HIGHWAYS AGENCY

Area 1
Service Provider
Contingency Plan
Final Version 1.0

April 2012

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

Transport

Area 1

Service Provider Contingency Plan Version 1.0

Issue and Revision Record

Rev	Date	Originator	Checker	Approver	Description
1.0 Draft	20/03/12	▇▇▇	▇▇▇	▇▇▇	First Issue
1.0 Final	12/04/12	▇▇▇		▇▇▇	First Issue

Changes made at 20/03/2012 Review

Section 1.16 – Remove comments relating to response times and replace with reference to Incident Management Plan & minor rewording to final paragraph on Traffic Officers.

Section 8.2.1 – Insert' 6 years' for retention of records.

Section 10.2 – Major Stakeholder Emergency Plans: Remove dates from others Severe Weather Plans, add DCC, CC & PC Winter Service Plans, add Area 1/TOS Joint Operating Principles and under Service Provider Operational Plans: add Haldon Hill Severe Weather Response Plan.

Section 10.3 – Add Turn Around Points Sign Bin Inventory, add Spillage & Pollution Bin Locations, amend VMS locations to show also stored on 'S' drive, amend Major Works on or off Network to show also stored on 'W' drive, External Events amend to show these are recorded on SRW system, Traffic Officer Boundaries amend to show they patrol the A38 in Devon. And remove ISU patrol routes.

Appendix A – update Plan Holders table.

Appendix B4 – remove ███████ from Admin Team.

Appendix B7 – change ███████ title.

List of Contents

Executive Summary

This is the Contingency Plan for EnterpriseMouchel Area 1.

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.

The Plan is updated 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.

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 1 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

    o And/or

- They require support/authority to activate additional resources or authorise decisions

    o 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

Escalation Process Diagram

Gold - Strategic Command

Escalates to | De escalates to

Silver - Tactical Command

Escalates to | De escalates to

Bronze - Operational Command
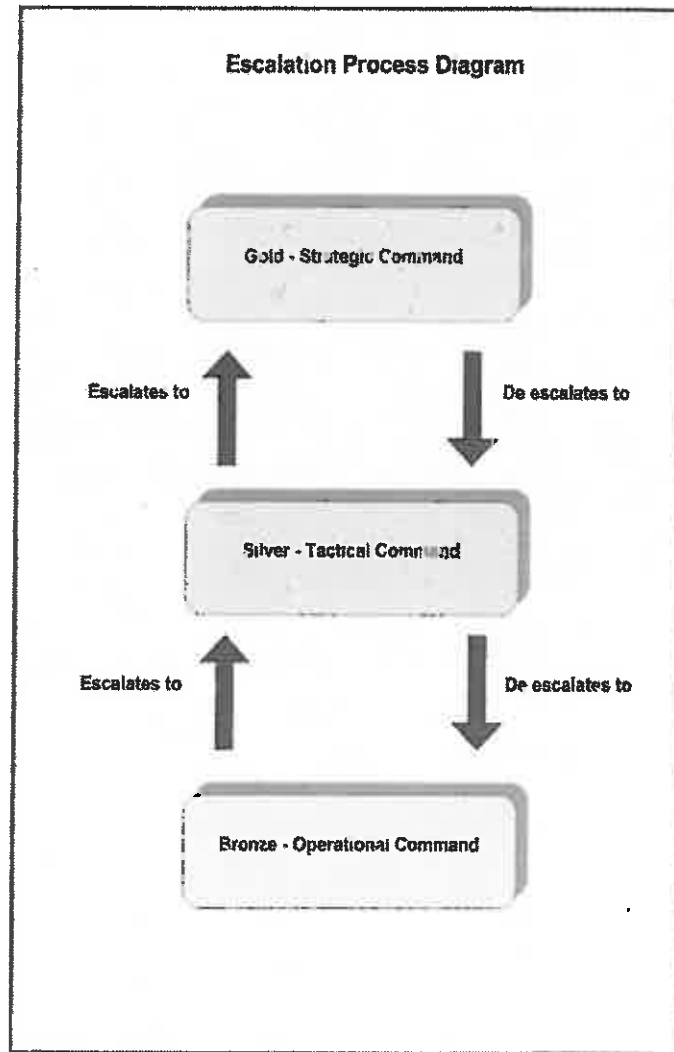
1.9   Strategic Management by the HA Traffic Officer Service (RCC)

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 West 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

██████████ – JTR, Network Occupancy & Severe Weather Manager
EnterpriseMouchel Area 1
Ash House
Exeter
██████████

1.12   Plan Updates

The Plan is a live document that is to be updated every six months (see Plan Managers Review Record held in the Master Copy). 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 Area Performance 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.*

* *All Enterprisemouchel staff (duty managers) involved in the implementation of the Plan have been 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

Traffic Officer Patrolled Network
(A38 Devon from J31 to Tamar Bridge)
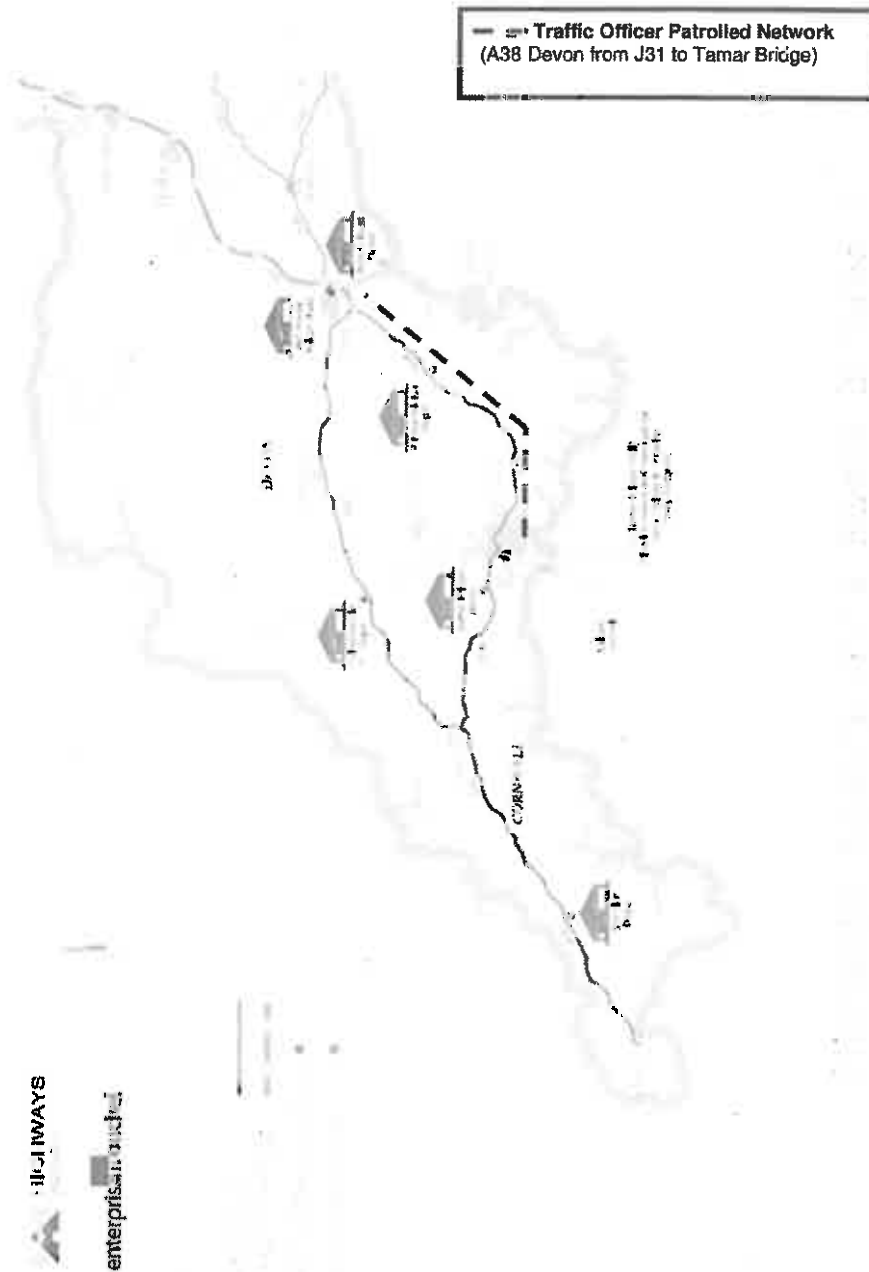
1.16   Network Area Description

EnterpriseMouchel (EM) are the Highways Agency's MAC Service Provider for Area 1 and manage the A38 and A30 in Devon and Cornwall. Both roads run from the M5 at junction 31 south of Exeter to either Bodmin (for the A38) and Penzance (for the A30). Current contract duration is July 2010 to June 2015

The A38 and A30 are predominantly rural and are comprised of rural single and dual carriageways without hard shoulder.

The A30 (all dual carriageway in Devon) which skirts north Dartmoor is a fairy high and exposed route between Whiddon Down and Launceston. Although generally quiet and with low traffic flows during the winter, the A30 becomes extremely busy throughout the summer as it is the main holiday route into Cornwall for most of the country. West of Launceston it runs over the top of Bodmin Moor which can be prone to severe weather events. between Bodmin Moor and Penzance there are a number of single carriageway summer congestion 'Hot Spots' namely Temple, Carland to Chiverton and Camborne to Penzance.

The A38 (all dual carriageway in Devon) although it does not carry the same amount of holiday traffic as the A30 is commuter sensitive throughout Devon and in east Cornwall. It also bisects the city of Plymouth and then crosses the privately owned Tamar Bridge into Cornwall. With the exception of Haldon Hill, which is just south of Exeter and at over 220m above sea level is a high risk location during snow fall, the A38 passes to the south of Dartmoor and generally is not as exposed to severe weather as the A30.

The Tamar Bridge on the A38 which spans the River Tamar between the city of Plymouth and Saltash carries three lanes and has a toll collection system for eastbound traffic. The bridge is privately owned and is managed and maintained by the Tamar Bridge and Torpoint Ferry Company from their office/control room on the eastern side of the bridge approach.

On the west side of the bridge is the Saltash Tunnel; this single bore structure carries the A38 below the town of the same name. The tunnel, which is owned by the H.A and maintained by EM, has three lanes and operates on a tidal flow system which is a continuation of that used on the Tamar Bridge. Both the tunnel and the bridge function using a wide range of technology including overhead and road stud lane control, CCTV and incident detection equipment; for these reasons the day to day management of the tunnel and its technology is the responsibility of the Tamar Bridge Office. The Saltash Tunnel has its own specific contingency plan (Multi Agency Response Plan MARP) which will be initiated should a serious incident occur in the location.

From west of Saltash to Bodmin the A38 is mainly single carriageway and bisects a number of small communities.

The 24/7 Area 1 Network Control based at Ash House Exeter manage and deploy the appropriate resource to incidents as and when they occur as detailed in the Area 1 Incident Management Plan.

Operating from an out station at Buckfastleigh, Traffic Officers patrol the A38 between M5 J31 and the Tamar Bridge.

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

- Provide on-site liaison with the emergency services

- Provide on-site liaison with other relevant organisations such as the Environment Agency, Tamar Bridge Office etc, and provide any support as required.

- Co-ordinate and manage any repairs to the highway infrastructure as required which will return the network to normal operation as soon as is possible.

- Monitor the operation of the network via CCTV

- Request the activation and deactivation of NTCC VMS on the M5, A38 and A30.

- Request the activation and deactivation of the A38 VMS.

- Activate and deactivate the Area 1 mobile VMS

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.

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.

Figure 3.1: Service Provider's Standard Incident Response Procedures
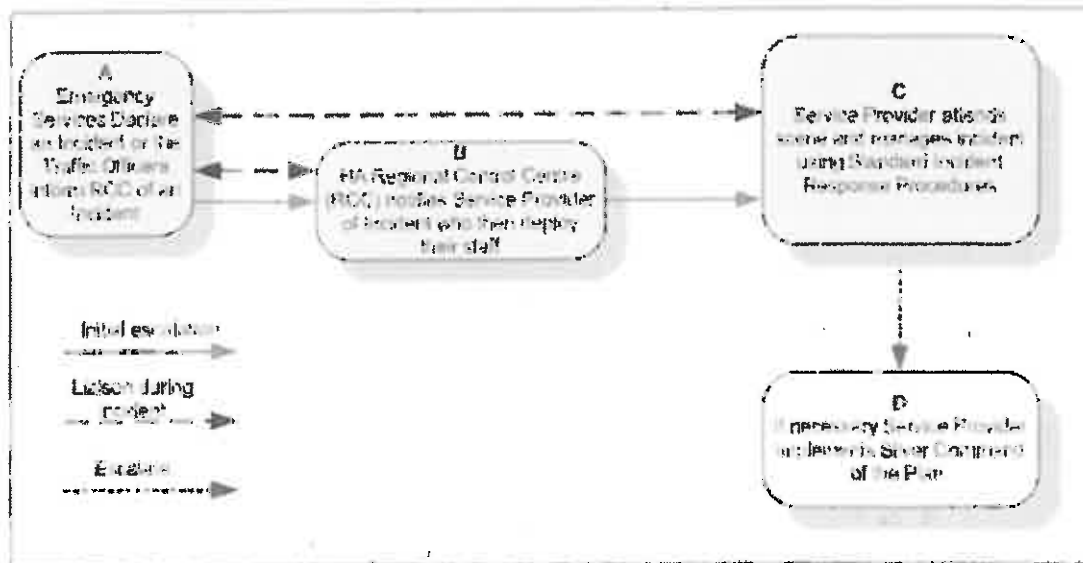
3.2 Box A

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 ISU, 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 sends an Incident Support Unit (ISU) and 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

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, the Tactical Manager and NCC

- Monitor CCTV images if available to determine an appropriate response

- Monitor the messages set by the RCC & NTCC and inform them if they are not appropriate.

- Inform Major Stakeholders affected by the incident

- Inform Senior Management and regularly update

- Keep the RCC and NILO informed

- Inform and regularly update the local Highways Agency Network Performance and Resilience Teams

- Monitor media broadcasts concerning the incident (TV, websites, radio)

- If a media message is incorrect, inform the RCC

- Liaise with and provide up to date and reliable information to the HA COI

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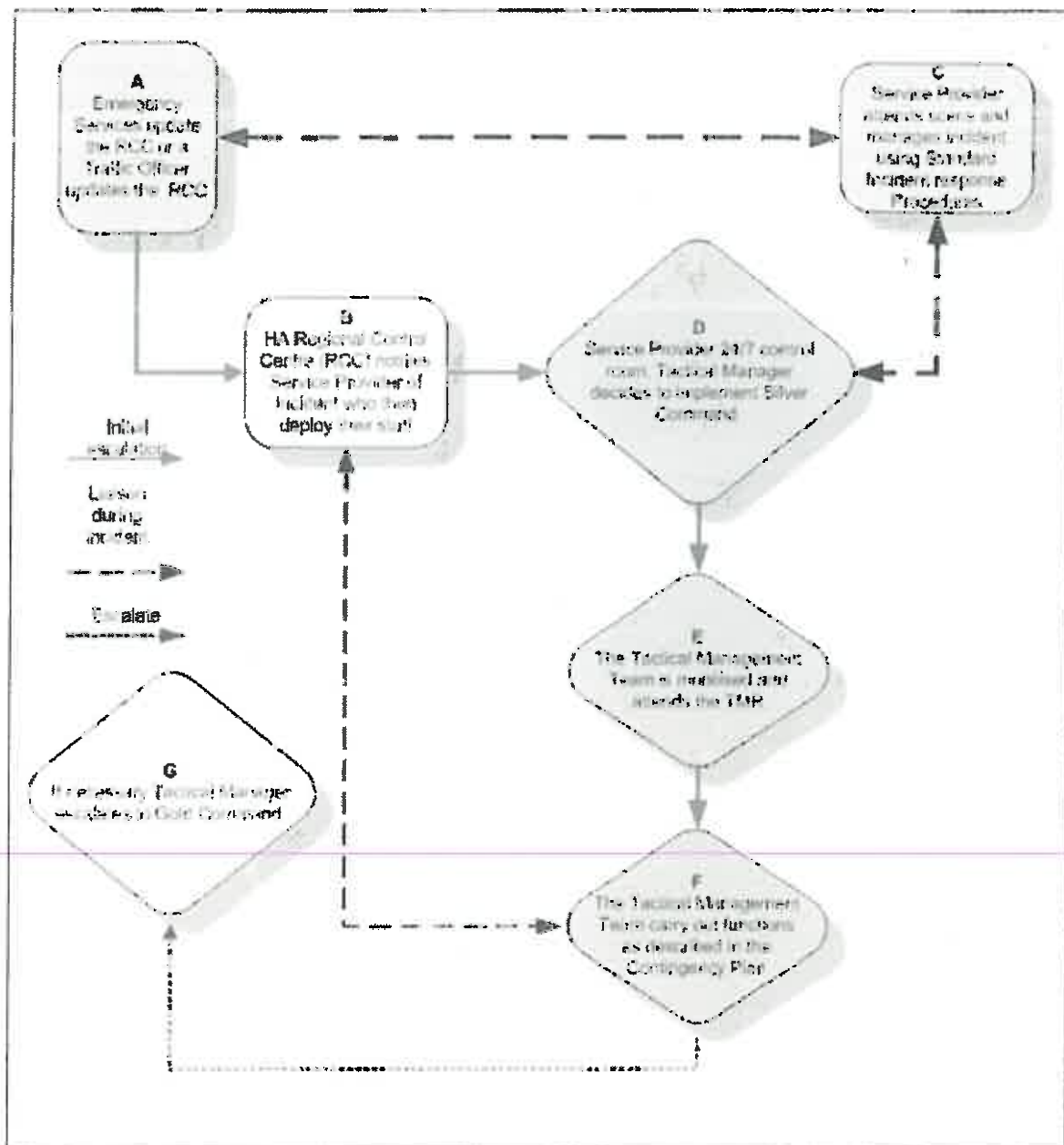
Figure 4.1 : Full Mobilisation of the Plan (Silver Command)

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.

The TM will instruct escalation from the Standard Incident Response to Tactical Silver Command and the mobilisation of the Tactical Management Team (TMT) when he has been made aware by the emergency services or the duty supervisor at the scene that one or more of the incident objectives (Sec 1.7) have been compromised. However, although Silver Command has been initiated, it is recognised that the incident can still be contained using the service providers standard operational response at the scene.

The role of the TMT 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 TM will directly contact those staff named in Appendix B (Tables B1 to B5) and determine availability; all will be fully apprised of the situation and the TM will then develop a rota based on staff availability and expected duration of the incident. If necessary shift patterns will operate on a 08:00hrs to 20:00hrs and 20:00hrs to 08:00hrs basis with half hour overlaps to ensure effective hand-over. Each TMT shift will comprise a Tactical Decision Team of two, one of which will be the TM, an Information Management Team of one and an Administrative Team of two.

The TMT will operate from within the Area 1 NCC at the Ash House Office. Should Ash House become unavailable because of an emergency or power loss, resilience will be maintained by relocating to the operational compound at Avocet Road which is approximately one mile from Ash House.

The TMT will operate from within the meeting room (G3) adjacent to the NCC (separated by folding doors which will be opened), the TM will ensure any meetings booked for G3 have been cancelled for the duration of the Silver Command phase. The TMT will carry out their function on workstations separate from the normal NCC operations and there will be restricted access to the room at all times with a member of the IMT being responsible for dealing with and briefing visitors as required.

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)

- 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).

A minimum of five staff will form the TMT.

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
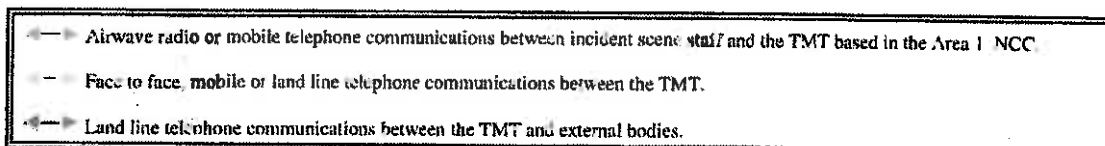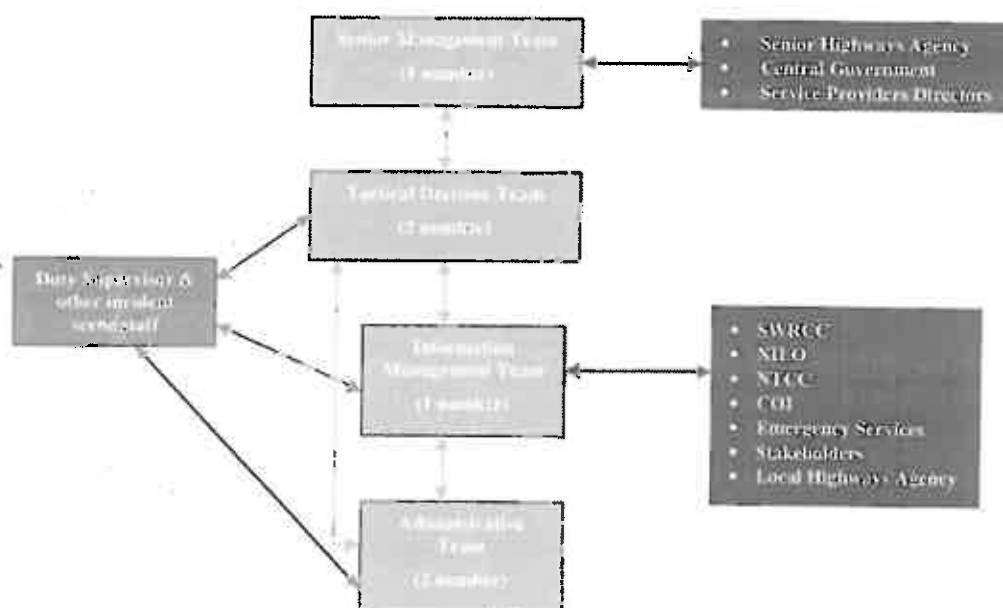
If the incident looks to be a prolonged event then a 12hr working rota (similar to how we resource severe weather desks every winter) will be developed drawing from the following staff:

* Duty Managers x 5
* Duty Supervisors x 10
* Communications Officers x 2
* Admin Support x 9
* Other staff based at Ash House

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 for Area 1 will co-locate within the 24/7 NCC on the ground floor at the Ash House office. Access is gained after passing security control at reception; however, direct access to the TMR during an incident will be restricted to TMT staff only.

4.5.12 Facilities

The TMR offers the following facilities:

- Computers – 4 x permanent work stations and 3 x docking stations for laptops. There are also a number of internet connections for additional laptop useage.
- Land line x 6 and 2 x NCC mobile phones
- Airwave radio base station and several hand held units
- TV and digital radio
- Dedicated laptop for setting Area 1 mobile VMS signs located around the network
- Magnetic display board
- Printer
- Box of Reference

4.5.13 Setup

All of the above are permanently located with the NCC and available should the TMT be mobilised.

4.5.14 Interface with other Tactical Teams

All other emergency operational plans or special events will be managed and co-ordinated by the 24/7 NCC staff, so should there be an incident requiring mobilisation of the TMT, then interface and any liaison or co-ordination will, because of the co-location, take place on a direct face to face level.

Generally, if mobilised, the Area 1 Severe Weather Desk (SWD) will operate from the NCC annex much in the same manner as the IMT, however, should a major incident occur at the same time as SWD is in operation or SWD is initiated during a major incident, then the SWD team will relocate to the operational depot at Avocet Road as described in the Area 1 Severe Weather Plan, a dedicated telephone line will be established to allow liaison between the two teams for the duration of the incidents.

4.6   Box G

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

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
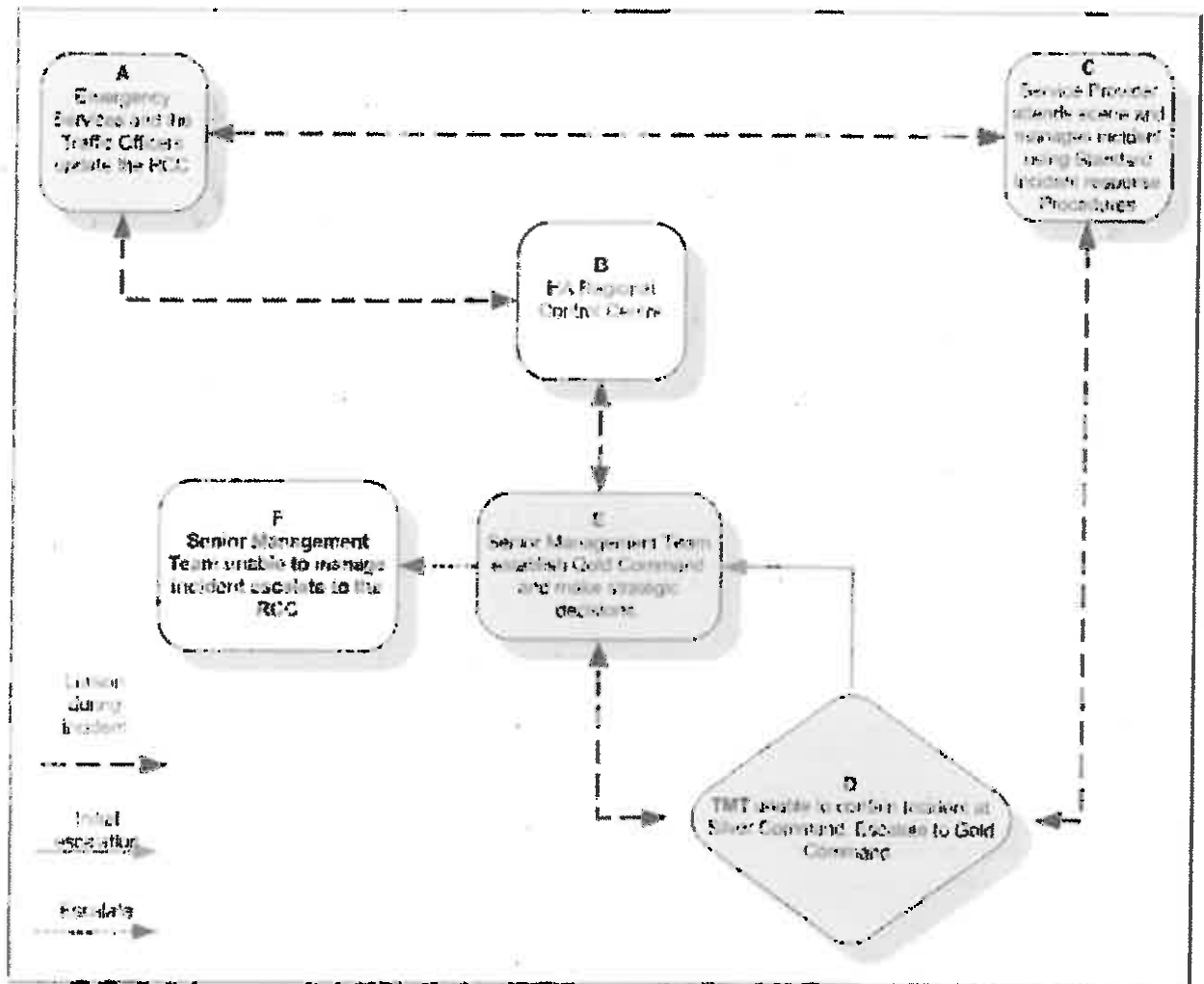
5.2 Service Provider Gold Command

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).

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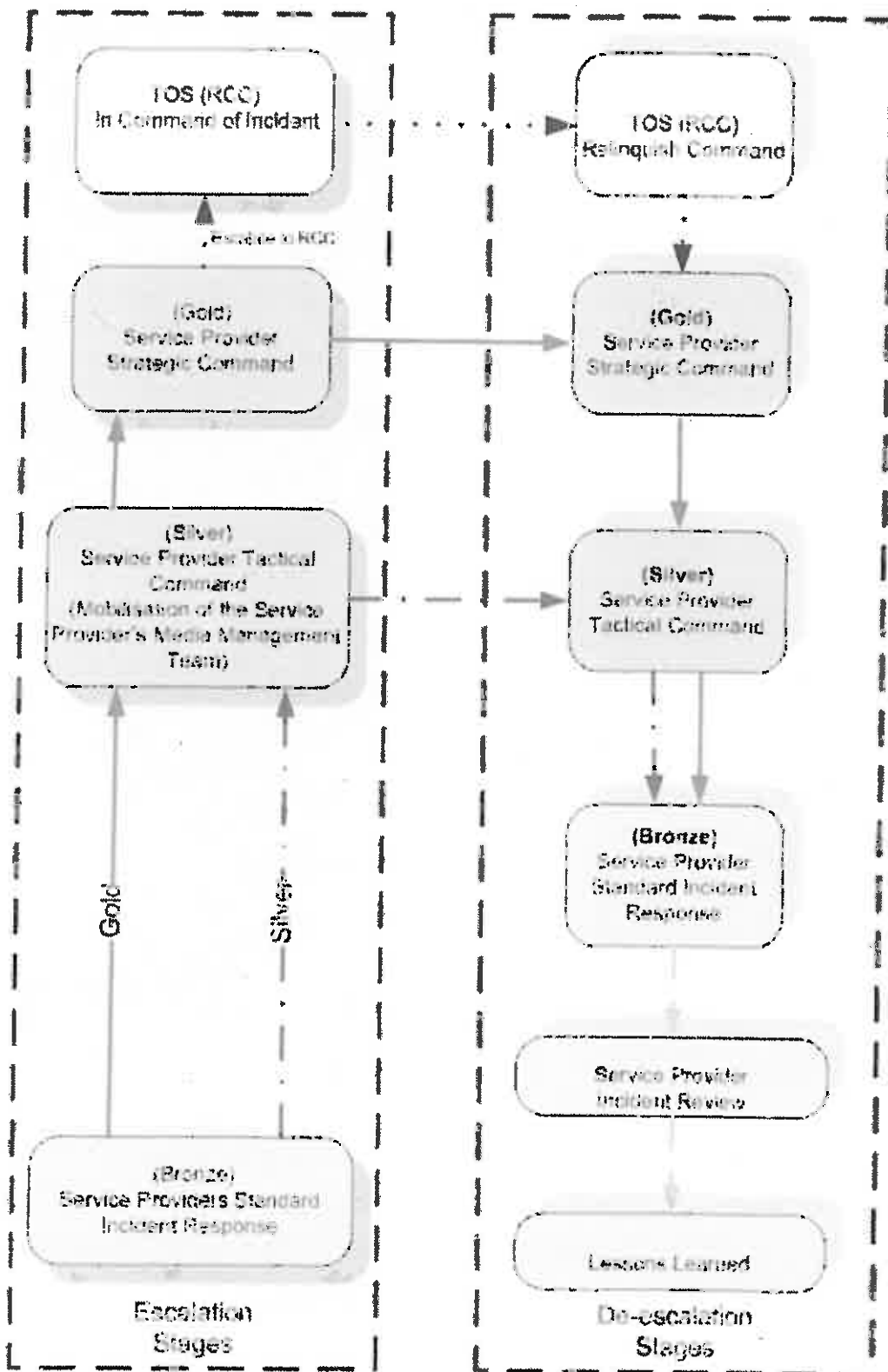
6.3 "Bottom-Up" Plan Escalation and De-escalation

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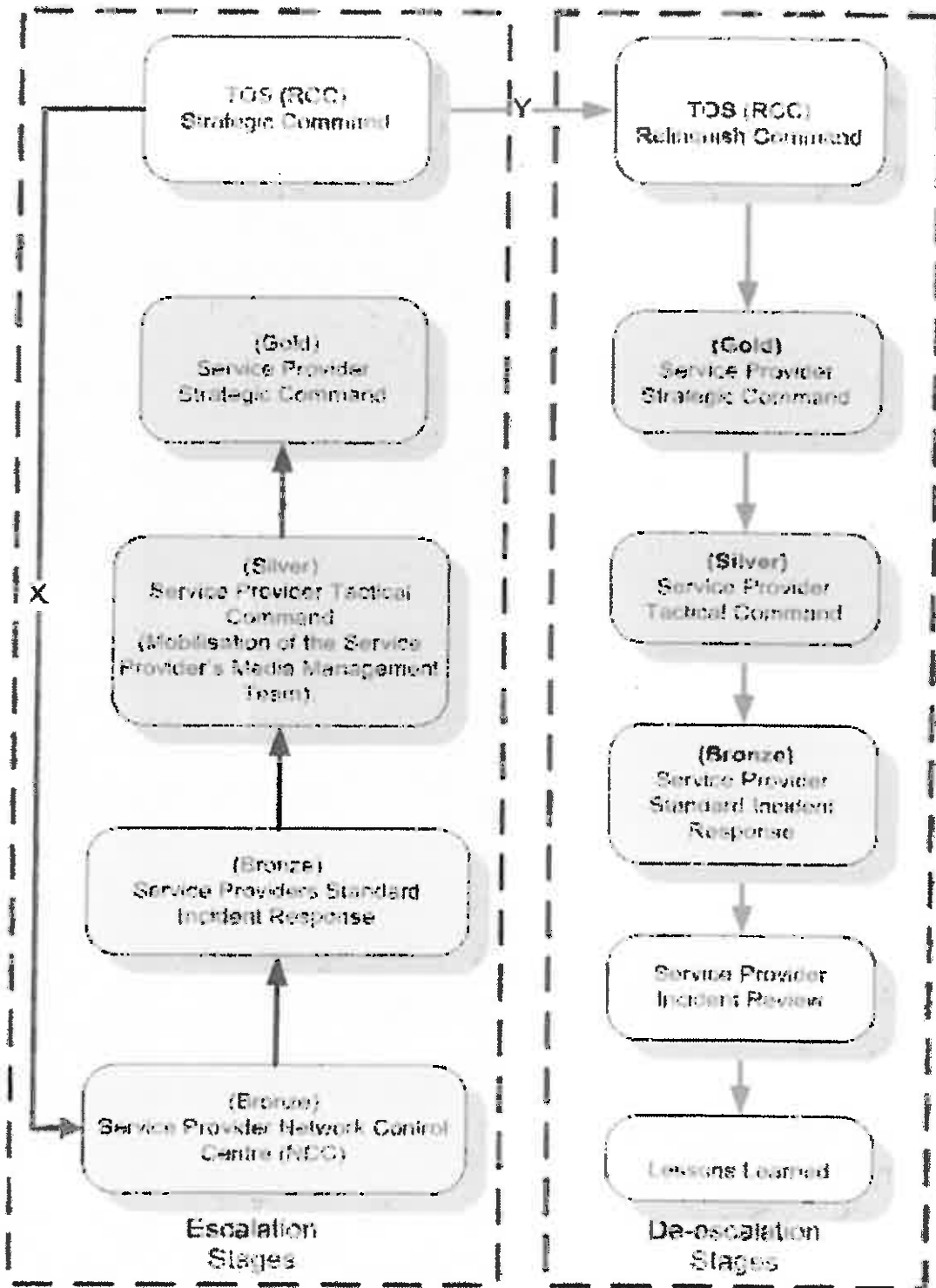
Implementation of the Service Provider's Contingency Plan may be triggered or instructed by HA, in response to events outside the Service Provider's Area.

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.

In the event of a top-down plan implementation, the RCC will contact the Area 1 NCC and advise them of the situation. The NCC will notify the Duty Manager who in turn will mobilse the TMT, MMT and advise the SMT.

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.

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
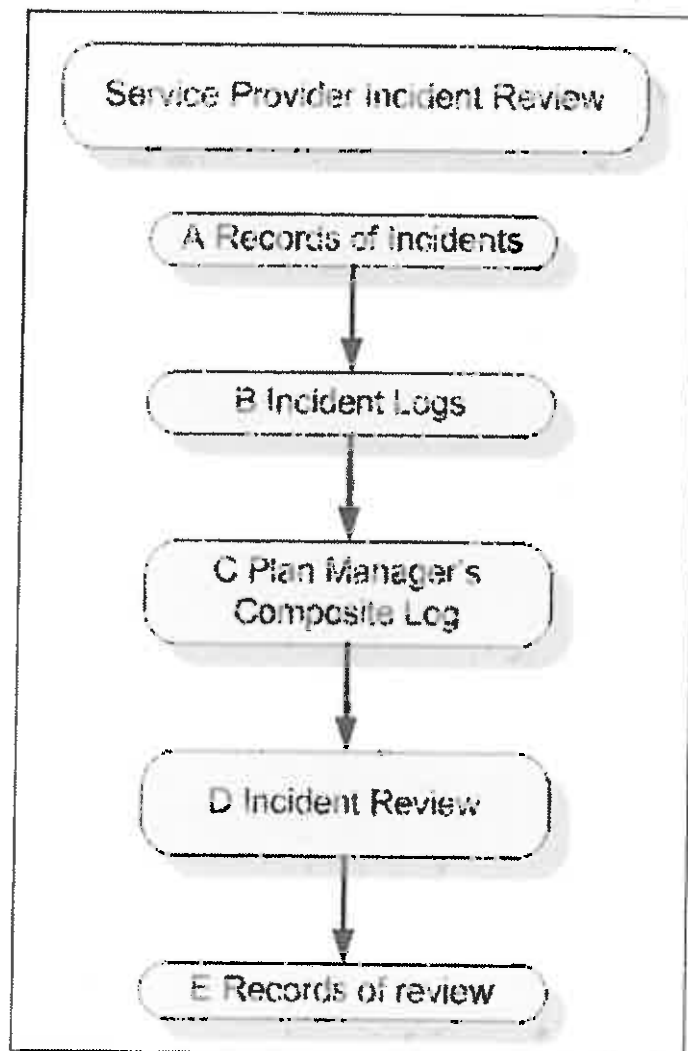
8.2 Box A – Records of Incidents

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)
* Records to be kept for a period of 6 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:

- The dedicated log keepers assigned to that task when the TMT is mobilised

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 and confidential counselling services will be arranged.

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 3 Boxes:

- One stored in the Tactical Management Room
- One stored at the South West RCC
- One stored at the Area 1 depot at Avocet Road Sowton

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
  - Area 2 Contingency Plan
  - Devon County Council Emergency Plan
  - Cornwall Council Emergency Plan
  - Plymouth City Council Emergency Plan
  - A38 Saltash Tunnel Multi Agency Response Plan (MARP)
  - Joint Response Plan for Industrial Incidents at Calor Gas – A38 Lee Mill
  - Defence Storage and Distribution Agency Ernesettle Plymouth – Off-Site Emergency Plan
  - Tamar Bridge & A38 Saltash Bypass – Manual for Police and Fire Services
  - Area 2 Severe Weather Plan
  - Area 32 DBFO Severe Weather Plan
  - DCC, CC & PC Winter Service Plans
  - DCC, Plymouth City Council & Torbay Council - Emergency Telephone Directory
  - HA Crisis Management Plan- Pandemic Support Pack
  - Area 1/TOS Joint Operating Principles

- Service Provider Operational Plans

  - Area 1 (EM) Contingency Plan
  - Severe Weather Plan
  - Area 1 NCC Evacuation & Relocation Procedures
  - Haldon Hill Severe Weather Response Plan

- 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** - These are diagrams showing the junctions, bridges, marker posts and all the key features on the Area 1 Network. These can be used for quick reference to check the layout of the Network at a given location. Both a hard copy, which is inserted in the RID lever arch file, and a CD copy is included in the Box of Reference, the drawings are also stored on – **EM's Business Collaborator Intranet Site**

- **Emergency Crossover Points** - These may be used in Emergencies to enable the Traffic Officers or Police to turn traffic around. A hard copy showing grid references, marker post locations and approximate length of the crossing together with procedures and method statements for opening central reservations is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Vulnerable Nodes** - These are strategic structures or junctions which if taken out of use by a terrorist act or a major incident will cause major disruption to the trunk and adjacent road network. A hard copy listing locations is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Emergency Access Points on Network** - These are access points which the Emergency Services can use to gain access to the HA Network from the adjoining county roads. A hard copy listing locations is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Area Depot Locations** - A map showing locations of all the Area 1 depots is inserted in the RID lever arch file (contact details can be found in Appendix B6), the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Stakeholder Contact Details** - Contact details for adjacent areas, local highway authorities, Emergency Planning Officers and Environment Agency who may be affected by an incident on the Area 1 network. A hard copy listing contact details is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Turn Around Points Sign Bin Inventory** - Maps and lists of contents of all the sign bins on the Area 1 network is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Spillage & Pollution Bin Locations** – Details inserted in the RID and also stored on **EM's Business Collaborator Intranet Site**

- **Location of CCTV Cameras** - A map showing the locations of cameras and details of who operates them on the Area 1 network is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Business Continuity Plan** - A CD copy of the Enterprisemouchel Area 1 Business Continuity Plan can be found in the Box of Reference. It is also held electronically on **EM's Business Collaborator Intranet Site** under Information Management System (IMS)

- **Network Lighting** - A map showing locations and types of Lighting on the Area 1 network is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Location of Traffic Signals** - A map showing locations of traffic signals and maintenance responsibilities is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **VMS Locations** - Maps showing locations of both mobile and permanent VMS on the Area 1 network is inserted in the RID lever arch file, the maps can also be found on the 'S' drive under Area 1 Network Control Centre

- **Major Works on or off Network** - A map showing Locations, dates and contact details of major works on the Area 1 network is inserted in the RID lever arch file, the details are also stored on the 'W' drive under Planned Schemes

- **External Events** - Locations, dates and contact details of External Events impacting on the Area 1 network are entered onto the SRW system

- **Police Boundaries and contact details** - Details of Police Boundaries relating to Area 1 are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Emergency Services contact details** - Contact details of fire and ambulance services on the Area 1 network are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Traffic Officer Service Boundaries** - Operating from an out station at Pridhamsleigh Buckfastleigh, Traffic Officers patrol the A38 between M5 J31 and the Tamar Bridge.

- **High Risk Weather Sites** - A map showing locations of all high risk weather sites, including sections of the network greater than 150 & 250 metres in height is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Hazardous Sites Adjacent to the Strategic Network** - A map showing locations of all hazardous sites adjacent to the Area 1 network is inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Network Rail Bridges over the Strategic Network** - Maps showing locations of all Network Rail Bridges that run over or under the Area 1 network are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Contact details for Service Provider Welfare** - Details for welfare assistance are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Plant and Equipment** - Details of plant and equipment that may be required during of after an incident on the network are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Specialist Contractors to assist the Service Provider** - Contact details and locations of specialist contractors that may be required to attend the scene of an incident are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Types of Communication Systems for liaison with all stakeholders** - Details of communication systems used by Enterprisemouchel are inserted in the RID lever arch file, the details are also stored on - **EM's Business Collaborator Intranet Site**

- **Liaison with Adjacent Areas** - This section should contain contact information regarding details and procedures on how to contact and work with adjacent Areas. Inserted in the RID lever arch file, also stored on - **EM's Business Collaborator Intranet Site**

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.

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 impacting partial or full closure of motorways or trunk roads due to collisions, security alerts or criminal/terrorist acts.

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

11. Suicide or attempted suicide resulting on the closure of lanes or carriageways.

12. Roadworks over running by 30 minutes or more, and likely to have an impact on the network.

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

This is an example of a glossary but should be modified to suit the contents of the Service Provider's own plan.

ACPO	Association of Chief Police Officers
AMM	Highways Agency "Area Management Memo"
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 ISU'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
ISU	Service Providers Incident Support Unit. These will attend the scene of an incident
MMT	Service Providers Media Management Team
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)
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	Highways Agency Traffic Officer Service
TRANSEC	Transport Securities and Contingencies Directorate (DfT)