)
SERCC	South East RCC
Service Provider	Managing Agent
Silver Level Command	Tactical Control
Stakeholder	An organisation with a vested interest in the efficient performance of the Area network, which should be informed of incidents which may affect them or their business.
Strategic Network	The HA Area motorways and trunk roads
SIMF	Highways Agency "Standard Incident Management Framework"
SIMG	Highways Agency "Standard Incident Management Guidance"
Senior Management Team	Service Providers Senior managers who will make strategic decisions for the service provider
Tactical Management Team	Team of Service Provider personnel responsible for the Tactical Management of an incident
Tactical Management Room	A designated room where the incident can be managed without interference from other day to day business. Should be fully functional with all equipment required to manage an incident.
TOS / HATOS	Highways Agency Traffic Officer Service
TRANSEC	Transport Securities and Contingencies Directorate (DfT)