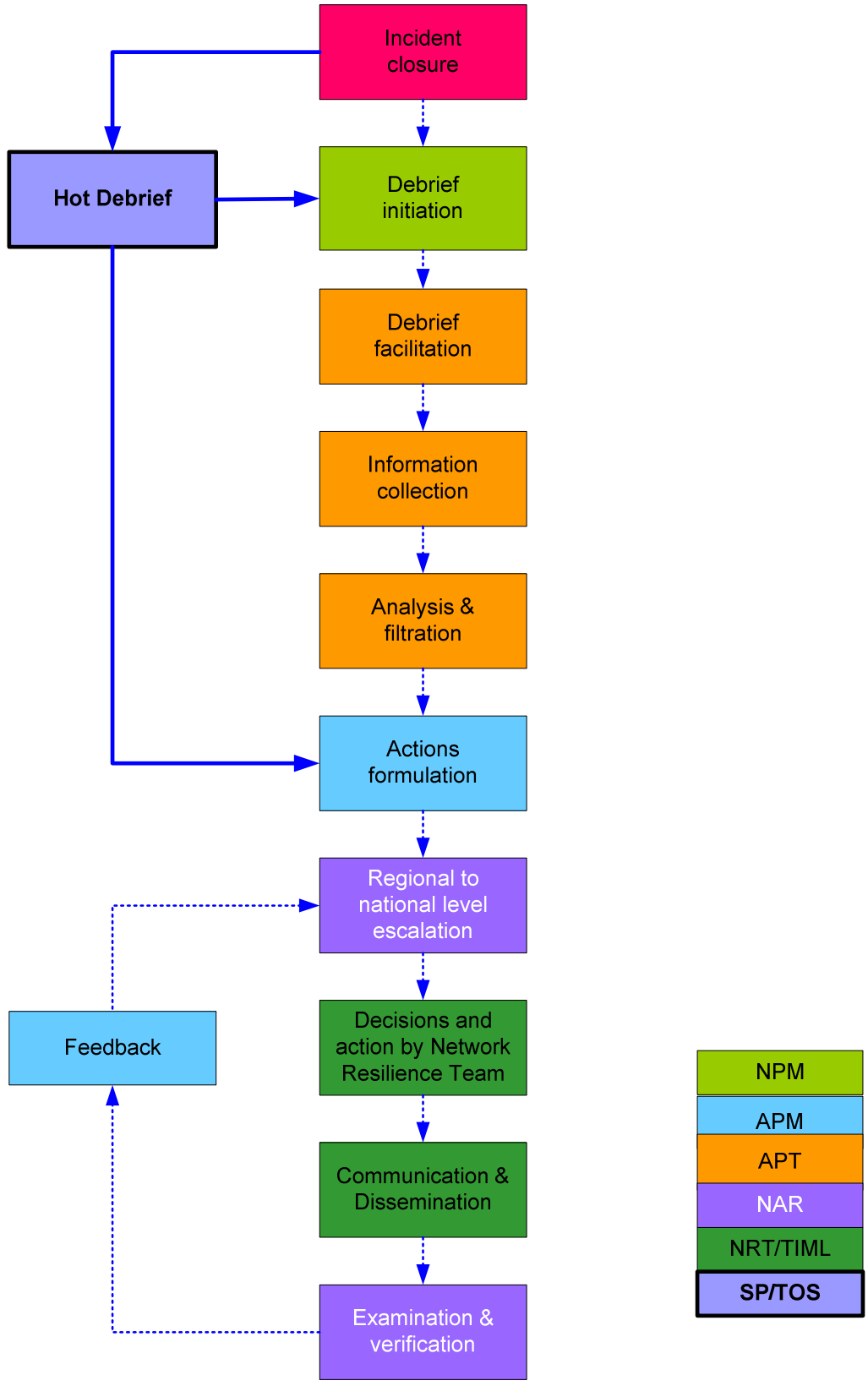
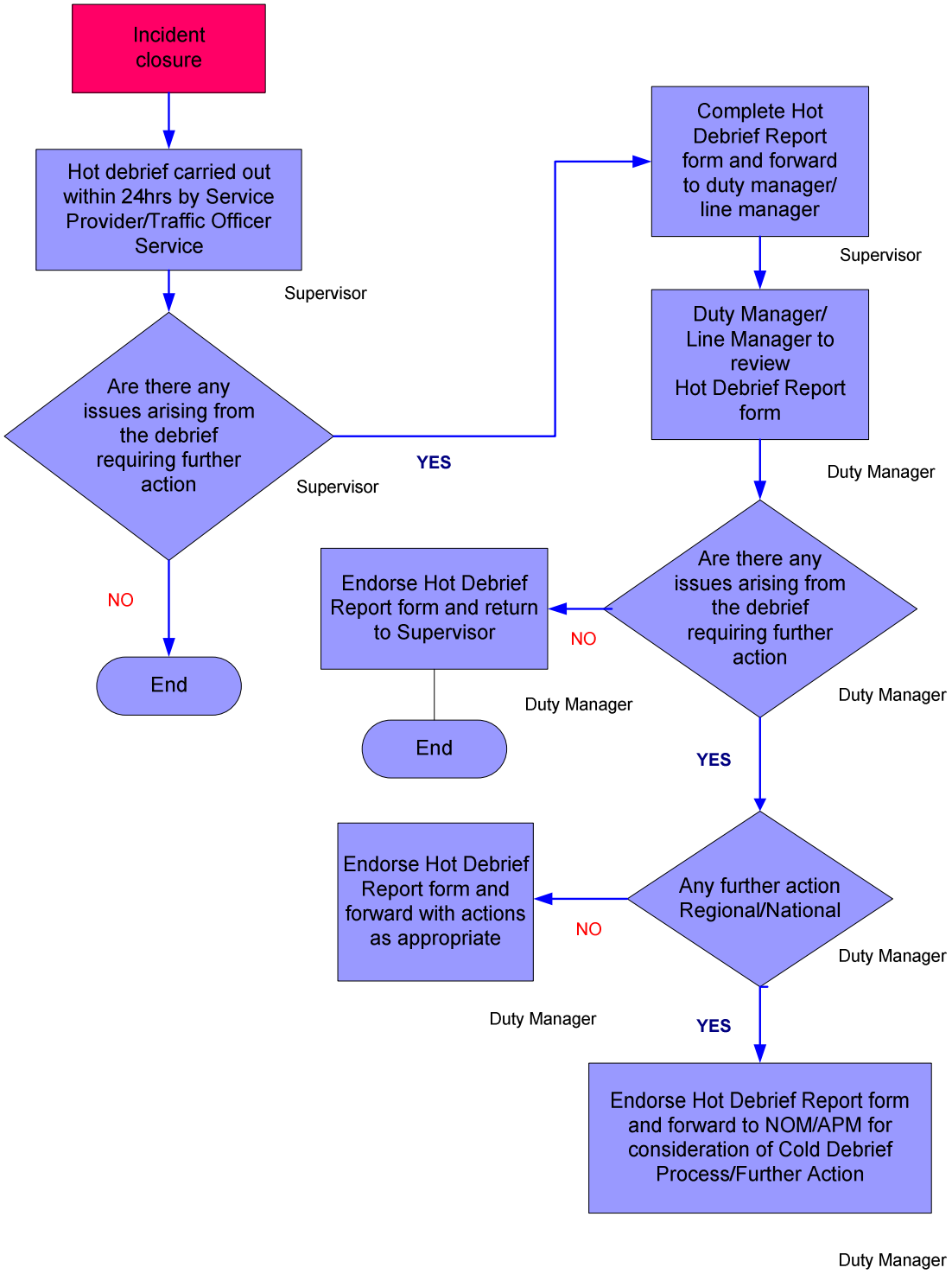
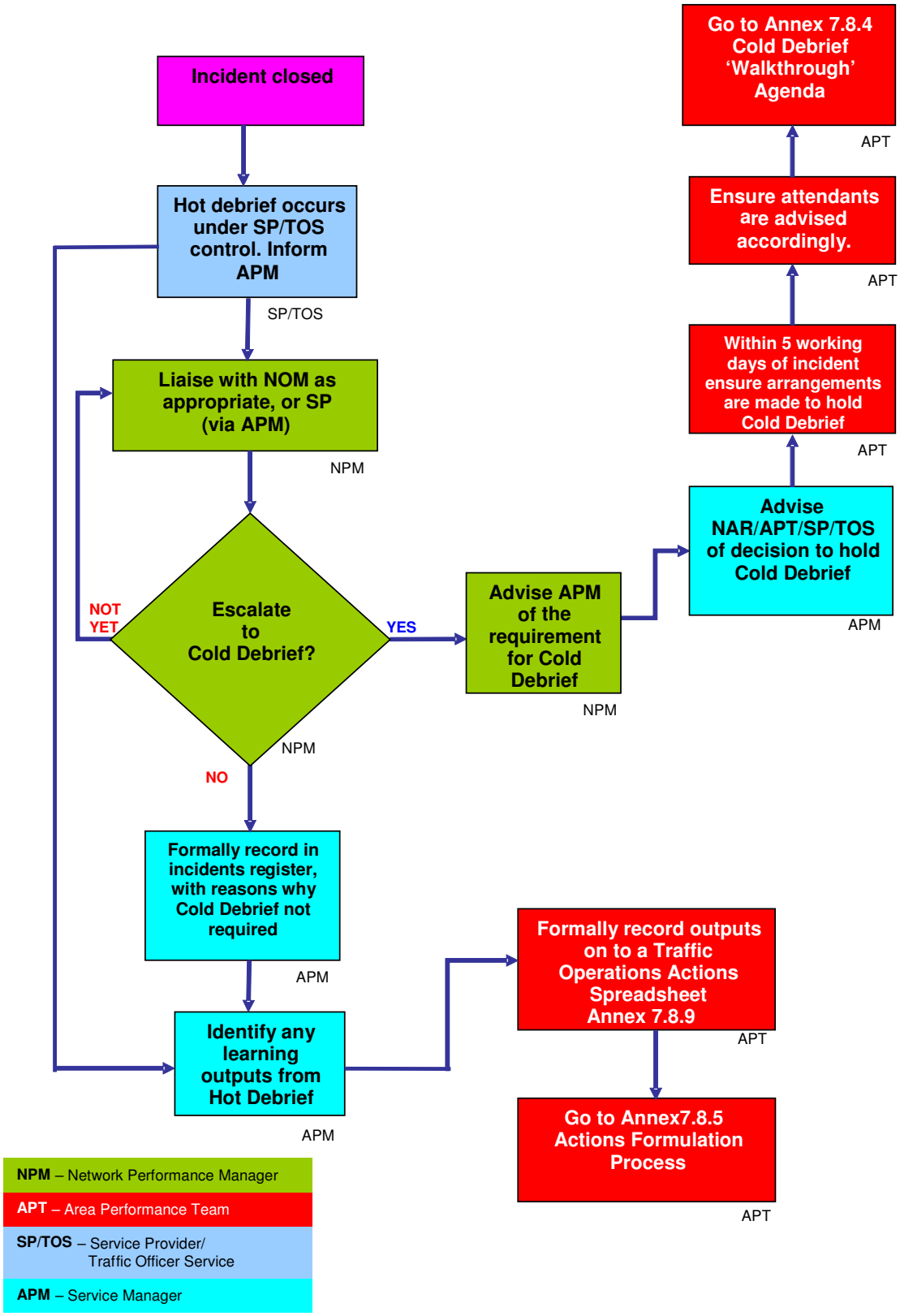
Annex 7.8.1 Framework for debriefs



Annex 7.8.2 Hot debrief process



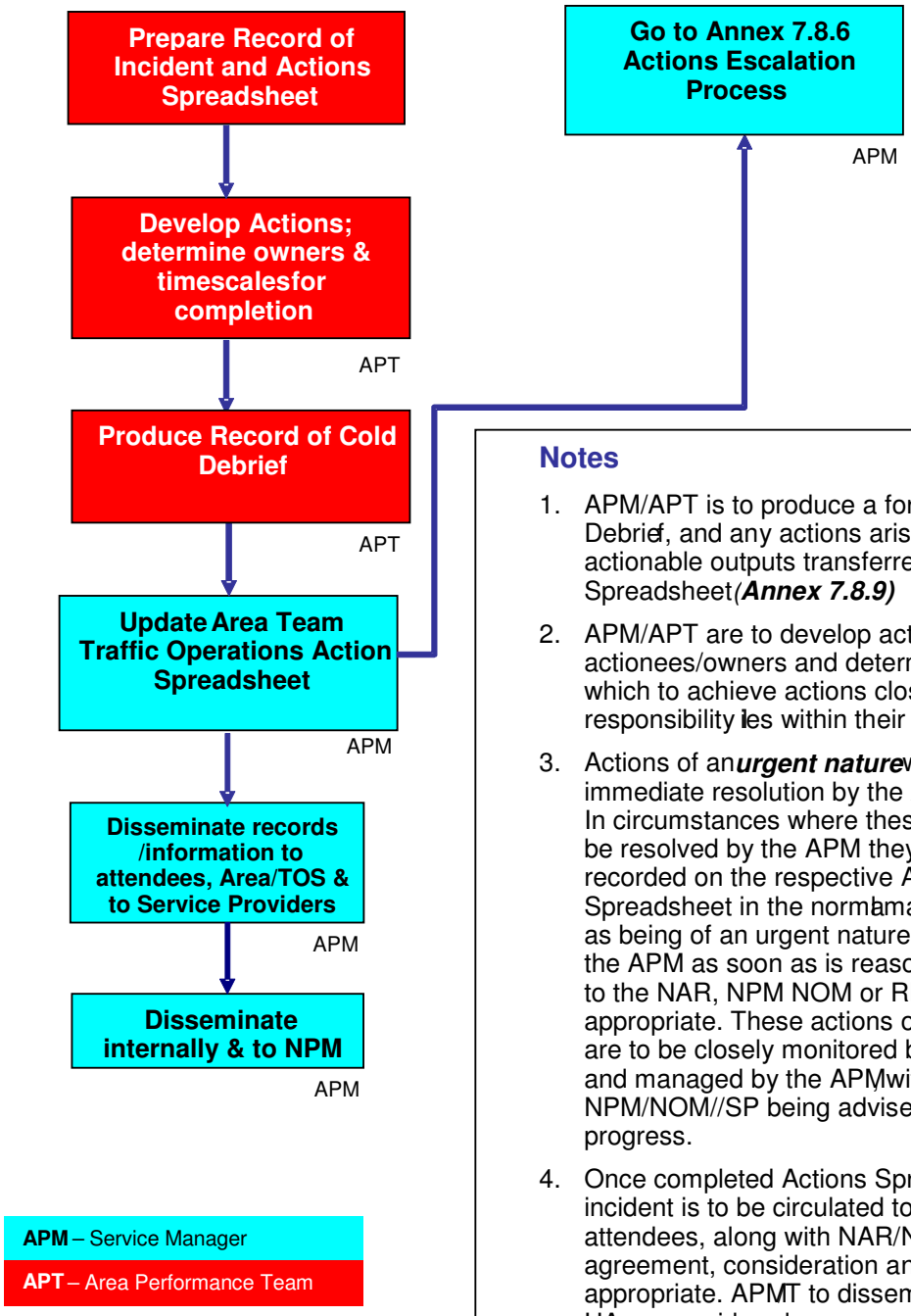
Annex 7.8.3 Cold debrief initiation process



Annex 7.8.4 Incident cold debrief 'walkthrough' agenda

Serial	Action	Comments
1	**Introductions**	Personalities/stakeholders
2	**Objective(s)**	
	Incident Details	• Description • Location – e.g. Ordnance Survey, lane(s) • Date & time – dd/mm/yy, 24 hour clock
3	**Walkthrough incident with timelines**	• Incident detection (How/when?) • Incident verification (How/when?) • Incident response (How/when?) • Recovery & repair (How/when?) • Restoration (How/when?) • Other relevant inclusions
4	**Review/discuss individual organisation incident logs**	Agree sequence of events in chronological order
5	**Formulate consolidated incident log plotted against timeline**	Period from incident notification through to incident site clearance
6	**Identify any problems experienced, or issues identified, by any organisation, & cause(s)**	Gather all information needed to draft Incident Report and enter actions onto Actions Spreadsheet post de brief. Consider • Communications • Diversions • Resources • Sign setting • Media • Weather • Access • Egress • Welfare • Command & Control • Processes/Practice/Junctions/Network • Other
7	**Identify things that went well, any Lessons to be learned, good and bad practice and lessons and agree actions, owners and timescale**	
8	**Identify where improvements/ research/study could be made**	
9	**Any additional relevant information**	
10	**Close debrief meeting**	

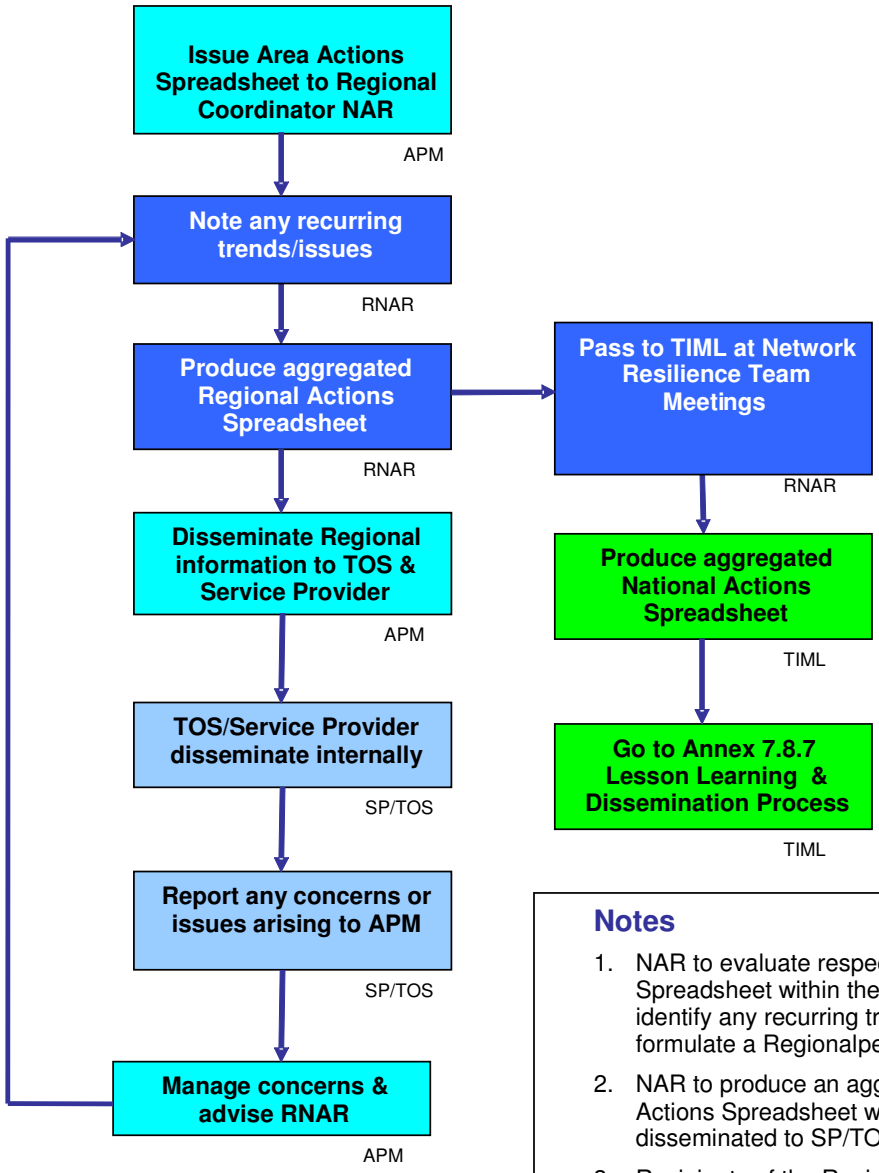
Annex 7.8.5 Actions formulation process



Notes

1. APM/APT is to produce a formal record of Cold Debrief, and any actions arising and other actionable outputs transferred to the Actions Spreadsheet *(**Annex 7.8.9**)*
2. APM/APT are to develop actions, determine actionees/owners and determine timescales in which to achieve actions closure, where responsibility lies within their Area.
3. Actions of an ***urgent nature*** will require a more immediate resolution by the APM/NPM or RD. In circumstances where these actions cannot be resolved by the APM they are to be recorded on the respective Actions Spreadsheet in the normal manner, annotated as being of an urgent nature, and escalated by the APM as soon as is reasonably practicable to the NAR, NPM NOM or RD where appropriate. These actions of an urgent nature are to be closely monitored by TIML & NAR, and managed by the APM with respective NPM/NOM//SP being advised accordingly on progress.
4. Once completed Actions Spreadsheet for the incident is to be circulated to Cold Debrief attendees, along with NAR/NOM and SPs for agreement, consideration and action as appropriate. APMT to disseminate within the HA as considered necessary.
5. APM/T to issue updated Actions Spreadsheet to NAR within 28 days of the incident occurrence.

Annex 7.8.6 Actions escalation process



APM – Service Manager

TIML – Lesson Learning Wkstrm Ldr

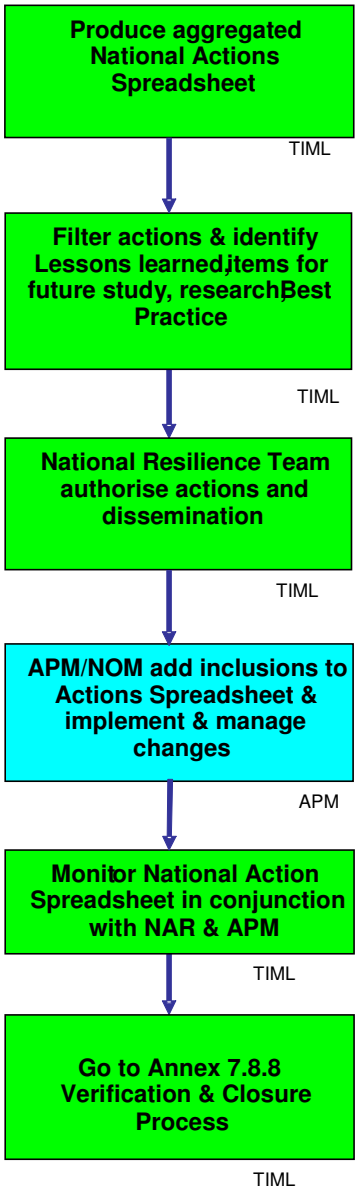
RNAR – Regional NAR

SP/TOS – Service Provider/ Traffic Officer Service

Notes

1. NAR to evaluate respective Actions Spreadsheet within the HA region in order to identify any recurring trends or issues, and formulate a Regionalperspective.
2. NAR to produce an aggregated Regional Actions Spreadsheet which is to be disseminated to SP/TOS on a 6weekly basis.
3. Recipients of the Regional Actions Spreadsheet should disseminate and report any concerns they may have, or any identified issues arising, to the appropriate APM. APM is to advise NAR of any of the above concerns.
4. NAR is to issue the Regional Actions Spreadsheet to TIML at the 6weekly NAR National Forum.
5. TIML is to produce an aggregated National Actions Spreadsheet for dissemination, identify national trends and issues, and formulate a national perspective postNetwork Resilience Team Meetings

Annex 7.8.7 Lesson learning & dissemination process



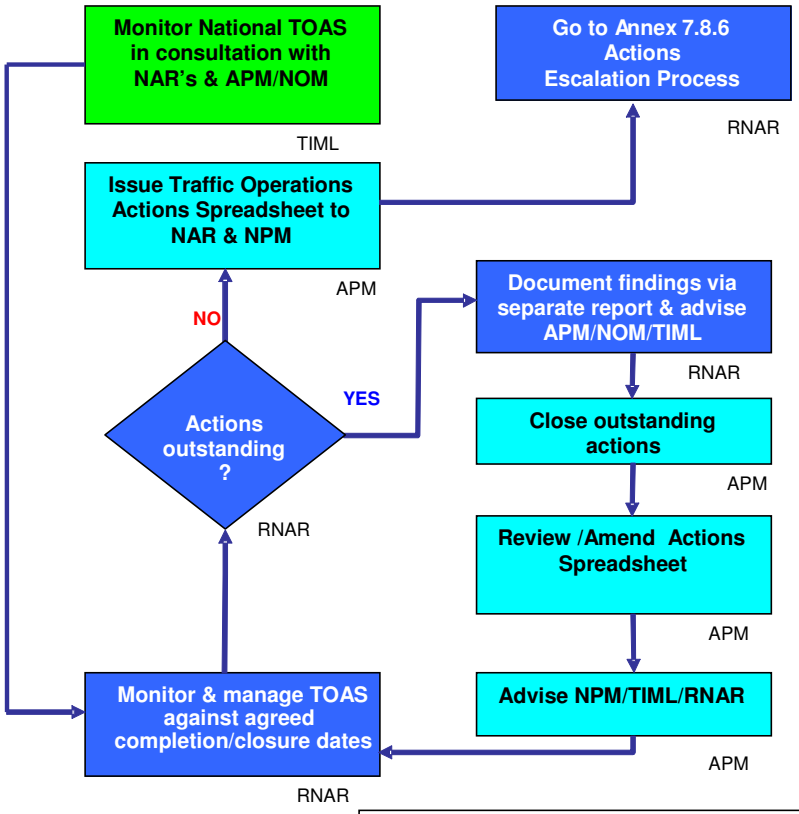
Notes

1. TIML is to review all actions and identify lessons to be learned from the aggregated National Actions Spreadsheet with the assistance of NAR's.
2. TIML is to disseminate information to TIM Programme, TIM Workstream Leaders, TIM Centre of Excellence (yet to be scoped), Regional Intelligence Units *(RIU)*, Roads Information Framework *(RIF)*, Traffic Information Service (TIS) and to all NAR's. They will also submit Network Resilience Team requests for actions to address identified problems to Regional or Specialist directors or TIM governance as appropriate.
3. NAR to disseminate information to APM/NOMs.
4. Network Resilience Team is to monitor Lesson Learning implementation in conjunction with NAR and APM/NOMs.

APM – Service Manager

TIML – Lesson Learning Wkstrm Ldr

Annex 7.8.8 Verification and closure process



APM – Service Manager
TIML – Lesson Learning Wkstrm Ldr
RNAR – Regional NAR

Notes

1. TIML is to monitor National Actions Spreadsheet in consultation with NAR's and APM/NOM.
2. NAR to manage actions against agreed completion/closure dates in order to verify that action closure is achieved.
3. TIML to liaise with NAR to agree any actions that are outstanding.
4. TIML/NAR to document erroneous findings via separate report, and advise respective APM.
5. APM to achieve closure of outsta nding actions.
6. APM to advise NPM/NAR & TIML when actions closed out.
7. TIML/NAR to re-examine as necessary, and agree actions closed out.
8. APM to review and revise Actions Spreadsheet post - agreement on action closures.
9. APM to issue updated Actions Spreadshee t to NPM & RNAR

Annex 7.8.9 Traffic Operations actions spreadsheet (TOAS)

INCIDENT & DEBRIEF								INCIDENT DEBRIEF ACTIONS								
Incident Number	Incident Date	HA Area	Incident Location (Road)	Incident Location	6 Figure Ord. Survey Grid ref	Incident Description	Cold Debrief Date	Owner Organisation	Action owner	Incident Action Details	Planned Close-out date	Actual Close-out Date	Completed	Best practice (Y/N)	Comments	Lessons Learned

Annex 7.8.10 ISU Incident data capture sheet & guidance note

Service Provider Reference number:

ISU type attending: **Motorcycle** ☐, **Car** ☐, **Van** ☐, **Truck** ☐

Motorway: ☐, **All Purpose Trunk Road**: ☐, **Road Number**: ☐☐☐☐☐☐☐
(For designations such as A1(M), please tick both motorway and trunk road)

Type of carriageway; S2 ☐, D2M ☐, D3M ☐, D4M ☐, **Other**

Mainline ☐ , **Entry Slip Road** ☐, **Exit Slip Road** ☐, **Junction no**.:

Secondary road *(number or name if appropriate)*:

Direction of travel of incident: north ☐, south ☐, east ☐, west ☐
clockwise ☐, anti-clockwise ☐, roundabout ☐

Is the incident in roadworks: **Yes** ☐, **No** ☐

Please locate the incident by at least one of the following options:

Ordnance Survey Grid Reference *(6 figure)*:

Marker Post: **Emergency Roadside Telephone**:

Lamp Post Reference: **Other location**:

NOTE: PLEASE USE THE 24 HOUR CLOCK FORMAT FOR ALL TIME RECORDS

Time of incident: ☐☐☐☐ **Date of incident**: ☐☐/☐☐/☐☐☐☐

Time incident reported to dispatcher: ☐☐☐☐, **Time of call to dispatch ISU**:☐☐☐☐

Time ISU dispatched: ☐☐☐☐ **Arrival time of ISU at incident**: ☐☐☐☐

Time incident cleared from running lanes (not hardshoulder): ☐☐☐☐

Time ISU left site: ☐☐☐☐

Please note: You only need fill in the times appropriate e.g. if you find the incident proactively there will be no dispatch time.

Other responders:	**Arrival Time**	**Departure time**
Traffic Officer…….	☐☐☐☐	☐☐☐☐
Police.. ……..	☐☐☐☐	☐☐☐☐
Another ISU……..	☐☐☐☐	☐☐☐☐
Motoring Service.	☐☐☐☐	☐☐☐☐

Comments:

Visibility;….. ……. Clear ☐, 500m to 1000m ☐, 100m to 500m ☐, less than 100m ☐
(Tick as appropriate) Light ☐, Dark, lit with streetlights ☐, Dark, with no, or unlit,lights☐
Affected by low sun ☐

Precipitation;……None ☐, Rain ☐, Snow ☐, Hailstone ☐, Sleet ☐

Road Conditions;...Dry ☐, Wet ☐, Slush ☐, Snow covered ☐, Icy ☐

Wind;……..None ☐, Light ☐, Moderate ☐, Severe ☐, Gusty ☐

Incident in Lane(s)*(tick as appropriate)*H/S☐, 1 ☐, 2 ☐, 3 ☐, 4 ☐, 5 ☐, 6 ☐, 7 ☐

Lane(s) affected*(tick as appropriate)*…H/S☐, 1 ☐, 2 ☐, 3 ☐, 4 ☐, 5 ☐, 6 ☐, 7 ☐

Effect on traffic flow in direction of incident (slow/static vehicles for):
Less than ½ a mile ☐, ½ mile to 1 mile ☐, 1 mile to 3 miles ☐, great than 3 miles ☐

Estimated time to clear slow/static vehicles in direction of incident
No time to clear ☐, Up to 15 minutes ☐, 15 to 60 minutes ☐, over 1 hour ☐

Length of queue on opposite carriageway/lane
None ☐, less than 1 mile ☐, 1 to 3 miles ☐, over 3 miles ☐, Unsure ☐

Number of cars involved..... ☐☐
Number of vans involved…… ☐☐
Number of LGV involved……..... ☐☐
Number of HGV involved……... ☐☐
Number of PSV involved…… ☐☐
Number of cranes involved…… ☐☐
Number of abnormal loads involved.. ☐☐
Number of motorcycles involved……. ☐☐
Number of cycles involved…… ☐☐
Number of pedestrians involved…….. ☐☐
Other …..

Nature of incident
Debris ☐ - go to **Debris Details**
Vehicle Incident (VI) ☐ - go to **Type of VI**
Flood……. ☐
Subsidence. ☐
Abandoned vehicle ☐
Other ☐ (state below)

Please tick here ☐ if details were provided by another authority e.g. police
Please tick here ☐ if HAZCHEM is involved

Debris Details *Please describe the item in the Comments box.*
HGV/LGV strap ☐, HGV/LGV tyre ☐, HGV/LGV lorry part ☐
car tyre ☐, car part ☐, wood ☐, dead animal ☐, mud ☐
burnt out vehicle ☐, Fuel spill ☐, Other ☐ (state below)

Comments:

Type of VI Collision ☐, fire ☐, breakdown ☐, other ☐ (state below)

Cause (if known) Mechanical failure ☐, road conditions ☐, abnormal load ☐
apparent over height/weight/length vehicle ☐ Other ☐ (state below)

Was the network damaged:..**Yes** ☐, **No** ☐ (If yes please tick appropriate boxes below)
safety barrier ☐, surfacing ☐, structure ☐, lighting column ☐
cabinet ☐, signals ☐, signage ☐, emergency roadside telephone ☐
Fence ☐, Other ☐ (please state below)

GUIDANCE NOTE FOR COMPLETION OF INCIDENT SUPPORT UNIT (ISU) INCIDENT DATA CAPTURE SHEET (Version 1.0)

1. Introduction

This guidance describe the information to be recorded concerning incidents attended by ISUs on the Highways Agency strategic road network and the accompanying Incident Support Unit (ISU)-Incident Data Capture Sheet (IDCS) must be completed.

The information collected on the IDCS is designed to aid consideration and development of current and future practices and methodologies for dealing with incidents.

The collection of information on an ISU's day-in-day-out involvement with incidents will allow a fuller understanding and appreciation of the magnitude of incident management. It is therefore highly important that the IDCS be completed and submitted as stated in **3. Reporting and Performance Monitoring** of this Guidance.

2. General

It is recognised that ISUs are not always the first attendee to an incident. In these circumstances the ISU must record the information they are aware of. This means that only those facts that are known to the ISU, or can be accurately provided by others, for example from the other attendee(s) or the Regional Control Centre (RCC) or Network Control Centre (NCC), can be recorded. Where information cannot be obtained, the appropriate boxes should be left blank and comment made in the comments box where appropriate.

Some ISUs may also be called to attend an incident by another ISU crew to provide assistance or address specialist roles. In these situations the action of the second ISU must be recorded as if they were attending an incident. Therefore the RCC reference and the time of the incident must be obtained from the first ISU and the rest of the document filled in as if it was a separate call out.

The data captured may be available under Freedom of Information.

3. Reporting and Performance Monitoring

The ISU-IDCS must be completed for every incident at the time of the incident.

Each month the completed ISU-IDCSs must be submitted to the HA in an electronic comma separated value (CSV) format. Please note that the tilde (~) character must be used as the delimiter for the attributes, which are described in **5. ISU Data Attributes**.

The data must be virus checked and sent by e-mail to the following address on the last working day of every month: ISU-IDCS@Highways.GSI.Gov.UK

The e-mail subject description must be the name of the attached file. Note that if a file exceeds 5Mb then it must be divided into smaller files (ensuring that incident data records are not split) and each file e-mailed separately to the HA.

The body of the e-mail must contain the following transmission details:

- Originating Organisation
- Contact Name
- Contact Telephone Number

- Date virus check carried out

The naming of the data files must follow the convention set out below:

ISU_IDCS_<Supplier Identifier>_<Date>_<Number>_OF_<Total>.CSV

<Supplier Identifier>	This identifier will be supplied by the HA – contact the Agency's IT help/service desk facility known as Service Direct (0113 2541140)
<Date>	The Date that the file is submitted. This must be in the format YYYMMDD
<Number>	The sequential part number of the submission
<Total>	The total number of parts comprising the submission

An example of such a file name would be: ISU-IDCS_MAC16_2006-08-07_1_OF_1.CSV

The HA must process the data and provide an automated response indicating whether the data was successfully loaded. If the response indicates that the processing was unsuccessful then contact Service Direct as soon as possible.

4. Completing the ISU Data Capture Sheet

The IDCS is split in to seven separate boxed sections. Each section deals with a different aspect of an incident. The first five sections must be filled in as completely as possible. The two remaining sections are completed depending on Section 5.

Section 1

The first section of the data sheet is mainly concerned with recording the location of the incident. This section must be fully completed. The information required should be readily available or known to the ISU operatives.

After completing the Service Provider Incident Reference number and type of ISU attending, the section asks for the road the incident is on and to identify if it is motorway or trunk road. When dealing with road designations such as A1(M), both motorway and trunk road boxes must be ticked. If the road has a standard motorway or trunk road designation, only one of these boxes must be ticked.

The secondary road of an incident refers to incidents that occur at junctions. If the incident happened on a HA road at a junction, this is the primary road and will already have been filled in earlier in this section. The secondary road is then the name of the other road at the junction. Where there are more than two roads at a junction, the first is always a HA road and the second must always be the next major road or the one from which any car involved in the incident came from if this can be positively determined and is one of those at the junction in question. Should the incident have started on a none-HA road and come to be on a HA road, either as a consequence of skidding or being shunted/falling on to it, the primary road must always be the HA road. The secondary road would be the one where the incident originated, leading to the effect on the HA network.

The direction of travel relates to the primary direction in which the main vehicle, or in the case of debris the direction of the lane(s) in which it comes to rest, is heading. This must be related to the standard accepted local directions for the network. Under this referencing the M18 runs north-

south, although some sections are known to run almost east-west, the general accepted direction given is northbound or southbound.

The incident must be classed as being within roadworks if it is between the first cone of the lead taper and the Roadworks End sign.

The last part of Section 1 requires at least one box to be completed. The system for referencing the Highways Agency's network is not yet fully consistent from one type of road to the next, or from one area to the next. Therefore the most accurate detail should be recorded. It is not necessary to attempt to complete every box in this section.

Section 2

The second section of the sheet is related to when an incident has occurred and when it is addressed.

The date must be entered as the date/month/year, e.g. 02/12/2005. The remainder of the section refers to the times involved in the handling of the incident. These must be filled in using the 24 hour clock, e.g. 0713, 1452.
There will be occasions when the data in this section cannot be fully completed. Examples of this are when an ISU proactively finds an incident, resulting in there being no dispatch information, or where the ISU is the second ISU at an incident or is in attendance after some of the other responders.

In the cases where an ISU cannot supply all the details of the times, those details that are known must be completed as fully and accurately as possible. Therefore in the example of being the second ISU at an incident, the time of the incident can be obtained via the dispatcher, the dispatch time is known, arrival time is known and the time of clearing the incident may be known from the first ISU if they are not on site when it is cleared. The time of the other responders must be noted as best as possible.

The comments section allows the ISU attendees to record anything of merit. If times were obtained from other parties, this can be recorded here. If an attendee arrives then just leaves for an unknown reason, this can also be recorded. Any valid comment can be entered.

Section 3

The third section of the sheet is associated with the immediate weather and road conditions at the time of the incident.

Under visibility, the distance that vision is practical must be recorded. This is not precise and is to be the best estimate of the ISU team. However, good guides to restricted visibility in fog or heavy rain/spray conditions may be the number of marker posts or lamp columns that can be seen. The next section of visibility relates to whether it is daylight, or night time with or without street lighting, and must be filled in as well as the visibility.

Precipitation, road condition and wind must record the condition at the time of the incident. If the time that has elapsed between the incident and the ISU arrival is significant, and conditions might have changed within that time, the conditions at the time of attendance must be recorded.

Section 4

Section 4 is highly useful for determination of the effect of incidents in various lanes.

This section must be completed as fully and accurately as possible. However, it is recognised that some of the information requested is subjective and may not always be available. Every effort must be made to complete this section though.

Where an ISU is the second ISU to an incident and has potentially been requested to undertake a specialist role, e.g. repairing barrier damage, the first two questions in this section must be completed with the information from the first ISU.

When an incident occurs there is the possibility of traffic slowing or queuing on the same carriageway. If this happens a record must be made of the approximate length of the slow moving or queuing traffic. The queue can be seen in some circumstances, but in others, where the queue is long or trails around a corner or over a hill, then information from other attendees should be used if it is known, or an estimate based on knowledge of the circumstances should be made.

If slow moving traffic or a queue builds up behind the incident, local knowledge and experience would allow an approximation to be made of how long it might take to clear the effect of the incident. This is highly subjective but must be entered as thoughtfully as possible.

The effect of the incident on the opposite carriageway must be the maximum observed queue whilst the ISU deals with, or leaves the incident. Therefore if there are two ISUs, one of which has just been called to repair safety barrier damage, then the first ISU to leave may record one queue length, the second ISU a different length as its works go on longer and potentially have a different effect on traffic.

The first two questions must be completed for every incident.

Section 5

This section is targeted at identifying the nature of the incident and the nature of any vehicles if involved. It is split essentially in to two sub-sections; vehicle numbers and type of incident.

Where the number of each type of vehicle involved in an incident is known, this must be entered on to the sheet. However, the ISU crew is not required to approach the exact scene of an incident to collect this data where it may be inappropriate to do so. Examples of incidents where it may not be appropriate or practical to obtain details about vehicles are when HAZCHEM is involved or the police are leading an incident and have set up an exclusion zone in either instance. On occasions where the data cannot be obtained first hand, it is feasible that the other attendees may be able to provide the details. This may involve discussion with the police or other emergency services. When the details have been provided by others, the details must be entered on to the sheet and the sentence concerning data being provided by other authorities must be ticked. If HAZCHEM is involved, regardless of how this fact has been determined, it must be noted in the appropriate location.

The “Nature of Incident” sub-section must be completed by filling the box that most adequately reflects the nature of the incident.

If an ISU has been called to attend a location to remove debris, or removes debris without a call to request this, then the Debris box must be completed. If the ISU attends an incident where one or more vehicles have been involved, and this is purely related to the action of the vehicles and not that they have been caught up in a different issue, then the vehicle incident (VI) box must be completed.

If the carriageway has flooded, or has sufficient standing water to potentially cause difficulties for vehicles, then the Flood box must be completed. If there are vehicles standing in the water, or

have collided as a result of the water, then this must still be recorded as a Flood, but the "Type of VI", Section 6, must also be completed.

Section 6

This section is only to be completed if the incident is debris related.

A lot of debris is removed from the highway during the course of a day. The debris can range from a lorry straps to settees. It is important to understand what is being removed from our network to identify if there are any issue with littering in areas or potential health and safety concerns.

The type of debris removed should seek to identify all the debris. More than one tick box can be ticked if appropriate. If the debris is very varied then appropriate boxes must be ticked and the remainder covered in the Comments section.

Under the comments section the ISU crew must seek to describe the debris in nature and size. Therefore if a lorry tyre part is removed, the tick box for this is checked and an example of the entry in the Comments box would be '4 foot by 2 foot, approx 7kg'. If a dead animal was removed the Comments box might be filled as 'full grown deer'.

Section 7

This section must be completed if the incident involves vehicles by either being the incident or having been caught up in one, e.g. flooding, and relates to the type of vehicle incident attended if vehicles are involved.

This section must be completed as fully as is practical. However, we do not wish anyone to be subjected to questioning to gain the information.

Therefore the details entered here are likely to be those readily and easily discernable to the ISU crew, or to have been obtained from the normal course of asking if people are okay after an incident. Details must not be obtained by directly asking those in an incident.

Under "Type of VI", only one box must be ticked, with comments provided where required.

Under "Cause", only one box must be ticked. This part of Section 7 is subjective. However, there are some incidents where it is apparent that something has been a major contributory factor to an incident e.g. the height of a vehicle should it have hit the underside of a structure.

Under "Was the network damaged", the response is yes or no. If damage was caused all the identified damaged elements must be ticked. This may mean more than one box is ticked if damage was caused.

5. ISU Data Attributes

ISU Data Attributes

	Attribute Name	**Attribute Description**
1.1	**SVCPROVREF**	Service Provider Reference number
1.2	**ISU_TYPE**	ISU Type attending

1 Motorcycle
2 Car
3 Van
4 Truck

1.3 **RD_CLASS** Road Class

1 Motorway
2 All Purpose Trunk road

	Attribute Name	**Attribute Description**
1.4	**1ST_RDNO**	1st Road Number
1.5	**RD_TYPE**	Road Type

1 Single Carriageway 2 lane
2 Dual Carriageway 2 lane
3 Dual Carriageway 3 lane
4 Dual Carriageway 4 lane
5 Other

1.6 **JNCT_TYP** Junction Type
1 Main Line
2 Entry Slip Road
3 Exit Slip Road
4 Junction

1.7 **JNCT_NO** Junction Number

1.8 **2ND_RDNO** 2nd Road Number

1.9 **DIR_TRAVEL** Direction of Travel of Incident
1 North
2 South
3 East
4 West
5 Clockwise
6 Anti-Clockwise
7 Roundabout

1.10 **RD_WORKS** Roadworks

1.11 **INC_LOC_OSGR** Incident Location OSGRs

1.12 **INC_LOC_MRKR** Incident Location Marker Post

1.13 **INC_LOC_EMERG** Incident Location Emergency Roadside Tel.

1.14 **INC_LOC_LAMP** Incident Location Lamp Post Reference

1.15 **INC_LOC_OTHER** Incident Location Other

TIME OF DAY

1.16 **INC_TIME_HR** Hour of Incident

1.17	**INC_TIME_MIN**	Minutes of Incident
	Attribute Name	**Attribute Description**

ACCIDENT DATE

1.18	**ACC_DATE**	Accident Date
1.19	**INC_TIME_REP**	Time Incident Reported to Despatcher
1.20	**CALL_TIME_DISP**	Time of Call to Dispatch ISU
1.21	**TIME_DISP**	Time ISU Dispatched
1.22	**ARRIV_INC**	Arrival Time of ISU at Incident
1.23	**TIME_INC_CLEAR**	Time Incident Cleared from Running Lanes
1.24	**TIME_LEFT**	Time ISU Left Site
1.25	**TO_ARRIV**	Traffic Officer Arrival Time
1.26	**TO_DEPART**	Traffic Officer Departure Time
1.27	**POL_ARRIV**	Police Arrival Time
1.28	**POL_DEPART**	Police Departure Time
1.29	**OTH_ISU_ARRIV**	Other ISU Arrival Time
1.30	**OTH_ISU_DEPART**	Other ISU Departure Time
1.31	**MOT_SRV_ARRIV**	Motoring Service Arrival Time
1.32	**MOT_SRV_DEPART**	Motoring Service Departure Time
1.33	**ARR_DEP_COMMENTS**	Arrival and Departure Comments
1.34	**VISIB_COND**	Visibility

1 Clear
2 500m to 1000m
3 100m to 500m
4 Less than 100m

1.35 **LIGHT_COND** Lighting

1 Light
2 Dark, lit with streetlights
3 Dark, with no, or unlit, lights
4 Affected by low sun

	Attribute Name	**Attribute Description**
1.36	**PRECIP_COND**	Precipitation

1 None
2 Rain
3 Snow
4 Hailstone

5 Sleet

1.37 **ROAD_COND** Road Conditions
1 Dry
2 Wet
3 Slush
4 Snow covered
5 Icy

1.38 **WIND_COND** Wind Conditions
1 None
2 Light
3 Moderate
4 Severe
5 Gusty

INCIDENTS IN LANE

1.39 **INC_LANE_HS** Incident in Hard-Shoulder

1.40 **INC_LANE_1** Incident in Lane 1

1.41 **INC_LANE_2** Incident in Lane 2

1.42 **INC_LANE_3** Incident in Lane 3

1.43 **INC_LANE_4** Incident in Lane 4

1.44 **INC_LANE_5** Incident in Lane 5

1.45 **INC_LANE_6** Incident in Lane 6

1.46 **INC_LANE_7** Incident in Lane 7

LANE(S) AFFECTED

1.47 **LANE_EFFECT_HS** Lane affected – Hard-Shoulder

1.48 **LANE_AFFECT_1** Lane affected 1

1.49 **LANE_AFFECT_2** Lane affected 2
Attribute Name **Attribute Description**

1.50 **LANE_AFFECT_3** Lane affected 3

1.51 **LANE_AFFECT_4** Lane affected 4

1.52 **LANE_AFFECT_5** Lane affected 5

1.53 **LANE_AFFECT_6** Lane affected 6

1.54 **LANE_AFFECT_7** Lane affected 7

1.55 **TRAF_EFFECT** Effect on Traffic Flow in Direction of Incident
1 Less than 0.5 mile
2 0.5 mile to 1 mile

3 1 mile to 3 miles
4 Greater than 3 miles

1.56 **EST_TIME_CLEAR** Estimated time to Clear Slow/static vehicles in Direction of Incident

1 No time to Clear
2 Up to 15 mins
3 15 to 60 mins
4 Over 1 hour

1.57 **LENGTH_QUEUE_OPP** Length of Queue on Opposite Carriageway/Lane

1 None
2 Less than 1 mile
3 1 mile to 3 miles
4 Over 3 miles
5 Unsure

1.58 **NO_OF_CARS** Number of Cars involved

1.59 **NO_OF_VANS** Number of Vans involved

1.60 **NO_OF_LGV** Number of LGV involved

1.61 **NO_OF_HGV** Number of HGV involved

1.62 **NO_OF_PSV** Number of PSV involved

1.63 **NO_OF_CRANES** Number of Cranes involved

1.64 **NO_OF_ABNORMAL** Number of Abnormal loads involved

1.65 **NO_OF_MCYCLES** Number of Motorcycles involved

Attribute Name **Attribute Description**

1.66 **NO_OF_CYCLES** Number of Cycles involved

1.67 **NO_OF_PED** Number of Pedestrians involved

1.68 **OTHER_VEH** Other vehicle categories involved

1.69 **INC_NATURE** Nature of Incident

1 Debris
2 Vehicle Incident
3 Flood
4 Subsidence
5 Abandoned vehicle

1.70 **INC_NATURE_OTH** Other nature of Incident

1.71 **DETS_PROV_OTH_AUTH** Details provided by another authority (eg Police)

1 Yes
2 No

1.72 **HAZCHEM** Hazchem involved

1 Yes
2 No

1.73 **DEBRIS_DET** Debris details
1 HGV/LGV Strap
2 HGV/LGV Tyre
3 HGV/LGV Lorry Part
4 Car Tyre
5 Car Part
6 Wood
7 Dead Animal
8 Mud
9 Burnt Out Vehicle
10 Fuel Spill

1.74 **DEBRIS_DET_OTH** Details of Other Debris

1.75 **VEH_INC_DET** Vehicle Incident Details
1 Collision
2 Fire
3 Breakdown

1.76 **VEH_INC_DET_OTH** Details of Other Vehicle Incident

Attribute Name **Attribute Description**

1.77 **INC_CAUSE** Incident Cause
1 Mechanical Failure
2 Road Conditions
3 Abnormal Load
4 Apparent Over height/ weight/length Vehicle

1.78 **INC_CAUSE_OTH** Details of Other Incident Cause

1.79 **NETWORK_DAM** Was the Network Damaged?
1 Yes
2 No

1.80 **NETWORK_DAM_DET** Network Damage Details
1 Safety Barrier
2 Surfacing
3 Structure
4 Lighting Column
5 Cabinet
6 Signals
7 Signage
8 Emergency Roadside Telephone
9 Fence

1.81 **NETWORK_DAM_DET_OTH** Details of Other Network Damage

ISU File Record Layout

Variable	Variable Description	Character Position	Data Type Integer/Alpha
1.1	SVCPROVREF	1-10	A
1.2	ISU_TYPE	11	I
1.3	RD_CLASS	12	I
1.4	1ST_RDNO	13-16	I
1.5	RD_TYPE	17	I
1.6	JNCT_TYP	18	I
1.7	JNCT_NO	19-20	I
1.8	2ND_RDNO	21-24	I
1.9	DIR_TRAVEL	25	I
1.1	RD_WORKS	26	I
1.11	INC_LOC_OSGR	27-32	A
1.12	INC_LOC_MRKR	33-47	A
1.13	INC_LOC_EMERG	48-62	A
1.14	INC_LOC_LAMP	63-77	A
1.15	INC_LOC_OTHER	78-107	A
1.16	INC_TIME_HR	108-109	I
1.17	INC_TIME_MIN	110-111	I
1.18	ACC_DATE	112-119	A
1.19	INC_TIME_REP	120-123	A
1.2	CALL_TIME_DISP	124-127	A
1.21	TIME_DISP	128-131	A
1.22	ARRIV_INC	132-135	A
1.23	TIME_INC_CLEAR	136-139	A
1.24	TIME_LEFT	140-143	A
1.25	TO_ARRIV	144-147	A
1.26	TO_DEPART	148-151	A
1.27	POL_ARRIV	152-155	A
1.28	POL_DEPART	156-159	A
1.29	OTH_ISU_ARRIV	160-163	A
1.3	OTH_ISU_DEPART	164-167	A
1.31	MOT_SRV_ARRIV	168-171	A
1.32	MOT_SRV_DEPART	172-175	A
1.33	ARR_DEP_COMMENTS	176-225	A
1.34	VISIB_COND	226	I
1.35	LIGHT_COND	227	I
1.36	PRECIP_COND	228	I
1.37	ROAD_COND	229	I
1.38	WIND_COND	230	I
1.39	INC_LANE_HS	231	I
1.40	INC_LANE_1	232	I
1.41	INC_LANE_2	233	I
1.42	INC_LANE_3	234	I
1.43	INC_LANE_4	235	I
1.44	INC_LANE_5	236	I

Annex 7.8.11 Standard Incident Management Framework

Contents

Why do we need a Standard Incident Management Plan?

The Highways Agency, as an Executive Agency of the Department for Transport, is responsible for managing, maintaining and operating the strategic road network of England, which includes all motorways and a significant proportion of trunk roads. In the case of a 'National Incident' under the Civil Contingencies Act 2004 as a Category 2 Responder it becomes involved with any 'incident' that adversely affects or disrupts the normal operation and availability of the strategic road network. These include incidents involving vehicles and such things as terrorist threats/activity, demonstrations on the roads or severe weather.
The business objectives of the Highways Agency that relate to Incident Management are:

- Improving road safety.
- Reducing congestion and improving reliability on the strategic road network through:
  - A programme of improvements to the strategic road network,
  - Improved management of incidents and roadworks,
  - Influencing travel behaviour through better information to inform journey choices.

The Public Service Agreement (PSA) targets for the Highways Agency that relate to Incident Management are:

- By 2007-08, make journeys more reliable on the strategic road network.
- Reduce the number of people killed or seriously injured in Great Britain in road accidents by 40% and the number of children killed or seriously injured by 50%, by 2010 compared with the average for 1994-98, tackling the significantly higher incidence in disadvantaged communities.

As such, the Agency has certain functions, objectives and responsibilities to fulfil. To do this will, on numerous occasions, mean working with other agencies. Consequently, there is a clear need for the Agency to have in place an effective and efficient standardised Command and Control system. This system must enable co-ordinated and cohesive working and be compatible with the Emergency Services and other responder organisations.

Highways Agency Traffic Officer Service

The Traffic Officer Service and Incident Support Units are the visible presence of the Agency on the strategic road network and in particular the motorways. The Traffic Officer Service is key to enabling successful working partnerships with the police service, the fire service, the ambulance service and other agencies who provide a response to incidents and events on the road network. It provides the Agency's first response to incidents or events through requests for service, to Regional Control Centres, Traffic Officer Service patrols and through the Highways Agency's service providers.

Components of the Standard Incident Management Plan

The Agency's Standard Incident Management Plan consists of three parts:

Standard Incident Management Plan	Framework Document	Strategic overview of the Agency's Incident Command and Control Co-ordination Structures and Systems	Strategic
	Guidance Document	Defines clear functions and responsibilities of all those involved in managing or supporting those managing an incident	Tactical
	'The Way We Work' manuals	Detailed "Process Instructions" on how to carry out specific tasks	Operational

This framework is applicable to and compatible with the Agency's Area/Regional Contingency Plans and the National Crisis Management Plan.

The Traffic Officer Service is only one of a number of service functions that the Agency has at its disposal. The plan includes descriptions, responsibilities and accountabilities for all functions throughout the Agency that can contribute to the resolution of an incident. However, the initial focus is on the Traffic Officer Service.

Standard Incident Management Plan

Framework Document Strategic overview of the Agency's Incident Command and Control Co-ordination Structures and Systems Strategic

Guidance Document Defines clear functions and responsibilities of all those involved in managing or supporting those managing an incident Tactical

'The Way We Work' manuals Detailed "Process Instructions" on how to carry out specific task Operational

Gold/Silver/Bronze Incident Command Structure

The Agency will employ the standard Gold, Silver and Bronze Command of incidents in line with the Police and other emergency services. Incidents are escalated by the existing Commander to the next level when they require additional resources or coordination.

Incidents should be commanded at the lowest level where the Commander has the authority, competencies and resources to resolve the incident.

Recent reviews and analysis of operational incidents involving the Agency have highlighted the need for the Agency to work in a disciplined, co-ordinated and controlled manner under the Command and Control of a clearly defined Agency Incident Commander to bring about an effective resolution to the incident and achieve the Agency's objectives and PSA targets. Thus there is a need for a Standard Incident Management Framework (SIMF).

Bronze	Operational Commander at incident
Silver	Tactical Commander
Gold	Strategic Commander
Gold Coordinator	Coordinates strategy across the Highways Agency

Context of the Standard Incident Management Framework

The Highways Agency Standard Incident Management Plan is a compilation of practices and procedures based on legislation, agreement, experience and good practice. The Agency recognises that the emergency services will take the lead at many incidents, and seeks to offer them support.

To achieve compatibility and thereby alleviate the potential for confusion between and within the various response agencies, the procedures, terminology and documentation contained within this document have been standardised wherever possible. The framework will share common terminology with other responder organisations, which will be adopted throughout the Agency and by its service providers to avoid misunderstandings.

There is an obvious expectation that all Agency activities will be conducted reasonably and within the bounds of the law.

The legal parameters within which the Agency operates are encompassed within:

1. UK Domestic Law including
   - The Highways Act 1980
   - Traffic Management Act 2004
   - Civil Contingencies Act 2004
   - Data Protection Act 1998
   - Human Rights Act 1998
   - Control of Substances Hazardous to Health Regulations 1994
   - Health & Safety at Work Act 1974 and related regulations

2. International law, specifically the provisions of the European Convention of Human Rights (ECHR).

During the development of this framework, consideration has been given to the compatibility of the processes and related procedures with the Human Rights Act. Particular attention has been given to the legal basis of its precepts, the legitimacy of its aims; the justification and proportionality of the actions intended by it, that it is the least intrusive and damaging option necessary to achieve the aims, and that it defines the need to document the relevant decision making processes and outcomes of action.

This framework is a living document and will be maintained by the Agency. The need to ensure an inclusive approach to the delivery of the service is of paramount importance. To this end it will be published on the Agency's intranet and formally reviewed on a regular basis. However, it is

intended that amendments will be posted as necessary on the Agency intranet (Way we Work site).

Enquiries regarding the content of this document should be emailed to: **SIMF@highways.gsi.gov.uk**

Command, Control, Co-ordination

Central to any plan is the system of operational decision-making and control. There are two main activities concerned with command and control of an incident and these must be seamlessly combined if command is to be effectively exercised. They are:

- The command system for the execution of decisions and the carrying out of operational plans.

- The support system (support and supply functions) - the collation and dissemination of information, the co-ordination of human resources, the identification of equipment and the creation of plans and options. These support requirements, in different proportions, are common regardless of incident type and provide the context in which to make decisions.
- Two principles that are at the centre of an effective approach are that:
- Common terms and command structures are used
- These terms and command structures should fit normal working practices and reinforce recognised methods.

In this context:

Command means the authority for an organisation to direct the actions of its own resources (both personnel and equipment).

Control means the authority to direct strategic and tactical operations in order to complete an assigned function. It includes the ability to direct the activities of other agencies engaged in the completion of that function. The control of an assigned function also carries with it a responsibility for the health and safety of those involved.

Co-ordination means the harmonious integration of the expertise of all the agencies both internally and externally with the objective of effectively and efficiently bringing an incident to a successful resolution.

In the case of the Agency the Regional Control Centres are at the centre of this framework. They work with other responder organisation control centres engaged in resolving the incident. They must be capable of using and activating a command system with a support system that complements the normal method of incident response when required.

Where the scale, volume, intensity or duration of some scenarios is beyond the capacity of a single Agency operating base or region, a set of common procedures is set out in the Agency's National Crisis Plan. This will ensure that command is cohesive and resources are harnessed, co-ordinated and organised with purpose. The response to such scenarios must be such that it can withstand significant scrutiny at a later date.

SIMF is equally applicable to police-led, other service-led or Agency-led incidents as indicated in the National Guidance Framework for the Traffic Officer Service and the Guidance on Policing Motorways.

Principles of Incident Command

The principles contained within this document are fundamental to the command and resolution of any incident no matter how serious and no matter the grade or level of the person in command.

Effective command requires the provision of administration and support functions to extend the thinking of the Commander. It also requires a regime, a disciplined organisation of people and systems in which the function holders are empowered to execute strategy and deploy resources.

The exercise of command is always situational. Command is not, however, merely a mechanical response. The SIMF places the Incident Commander in a position to exercise control, but command at any level also involves leadership and perspective. An Incident Commander must balance competing demands in a complex environment and, because of these complexities and their accountability, they will find it advantageous to operate according to a set of command principles.

Incident Command has four critical elements. These are:

- Decisions being made by those empowered to do so and from those decisions, instructions being distributed.
- A climate supporting effective decision making being created.
- A level of competence being in place, i.e. that the Incident Commander will be versed in the general rules embodied in professional good practices.
- An established command and incident management structure within each Agency region.

An Incident Commander can depart from the general rules provided that they do so from a position of full knowledge of the prevailing circumstances, and can justify their decision to do so through a Dynamic Risk Assessment. The Incident Commander should document any departure from the general rules.

Command is also about delegation. The more tactical the decision, the more local the decision-making will need to be. Plans at the highest level should always be of a general nature and focus on the mobilisation of information and resources to enable local Commanders to achieve a given aim. Tactical deployment to achieve that aim is usually devolved to those with the most immediate knowledge and sufficient resources to deal with the situation. For example, winter weather initiatives have a national strategy, tactically developed in more detail in the regions and areas and operationally detailed at the local depots.

In this context, command is a descending structure. At the highest levels the plan is general. At each level of authority beneath this, the decisions become progressively more specific.

The decision maker should be in a position to have an overview and perspective of the entire scene of operations within their command, and control of sufficient resources to achieve their aim.
Command at any level assumes responsibility for everything that occurs beneath. Vicarious liability of this sort is a serious responsibility. Commanders may rightly seek assurance that what is happening within their sphere of responsibility but out of their view is being dealt with appropriately. To this end, Commanders should, as necessary, become mobile and make personal assessments both of the situation and the ability of subsidiary Commanders. **They do this to make a first-hand assessment, NOT to take over responsibility.**

If subsidiary command is not coping it may be because they are inadequately supported and the Senior Commander may provide more resources. If they are not coping because they are not capable or have become exhausted then they should be replaced. The Senior Commander

should intervene in this way, but not by taking the decisions associated with the position they are observing.

In the event that the Gold Commander departs the location of Gold Command, generally the Gold Support Lead (see page 27) will assume their seat. The Support Lead will of course be in direct contact with the Gold Commander and should sustain communication links at all times. This principal also applies to the Silver Commander.

If too rigid a view is taken about the distinctions between Gold, Silver and Bronze roles, command develops a bunker mentality - Senior Commanders become merely logistics officers and remote from critical decisions. The art of command is to achieve the appropriate balance between maintaining the strategic control associated with the position, but being on hand enough to assess and influence the performance of subsidiary Commanders. No matter how successful an intelligence system is, there is often no substitute for the Commander taking a close-up view of critical zones of activity and to intervene directly in bottlenecks where necessary.

Overall the Commander has to be decisive but sufficiently light of touch to encourage situational leadership. The development of strategy implies the choice of a plan. The implementation of a plan requires the issue of instructions. Instructions should be succinct, unambiguous and clear about the flexibility allowed. As familiarity can vary as much as circumstances, the level of intervention Senior Commanders should make will depend on the situation. A Commander familiar with his or her Silver and Bronze Commanders will need to spend less time seeking assurance. Where that familiarity and knowledge does not exist, the Commander and subsidiary Commanders will gain reassurance from more frequent contact until a proper rapport is established.

Commanders should be precise about the aims, delegate the means to carry them out, and satisfy themselves that things are working by whatever suitable means.

Objectives of Incident Command

The specific objectives of the Agency and it's service providers in the management of incidents are:

- restoring the network to normal conditions as quickly as possible,
- minimising the effect of an incident on the travelling public
- providing information to road users, management and Ministers.

Common objectives

In addition to the specific objectives of the Agency, all the organisations involved in the management of an incident will work to the following common objectives set out in the Civil Contingencies
Act 2004:

- 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
- facilitating investigations and inquiries
- promoting self help and recovery

- restoring normality as soon as possible
- evaluating the response and identifying lessons to be learned

Incident Resolution and Risk

The handling of any incident requires a strategy for resolution. The more serious the incident, the greater the assumption that things could go wrong. The situation carries risks and the Incident Commander's objective is to bring a difficult situation under control. **The primary thought should be one of efficient resolution**.

The issue of risk is central to decision making. There is a danger that estimating risk produces risk-averse Incident Commanders. This condition is made worse by the expectation of subsequent reviews and tribunals operating in opinionated conditions and with the wisdom of hindsight.

The concept of assessing risks should, lead to risk management, not to risk aversion. Risk assessment, particularly at command level, is comprehensive. That is to say the full range of hazards should always be considered and the necessary control measures evaluated in terms of reasonableness and practicality. It is recognised that everyone involved in the incident is potentially exposed to the risk arising from these hazards.

Efficient resolution is based on obtaining a balance between a number of considerations:

- Safety of members of the public;
- Safety of Responders;
- Earliest reasonable resolution;
- Impact of prolonged situation on the public, including congestion and
- Most efficient resource use.

Efficient resolution can only be achieved by balancing risks

Recording of Commander's Decisions (Decision Logs)

The handling of any incident will require the Commander to decide the strategy and the overall objectives for resolving that incident. The most appropriate tactics and operational methods for achieving the strategy and objectives will then need to be considered and decided upon from a range of possible tactics. This involves making balanced judgements which are reasonable in the circumstances.

Incident Commanders must record their decisions and the reasons on which they are based. The dimensions are time (and thereby disruption), resource (the greater the resource deployment the less available those resources are for other incidents) and opportunity (options for intervention). Decisions must be based on an assessment of whether the options for intervention are convincing. They should also take account of Human Rights in the areas of proportionality, legality, necessity and intrusiveness.

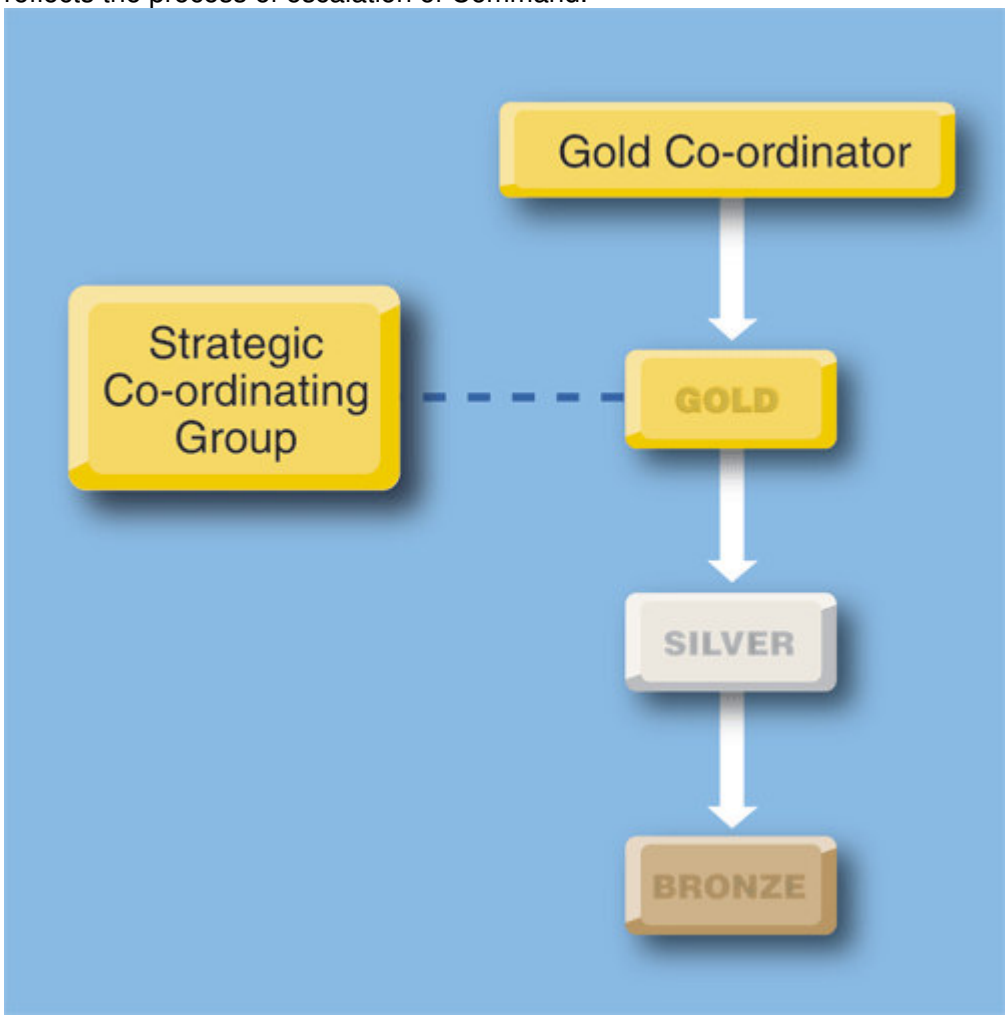
These options should consider the impact of dislocation and disruption and calculate the cost and availability of resources, setting these things against the likelihood of real physical risk to victims or responders. This will be a record of their strategy for resolution.

The Command System

The purpose of this section is to outline the first element of the regime. This is the Command System. This is based on the Gold/Silver/Bronze levels of command which correspond directly to the three levels of incident management recommended to all response organisations, i.e. GOLD

= Strategic, SILVER = Tactical & BRONZE = Operational. It also acknowledges the "Gold Co-ordinator" level. These levels are not in their own right rank-specific but invariably they will reflect the level of responsibility, experience, capability and empowerment that the role holder has within their organisation in dealing with the incident.

At the start of any incident for which there has been no warning the operational level will usually be activated first, with the other levels, tactical and strategic, being established with the escalation of the incident, or a greater awareness of the situation. It is possible that in some incidents, particularly those where there is a threat of a potentially serious problem, the activation of the three levels will be concurrent. Consequently this section is presented in a manner that reflects the process of escalation of Command.



Incident commanders line of command

Bronze

Bronze can be summarised as a level of operational deployment, reporting to Silver (when established) with a responsibility to carry out a particular plan or set of duties. There may be more than one Bronze depending on the scale of the incident (e.g. multiple scenes).

This level reflects the normal day-to-day arrangements for responding to smaller scale incidents. It is the level at which the management of 'hands-on' work is undertaken at the individual site.

Where the scale of the incident is such that resources needed are outside of the Bronze Commander's sphere of responsibility, an early requirement will be to consider whether circumstances warrant escalating by setting up a tactical (Silver) level of management.

The first Agency visible representation at the scene of an event will usually take on the function of Bronze and will take appropriate immediate measures and assess the extent of the problem in line with agreed procedures. They will retain this role until relieved either by a Supervisor or a more experienced officer on the instructions of the RCC.

They will concentrate on specific tasks within the Agency's areas of responsibility and remit, for example, the closure of junctions to prevent more traffic joining the rear of an incident and for advanced traffic management to prevent congestion. Should it be necessary, consideration should be given to assigning control for a specific task or area to a designated officer or service provider subsequently called to the scene. The command of the resources belonging to the Agency and applied within a geographical area, or used for a specific purpose, will be retained by the Agency. Each agency must liaise fully and continually with other responder services employed within the same area to ensure a sufficient and combined effort. If appropriate, the police will normally act as the co-ordinator of this response at the scene (Part 1 Section 4.1 and 5.5 of Traffic Management Act 2004 as it applies to Agency staff should be borne in mind as should The National Guidance Framework between the Agency and Association of Chief Police Officers (ACPO)).

These arrangements will usually be adequate for the effective resolution of most incidents. However for more serious or complex incidents requiring significantly greater resources, it may be necessary to implement an additional level of management such as Silver Command.

Silver

Silver can be summarised as a level of Tactical Command which carries out the plan for resolution and delivers Gold's strategy, when established. (There may be more than one Silver, depending on the scale of the incident e.g. multiple scenes)

It will involve a tactical level of command that exists to determine priority in allocating resources, to plan and co-ordinate when a task will be undertaken, and to obtain other resources as required. They must take appropriate risk reduction measures and give due regard to health and safety requirements.

Should the Agency establish Silver Control (from where Silver will direct the tactical operations) this should normally be at the Agency RCC Silver Command Suite. The Silver Commander needs to consider where the best place is for them to undertake their role and in exceptional circumstances an alternative location may be determined. This should be done in consultation with other services, who may have a better appreciation of the safety issues in those particular circumstances. If this is done it is always advisable to identify a secondary site to which these controls can re-deploy should changing circumstances make this necessary.

Where there is one identifiable scene, tactical management may be undertaken from an Incident Control Point established in the vicinity. Many tactical functions will then be discharged at or close to the scene. Where the Agency is operating Silver Control from its Regional Control Centre, Silver must ensure a Liaison Officer is present to enhance co-ordination.

When more than one agency is working at the Tactical Level there must be consultation between the various agency Incident Officers. In order to affect co-ordination, an inter-agency meeting should be held at regular intervals attended by each Tactical Commander or their empowered representative. Establishment of inter service communication links will support the running of the incident at the scene. Normally a written record of meetings should be maintained.

Planning must also take into account that there may be a number of individual scenes each requiring a Tactical Commander.
The Tactical (Silver) Commanders should not become involved with the activities at the scene being discharged by Operational (Bronze) Commanders.

Tactical managers must concentrate on overall management. While they need to be aware of what is happening at Operational level they should leave the responsibility for dealing with that level to Operational Managers.

If it becomes apparent that resources or expertise beyond the level of the Tactical Commander is required, or if there is a need to co-ordinate more than one incident/scene (where Tactical Command has been established) it may be necessary to implement a Strategic Level of management as soon as possible (Gold).

Gold

Gold can be summarised as coordinating, managing impact and collateral consequence, setting the strategy, providing resources and agreeing the scale of events.

In exceptional circumstances, one or more agencies may find it necessary to implement a Strategic Level of management. Incidents can place considerable demands on the resources of the responding organisations, with consequent disruption to day-to-day activities. Such matters require attention by senior management.

In these circumstances a Gold Command should be established as a matter of routine rather than the exception. It is easy to dismantle if not required and removes the potential for Tactical Managers/Commanders to be reluctant to ask for a Strategic Level of Management/Command. The need for a Strategic Level may arise if Tactical Management does not have the required resources or expertise available. It may also arise if there is a need to co-ordinate more than one incident/scene for which Tactical Command has been established. Strategic Management is normally undertaken away from any incident scene.

The requirement for Strategic Management may be confined to one particular agency. However, certain incidents require a multi-agency response at the Strategic Level when the issues that arise affect the responsibilities or activities of more than one organisation.

The purpose of the Strategic, overall Command is:

- To take overall responsibility for incident management and establish a framework of policy for that incident within which the Tactical Commander(s) will work;
- To give support to the Tactical Commander(s) by the provision of resources;
- To give consideration to the prioritisation of demands from the Tactical Commander(s); and
- To determine plans for the return to normality once the incident is brought under control.

Strategic Co-ordinating Group

Strategic Co-ordinating Group can be summarised as an enabling group at Gold Command Level existing in an incident in which a multi agency commitment and response at Strategic Level is required to bring about an effective resolution. This group will take some time to assemble and should be involved in only the more serious incidents when a longer-term multi agency co-ordinated strategy is required.

In accordance with nationally agreed procedures it will normally be a police responsibility to establish and Chair the Strategic Co-ordinating Group. The Group will comprise a nominated member from each agency involved. Each person must be able to make executive decisions in

respect of resources within their agency and have the authority to seek the aid of other agencies in support of their role. The Agency should ensure their presence on this group wherever an incident impacts on the Strategic Road Network.

Agency representation on this Group should be a person who is empowered to make executive decisions in respect of resources within the Agency and have authority to seek the services or aid of other providers and responders on behalf of the Agency in support of the Agency's functions. The representative would not normally be the Incident Commander, as that would significantly detract them from their role at that time. Good communication channels will be required between the Agency's representative on this Group and Agency Gold or Silver.

Tactical decisions are not the responsibility of this group. The group members will need to be supported by a number of members of staff provided by the various agencies involved. As the incident develops there should be regular evaluation of the need and purpose of the group. It is normally the police responsibility at a major incident initially to co-ordinate the strategic role of the agencies involved. However it is recognised that due to the nature of certain multi agency incidents this role may be undertaken by, or at some stage be passed to, another agency.

It is a fundamental principle of this system that officers of the various agencies consult on a regular basis. They must also consult with agencies providing additional resources required at the scene, and maintain a strategic overview. These management arrangements will need to be adapted to the task in hand and should be flexible enough to reflect changing circumstances, but it is good practice to adopt a corporate approach, with all meetings documented and signed by those present.

The Strategic Co-ordinating Group should be aware of its wider role which may encompass central government interests, handling requests for advice from individual services and agencies, and media demands. The group will ensure that strategy for dealing with the media is in operation, designate a media briefing centre and appoint a media briefing centre manager. The Agency will manage traffic related matters.

Members of the Strategic Co-ordinating Group should not normally attend the scene. They should remain with the group throughout in order to foster the establishment of trusting relationships between members of the group and an understanding of each other's strategic objectives and the sometimes complex negotiations which are required to achieve a particular outcome. If absent for any reason they must appoint a substitute from within their agency with full authority to discharge the strategic function. In a long running incident the need for personnel to hand over to a colleague will arise. It is preferable for agencies to stagger this hand over in order to maintain expertise as new members become fully briefed on the incident.

The Strategic Co-ordinating Group should be based at an appropriate pre-determined location, normally away from the noise and confusion of the scene. In some areas a purpose built Command Suite exists, in others contingency plans should identify the accommodation to be used. Because of the police function to initially chair the group it may be considered suitable for a Police Control Centre to be used.

Gold Co-ordinator

Gold Co-ordinator can be summarised as setting strategy and co-ordinating resources on a national level for incidents that are cross regional or have a profound national impact.

While command and responsibility for incidents remains at a regional level, in some circumstances it is necessary to coordinate not only resources but also strategy in relation to events having a significant national impact. Where these conditions apply, the National Traffic Director or nominee will become the overall Strategic Director with the description Gold Co-ordinator.

This role is required in the event of:

- A National Major Incident

Or

- An incident involving more than one Agency region

Or

- Where the Agency Crisis Management Team (CMT) is mobilised

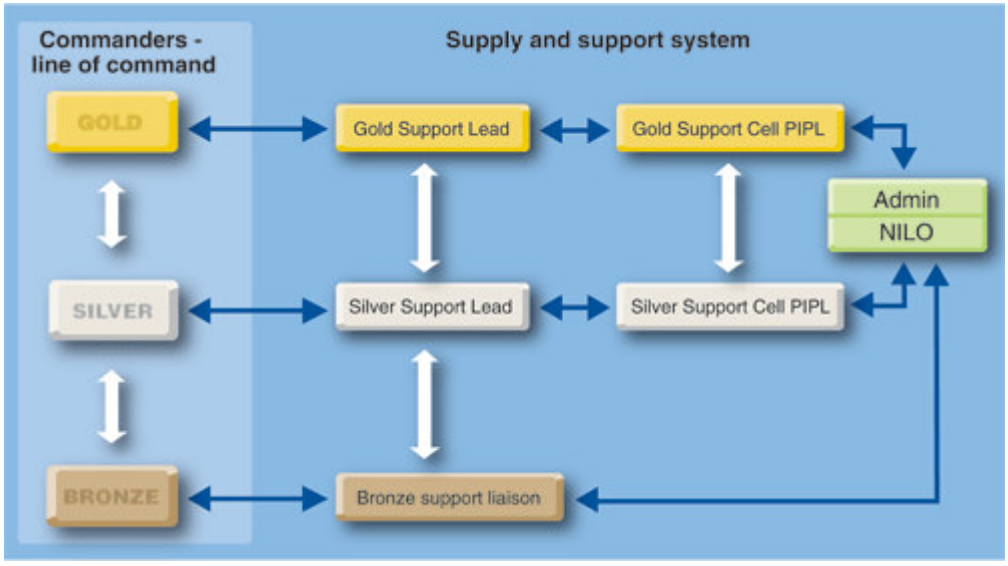
The CMT operates under the supervision of the National Traffic Director or a deputy coordinate the supply of additional resources. (As outlined in The Agency National Crisis Management Plan)

The Agency has a role to support the Dft Incident Room concept of Operations (CONOPS).
The Chief Executive or Gold Co-ordinator may have a seat within the Cabinet Office Briefing Room (COBR) and will endeavour to develop a national strategy in conformity with various departments of state. Whilst all command decisions must be taken locally the framework presumes conformity to general strategic direction in the event of a national emergency.

The Supply and Support system

The purpose of the Supply and Support System is in part to service the Gold and/or Silver Commanders with the best possible information to make decisions. It is also to provide them with space and time in which to make those decisions.

Essentially decision making in this context is about issuing instructions to achieve the outcome presumed in a plan. Planning options are a function of what we know and can best forecast with accurate situational awareness (good information flows); what resources we can muster; and our specialist capabilities.



The Gold Support Lead and Silver Support Lead coordinate: Planning, Information, People and Logistics (PIPL) Support functions and the staff performing them so that in a difficult or fast moving environment they are able to provide a current statement of events and options from a single point. This reduces speculation, lack of information and improves the 'world view' of the Commander. During 'normal' operation it also insulates the Commander from being interrupted with minor logistical and operational decisions. The local Commander retains flexibility over how best to maintain situational awareness.

	Planning	Information	People	Logistics

Gold support lead	• Immediate action plans
	• Considered action plans
	• Contingency plans
		• Collation
		• Dissemination
		• Briefing
		• Debriefing
		• Link control rooms
		• Intelligence reports
		• Situation reports
		• Media strategy
		• Impact assessment
			• Staff resources
			• Technical specialists
			• Contractors
			• Resilience
			• Welfare and support
			• Health and safety
				• Support and identify key sites for:
				  • Briefing
				  • RVP's
				  • Holding FCP's
				• Supply:
				  • Communications
				  • Transport
				  • Plant and machinery
				  • Signage
				  • Cordons
				  • Cones
				  • Lighting etc.

Silver support lead				
Bronze support liaison				
	Admin – NILO			

The Support Leads are responsible for receiving instructions from Commanders and apportioning work through the support system. Support Staff work formally to their Commander at Gold or Silver and informally between each support level. For example, a commander may indicate a particular requirement for vehicles and within the support system the Silver support staff will make their requirements known to their support equivalent in the Gold Support Office or Gold Control Room, who will do their best to mobilise Agency resources and distribute them.

The Support lead will arrange meetings, record and disseminate decisions and action requirements. This forum will include people the Commander deems it necessary to have present. In fast moving circumstances it may be a meeting of the Commander and Support lead alone.

Where other agencies are involved, their participation in the Group should be at a senior level with the authority to make decisions and commit resources. Depending upon the nature of the event there may also need to be liaison 'officers' from other agencies available at the Police Incident Control to assist with information gathering and the development of plans. This liaison is important to develop synergy and conformity with the overall Police Command. Consequently, other agencies will need to maintain a seat as required, in either the Gold Control or Silver Control or possibly both.

The support system has a particular advantage. If personnel are trained in key roles at each level, they will transmit information requirements up and down the staff system thus enabling rapid supply and development without immersing the Commander in logistical issues. For example, where an overall plan of action is decided on, staff at each level will develop their own plans of action and decide on the appropriate levels of personnel, transport and communication required to facilitate the outcome. The commander will then be free to execute the plan.

During a large protracted incident, Gold should have a Support staff capability providing the information for this level of Command to set a strategy and deliver command decisions; Silver (or Silvers) should have a parallel Support staff capability to facilitate tactical decision making; at Bronze level there should be a staff liaison so that information can be captured and passed through the staff system. Where there are smaller or less protracted incidents these functions will still need to be performed, but the scale of resources required will be influenced by the nature of the incident.

- ***The Gold Commander***

Has sole and overall command of the operation and is responsible for its success. Briefings and reports from Gold should be fed into PIPL via the Gold Support Lead and vice versa. The communication route from Silver Command to Gold is imperative to ensure a shared situational awareness. However the normal route for general information is via the PIPL Support system.

- ***The Silver Commander***

Responsible for achieving the objectives that fall to their discrete command and can vary in scale from a small scale incident to directing a large number of staff. The Silver Commander and staff must ensure they share the same 'situational awareness' as the Gold Command and other Silvers to ensure the effective resolution of the crisis.

Gold Support Lead & Silver Support Lead

A Support Lead is a senior position assigned to a member of staff who would be (depending on the scale and nature of the incident) working closely to a Commander. They transmit the decisions and instructions of the Commander with authority to execute the Commander's directions in the Support System and by virtue of the post must have access to their Commander at all times. The Support lead may act on their Commander's behalf in the immediate absence of their Commander but should seek to maintain contact at all times.

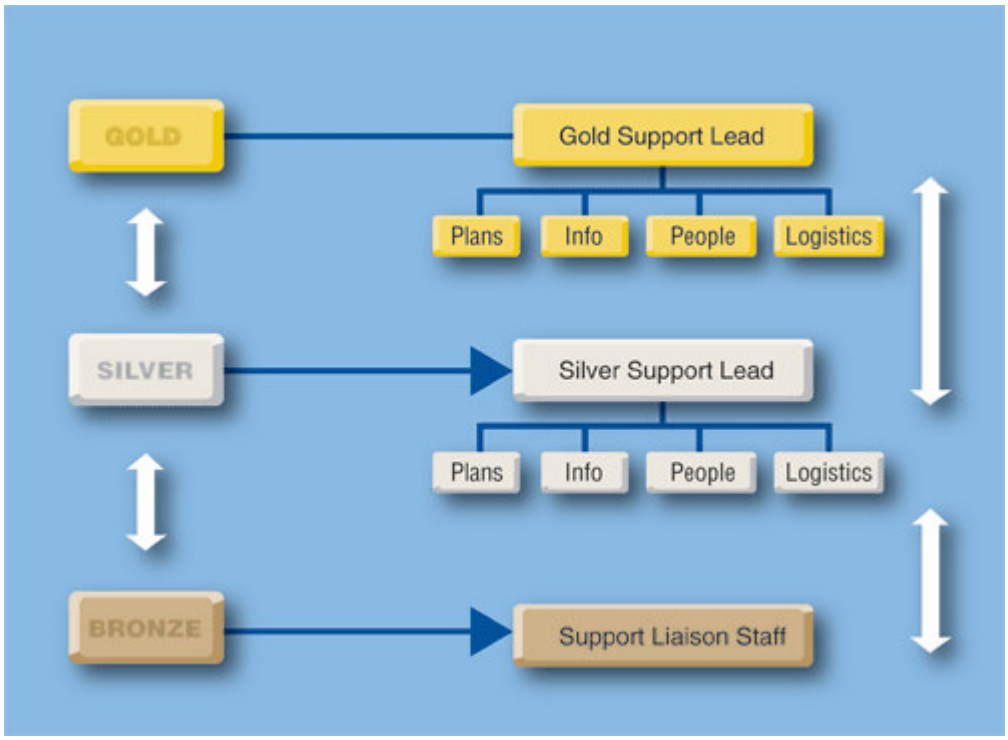
The Gold Support Lead

Provides an important role in overseeing the strategic imperatives and ensuring objectives are being met. They have a significant role in assisting with the formulation of policy with Gold and the Gold Coordinating Group, as well as coordinating the Strategic objectives of PIPL.

The Silver Support Lead

Has a similar role to that of the Gold Support lead in that they support policy making and tactics whilst ensuring that the objectives of the operation are met. They have a significant role in assisting with the formulation of tactical plans with Silver and the Tactical Coordinating Group, as well as coordinating the Tactical objectives of PIPL.

Supply and Support - structure and functions



Support and Supply System

Staff are assigned according to their specialist knowledge and skills in the support and supply functions as required. These functions are carried out by Agency staff who have the requisite training, competence and experience in the function they are undertaking.
While individual circumstances may cause the Gold Commander to vary or expand support functions, in general the support functions and PIPL are standard to most incidents and should be practised as part of the overall plan.
Support staff generate planning options but do not coordinate or execute plans. They collate and analyse information and supply personnel and equipment. The use and publication of information and the deployment of resources is a matter for Commanders.

PIPL (Planning, Information, People, Logistics)

PIPL is an acronym for the combined functions of the support system and represents the management of information, material, people and options for their deployment.

The Support and Supply Functions

Planning	Information	People	Logistics
Gold support lead	Silver support lead	Bronze support liaison	

- Immediate action plans
- Considered action plans
- Contingency plans

- Staff resources
- Technical specialists
- Contractors
- Resilience
- Welfare and support
- Health and safety

Support and identify key sites for:
- Briefing
- RVP's
- Holding FCP's

Supply:
- Communications
- Transport
- Plant and machinery
- Signage
- Cordons
- Cones
- Lighting etc.

Planning

The planning function is responsible for generating immediate operational plans as options for the Commander. Plans have to be realistic and are limited by time and the availability of resources. Plans may, therefore, be 'immediate action plans' which can be carried out in a short time frame or 'considered action plans' which take more time to develop. Plans must also be developed that manage identified risks. Planning Support Staff must actively engage in the identification and assessment of risk and provide options for the management of risk as appropriate.

At Gold level, the planning function generates options for Commanders in line with the broad strategy. They may, for example, look at area evacuation plans, isolation plans, transport and route planning or plans for consequence management.

At Silver level, the planning function would convert the general plan into a set of specific actions within a particular realm of activity and place. Planning in this context is to be distinguished from the 'Network Access and Resilience Teams' function of developing Contingency Plans.

Contingency Plans developed in slow time are rarely incident specific, although they may be. Where they exist, they can be used to develop operational plans.

Information

The Information function provides Commanders with accurate and up to date information, which is evaluated and assessed with a view to informing strategic and tactical decisions. The support staff for information will be responsible for linking to the intelligence system and obtaining and distilling information about the incident that may be useful in resolving it.

The early establishment of a system for information management and supply relieves those responsible for operational command and decision making from the constant demands for information.

It ensures all who need to know are in possession of relevant information. It enables the best available account of the whole operation to be collated. The system provides for an objective assessment of the success or otherwise of strategy and tactics. In long running major incidents support staff for information will work closely with support staff for planning to identify alternative courses of action in the light of prevailing assessments.

The information system should use the technologies and disciplines of the Agency intelligence system and usually rely on seconded intelligence staff to carry out these functions. A critical part of this role is to provide the best "live" information and interpretation for Agency Briefing Officers.

The Information function also plays a significant role in linking RCC's to the incident by monitoring and collating the state of the incident and reporting to the Commander through "situation reports." They should ensure that information flows to road users, and that a media strategy is implemented in conjunction with NTCC and the Press Office.

Informing others of an 'Agency' Critical incident

Making others aware of a critical incident and keeping them informed of developments is a distinct function quite separate to the command of the incident.

In the first instance when a critical incident is discovered or reported the person receiving the information should ensure that the National Incident Liaison Officer (NILO) is notified as soon as practicable. NILO will then inform the relevant parts of the Agency and ensure that those who need to be updated or made aware are provided with the necessary information in accordance with the procedures that are outlined in the Emergency Contact Procedures.

It is imperative for the smooth command of an incident to have rigid adherence to these information processes, as the Incident Command and Support team can then concentrate on incident resolution.

People

The People function is responsible for the supply of the right numbers of people in the right place at the right time. Their role is to develop an incident people plan in line with the requirements of operational commanders and the agreed protocols in respect of Agency technical specialists and the co-ordination of Incident Support Units (ISU's) and contractors. Incidents running over extended periods of time can make heavy demands on personnel, particularly specialists. Resource support staff must, therefore, be practised in developing resources on a sequential basis allowing for the replacement and refreshment of both front line staff and Commanders. They are responsible for ensuring that briefing locations, debriefing locations, rendezvous points and marshalling areas are properly managed, and for assuring the Commander that welfare and safety issues are properly managed.

Logistics

The Logistics function is responsible for organising and delivering communications networks, sufficient operating centres, administration support, transport, equipment, and heavy plant when required. A well-rehearsed logistical capability enables Commanders to act to resolve a situation quickly. The normal operations of a Region in providing transport, communications and other logistical commitments need to be brought to a level of readiness consistent with being part of a public service so that the Logistics function can accelerate the use of existing mechanisms.

The Cadre System

To enable the command and support functions to be effective and efficient, trained and experienced people who have a thorough grounding in the functions that they are performing must be utilised. Experience within the Police and other services has shown that a Cadre system utilises resources far more effectively and efficiently than a general competence approach.

The term Cadre is used in this context to refer to people with a particular appropriate and professional competence and who are available, and trained to fulfil that function if called upon.

The number of functions within the SIMF is considerable and includes positions at all levels. There may be some functions, e.g. Structures Engineers, Crash Barrier experts, who are permanently retained as specialist advisors (see page 34) but many other functions rely on personnel reverting in an emergency to a secondary function.

The Cadre system recognises this need and to sustain a capacity and capability designates a regular secondary function to staff who have been trained in a competence within the contingency plan. Staff so designated are kept at a level of proficiency and awareness and listed so that they can be readily rostered.

The Cadre system allows people to gain experience and generates flexibility as staff become distributed across a range of duties. It also provides for an easy rostering and call-out scheme.
A Cadre scheme must be managed in order to sustain capacity and to ensure skills levels are updated and maintained. Some roles will be frequently mobilised and competence sustained operationally; those least rostered need to be trained more frequently.
The essence of SIMF is, in part, to overcome the likelihood that the first hours in a crisis will be chaotic until a regime is established. If key staff know their functions and can take the initiative with limited briefing and be rapidly assembled, order can be shaped from confusion. A Cadre system constitutes resilience; limits training costs and generates flexibility.

Specialist Advisors

There is a requirement for the role of Specialist Adviser where specialist knowledge is necessary. Specialist advisers have specialist knowledge and will be able to offer an informed view about options. They must be trained to offer reasoned evaluations in support of decision making, but they are not decision makers and Commanders should consider their advice in the wider context. Specialist advice should never be presented as a single option but, rather, should be an expert evaluation of the options under consideration.

Incident Call Handling and Control Centres

The first point of discovery of an incident or event having taken place on the Strategic Road Network can be by a report to a Agency Regional Control Centre (RCC), detection by a RCC Operator through use of CCTV, through the observations of a Agency Traffic Officer on patrol or by an Agency service provider. In any case the RCC is the first point at which a management intervention can be made. It is the facility that enables the flow of information, instructions, requirements and requests relating to the incident. It is also likely to be the first point that any potentially significant event is recognised. Thus the RCC has a key role to play within the SIMF.

On receipt of a call at RCC, it is likely that the call will be classified according to the speed of response required that is:

- Immediate
- Prompt,
- Routine,
- Deferred,
- Non-attendance.

However, this classification merely presents a single-faceted view of the situation and does not realistically reflect the complexity of many situations. Consequently, to enable the Agency and other organisations including the Police to understand fully the dimensions and dynamics of an incident or event it is necessary to assess an incident from a number of dimensions. The key to this process is information and acting decisively upon receipt of the information in a structured, coordinated and systematic way.

Incident Initial Response

In the case of planned events it is likely that a Strategic or Tactical (top down) approach will be adopted with structures and command arrangements already in place.

Incidents are likely to be handled at the Operational level (bottom up) in the first instance therefore it falls to the initial call handler or the first person from a responding organisation on the scene to take initial actions acquire key information and make some initial decisions. It is these incidents, the majority of which could be termed as routine that form the base line of the Agency response work. However, it is incidents of a more serious or critical nature that require careful and systematic handling.

The key to achieving resolution and meeting objectives is having accurate information and obtaining a clear understanding of the situation. As the incident or event develops the operational lead at the scene and the call handlers must re-evaluate the situation. Their purpose at this point in addition to providing an open and unhindered line of communication to the scene is to ensure all the required resources with the appropriate command, control and support frameworks are in place. The RCC must have in place procedures which will **"trigger"** an enhanced or escalating response as the scale of the emerging incident is recognised.
The call handler acting on the advice of the lead officer at the scene will need to give the RCC Supervisor a clear picture of the situation. This person, working within this framework and the information provided will have to decide if the current level of response is appropriate or whether to escalate or de-escalate the level of response.

This responsibility for escalation rests in the short term with the RCC Supervisor. RCC Supervisors must be familiar with escalation procedures and given the complexity of call out arrangements there should be well rehearsed procedures with cascading levels of notification to generate an enhanced response. They must be empowered to escalate events if in their judgement it is appropriate to do so. The framework to make this decision is in this document, but a knowledge of the service provider and regional contingency plans will assist.

The decision to escalate is not based on a scientific formula. If decisions are taken to an inflexible formula the system will break down.

Good decision-making requires:

- Information
- Understanding
- Adaptability
- Flexibility
- Clarity
- Judgement

Judgement is a process of reasoning - a means of deciding how the general rules can best be applied in the circumstances. It is informed by experience.

Therefore escalation is not merely a mechanical response. The SIMF places the RCC Supervisor in a position to exercise control, but command at any level also involves leadership and perspective. The RCC Supervisor must balance competing demands in a complex environment and because of this and their ultimate accountability, they will find it advantageous to operate according to a set of principles.

It is on initial receipt of the first level of information that the first decisions on scale and escalation of the response will be made. These decisions will need to be reviewed in light of additional information or changing circumstance.

Incident Escalation Framework

Escalation Decision Considerations	
Time	Nature of Incident Public impact Resolution Resource availability
Responsibilities of Agency	Safety of Public Safety of Responders Other incidents Congestion
Alternatives	Routes Actions Resources Remedies
Credibility Capability and Capacity	Agency Other Responders
Knowledge	Network Area Disruptions Works Weather

Incidents should be commanded at the lowest level where the Commander has the empowerment, competencies and resources to affect a resolution.

To help inform the decision to escalate or not, the issues in the proceeding table should be considered. The decisions to escalate the command of an incident must be made against the level of risk, the probability of the risk occurring and an assessment of the overall impact of the incident. Please see Appendix A, the Incident Impact Criteria table from the Agency National Crisis Management Plan.

The RCC will act as the resourcing and communications centre in any incident until any separate command and control arrangements are in place.

Incident Control Points and Centres

Where an incident is escalated it may be necessary to have additional command and control facilities that can provide a dedicated focus to:

- The incident,
- Part of the incident
- A specific function
- A specific location

Some general principles apply in relation to all control points:

- If established, they must remain manned at times designated by Gold.
- Dedicated command channels must allow Commanders to communicate regardless of background traffic.
- Control points must be secure from the physical invasion of the incident and access must be tightly controlled to authorised persons only.
- Tight radio disciplines must be observed

In the case of incidents involving more than one agency it is probable that one of the Emergency Services (as a Category One responder) may have established one or all of the following points. In the case of a Agency Led incident or where the Agency is first on scene the Agency should consider establishing the following, if required. This may require consultation and communication with other responder organisations.

Rendezvous Point – (RVP)

Rendezvous Point (RVP)
A Rendezvous Point is a designated meeting location which allows for controlled access between incident zones on prescribed routes. It will fall under the remit of a Bronze Commander and will be a point of command and control.

Forward Control Point (Bronze Control)

In some circumstances, usually where there is danger associated with the incident, it is necessary to establish a Forward Control Point (FCP) within the ambit of Silver where immediate actions around the scene are controlled on a separate radio network or channel. An FCP is also used when strict control on entry and departure to an incident scene. A communications link is necessary to ensure that all organisations engaged in resolving the incident are aware of each others activities.

Incident Control Post (Silver Control)

The Incident Control Post (ICP) - often referred to as “Silver Control”, is a dedicated command and control function which carries out at Silver the functions which would have been carried out by the Major Incident Control Room (MICR) when the latter has not been activated. In the event of an MICR being activated ICP will assume command and control functions within a prescribed zone of deployment. The Agency ICP should normally be located at the RCC covering the incident, but may at the decision of the Agency Commander be located at the most appropriate point to enable effective incident management and resolution.

Major Incident Control Room (Gold Control)

A Major Incident Control Room (MICR) is established where Gold control assumes an active role. Its function is to:

- Provide liaison and command or control synchronising and information exchange with other Emergency Services.
- Handle calls from the public relating to the incident.
- Liaise with the Regional Control Centre regarding other business and contingencies.

The use of individual Regional command and control technology will provide infrastructure that will fulfil this function in respect of "command" of the incident.

Control Centre Resources

All control centres will require specific resources to enable them to carry out their function. These resources may include:

People

- Radio controllers
- Computer operators
- Call handlers
- CCTV operators
- Supply and Support function staff
- Administrative staff including Decision Log writers

Hardware

- Command and Control terminals
- Computer facilities including internet
- Fax machines
- Radio Communications including Command Band Network Channel
- Telephone lines
- Mobile telephones
- Heli Tele in liaison with the local police
- CCTV feed
- Area maps
- TV and radio receivers with access to SKY news
- Dry wipe boards and pens

Definitions

The police, other emergency services and local authorities have an established understanding of the terms 'Emergency' and 'Major Incidents.' The terms are used by Government to take powers to deal with such incidents.

The police or other emergency services will usually declare an Emergency or major incident and notify the Agency through the Regional Control Centre or the National Traffic Control Centre.

The term 'critical incidents' has also been established for those incidents that are important to a single organization. The term 'incident' should be regarded as the description of those occurrences that come to the attention of the Highways Agency and its' service providers.

Major Incident

Major Incidents are any Emergencies that require the implementation of special arrangements by one or more of the emergency services, the NHS or the local authority 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 organization of the emergency services and supporting organizations, e.g. Local Authority, to cater for the threat of death, serious injury or homelessness to a large number of people.

Emergency

This is a term that has been defined by Government and covers any challenges that present a serious threat to:

- Human welfare
- The environment
- Political, administrative or economic welfare
- The security of the UK

It includes the process of restoring and rebuilding the community in the aftermath of an incident. (Civil Contingencies Act 2004).

Critical Incident

Critical incidents are unforeseen events that seriously impact upon the Highways Agency and its ability to deliver its aim of 'safe roads, reliable journeys, informed travellers'. Importantly, the police, other emergency services or local authorities may not regard the incident in the same light and therefore may not implement the same level of response to a critical incident as the Highways Agency.

Critical incident

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

Glossary

COBR - Cabinet Office Briefing Room, where the government response to an emergency or crisis is managed.

Control Room - Centre for the control of the movements and activities of each emergency service's personnel and equipment. Liaises with the other services control rooms.

Cordon - Surrounds and protects the immediate scene of an accident.

Crisis Management Team (CMT) - The CMT will act to ensure that the Agency can continue to exercise its core functions by limiting the impact of a crisis or major incident in the event of an emergency, so far as is reasonably practicable.

DBFO - Design, Build, Finance, Operate, Refer to Service Provider

DfT - Department for Transport.

DRA - Dynamic Risk Assessment.

EMAC - Enhanced Managing Agent Contractor.

Forward Control Point (FCP) - Each service's command and control facility nearest the scene of the incident - responsible for immediate direction, deployment and security.

GNN - Government News Network

HAIL - Highways Agency Information Line

Heli Tele - Police Helicopter mounted video recording equipment with air to ground link which, with agreement from Police, allows pictures of incidents to be transmitted to control rooms or command suites.

Incident Control Point / Post - The point from which each of the emergency services tactical managers can control their services' response to an incident. Together, the incident control points form the focal point for co-ordinating all activities on site. Also referred to as 'Silver control'.

Incident Support Unit (ISU) - Service Provider/TMC personnel providing a first response 24/7 capability for any incident. They assess if any Emergency Call-Out Resources are required (in addition to the limited resources which they carry) and arrange for these to be provided through the Network Control Centre.

Inner Cordon - Surrounds and protects the immediate scene of an incident.

Major Incident Control Room - Established in protracted emergencies to co-ordinate the overall response, deal with ongoing resources and logistical requirements and provide facilities for senior command functions. Often referred to as 'Gold Control'.

Managing Agent (MA) or Managing Agent Contractor (MAC) - Refer to Service Provider

Marshalling Area - Area to which resources and personnel not immediately required at the scene or being held for further use can be directed to standby.

Media Centre / Media Briefing Centre - Central location for media enquiries, providing communication, conference and monitoring facilities, interview and briefing, access to responding organisation personnel staffed by spokespersons from all principal services/organisations responding.

Media Liaison Officer - Representative who has responsibility for liaising with the media on behalf of their organisation.

Media Liaison Point - An area adjacent to the scene which is designated for the reception and accreditation of media personnel for briefing on arrangements for reporting, filming and photographing, staffed by media liaison officers from appropriate services.

Mutual Aid Arrangements - Cross-boundary arrangements under which the Traffic Officer Service and Service Providers request extra staff and/or equipment.

NAR - Network Access Resilience.

NCMP - National Crisis Management Plan. See CMT.

NGF - National guidance framework.

National Incident Liaison Officer (NILO) - HA member of staff based at the NTCC available 24/7/365 to receive information about critical and major incidents and to disseminate information within the Agency and DfT as necessary.

National Traffic Control Centre (NTCC) - Control centre based in the Midlands to collect and disseminate information on road conditions and traffic flow for whole of England and set strategic diversion routes.

Network Control Centre (NCC) - The Service Providers 24 hour communications centre.

NIM - National Intelligence Model.

Outer Cordon - Seals off a controlled area around an incident to which unauthorised persons are not allowed access.

PSA Target - Public Service Agreement Target.

Regional Control Centres (RCC) - Control centre based regionally and staffed by the Police and HA to act as a central referral point for all emergency roadside services and monitors the network using roadside technology.

Rendezvous Point (RVP) - Point at which all resources arriving at the outer cordon are directed for logging, briefing, equipment issue and deployment. In protracted large-scale incidents there may be a need for more than one rendezvous point.

RIU - Regional Intelligence Units.

Senior Investigating Officer (SIO) - The senior detective officer appointed by the senior police officer to assume responsibility for all aspects of the police investigation.

Senior Officer On Call (SOOC) - Senior Highways Agency officer operating out of hours on a rota to deal with strategic management of incidents when/if contacted by the National Incident Liaison Officer (NILO).

Service Provider - The Agency's contractor responsible for the operation and management of the network

SIMF - Standard Incident Management Framework.

SIMG - Standard Incident Management Guidance.

SIMP - Standard Incident Management Plan - includes SIMF and SIMG.

SRW - Schedule of Roadworks.

SSR - Safety Standards & Research Directorate of the Agency.

Term Maintenance Contractor (TMC) - The Agency Contractor reporting to a Managing Agent, providing works and emergency response services for the operation and management of the Agency's Area network.

TiS - Traffic Information Services – private company employed to operate the National Traffic Control Centre (NTCC).

TM - Traffic Management.

TRL - Transport Research Laboratory.

Appendix A

HA Crisis Management Plan Incident Impact Criteria

Level	Level Description	CMT Activated	CMT Informed	Emergency Contact Procedure		Impact on Network	HA Resource Needed	Affect on HA Reputation	Media Attention towards the HA	Consider Debrief
				NILO	SOOC					
0	State of National Emergency	✓		✓	✓					✓
1	Cross Regional or National HA Major Incident	✓		✓	✓	Major impact across Regions / Nationally	Whole Agency / Significant reallocation of resources	Loss of Agency credibility	'Front page' National/ International TV/Radio	✓
2	Regional HA Major Incident		✓	✓	✓	Significant part of Strategic Road Network in Region	Reallocation of resources from other Regions	Development of Agency affected	Potential use as 'Front page' headline	✓
3	HA Major Incident		✓	✓	✓	Incident and diversion routes	Mutual aid from neighbouring Regions	Reputation materially affected	National Coverage	✓
4	Serious Incident			✓	✓	Incident and immediate vicinity	Resource covered by overtime	National reputation may be affected	Of interest to National Media	✓
5	Significant Incident					Incident	Local shift resource	Loss of local goodwill	Of interest to Local Media only	
6	Routine Incident					Minimal	HA Vehicle/ISU on Scene	No affect	No interest to media	

Annex 7.8.12 Service Provider Contingency Plan Model Document

Insert

Error! Unknown document property name.

Error! Unknown document property name.

Error! Unknown document property name.

Error! Unknown document property name.

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

Name of Service Provider
Address of Service Provider
Telephone number of Service Provider
Fax number of Service Provider

Error! Unknown document property name.

Error! Unknown document property name.

Error! Unknown document property name.

Issue and Revision Record

Rev	Date	Originator	Checker	Approver	Description

Insert details to suit Service Provider's Quality Assurance System. Insert any disclaimers required.

List of Contents **Page**

Executive Summary

This is the Contingency Plan for Area XXX.

It explains how the Area will escalate its Standard Incident Response from Operational Level (Bronze) to Tactical (Silver) and Strategic (Gold) levels when that is necessary.
This will ensure the most robust response possible to any level of emergency or disruption to network operations.

The plan has been written in accordance with the Highways Agency's (HA) Model Document for Area Service Provider Contingency Plans and has been approved by the HA's Area Performance Manager.

The plan is updated at quarterly intervals.

1.0 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)** levels on occasions when needed.
The Plan refers to the Highway network shown in **Figure 1.3.** It refers to incidents affecting that network, whether occurring on or off it.

1.2 Structure of the Plan

The Plan is in three parts:

- this Document, setting out the escalated response to a Major or Critical Incident, or Civil Emergency, referred to as the "Main Document"
- Tactical Diversion Route Document
- 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 Scope of the Main Document

The Main Document contains the following:

Section 1 Purpose of the plan - the scope and the structure of the Plan.
Section 2 Key Stages of the plan - the high level stages of the mobilisation of the Plan.
Section 3 Roles and Responsibilities the roles and responsibilities of the parties who may be involved in an incident.
Section 4 Stage 1 of Contingency Plan - Links between the Service Provider's established Bronze Control Incident Response procedures and explains how they link in to the Contingency Plan.
Section 5 Stage 2 of Contingency Plan - This section explains the Partial implementation of the Plan involving enhanced communications only.
Section 6 Stage 3 of Contingency Plan - The full implementation of the Plan to Silver control, including establishment of a Tactical Management Team (TMT) located in a Tactical Management Room (TMR).
Section 7 Stage 4 of Contingency Plan - Escalation of management of the incident is escalated to the RCC if necessary.
Section 8 Stage 5 of Contingency Plan - The further escalation to the HA Crisis Management Team if necessary.
Section 9 Stage 6 of Contingency Plan - De-escalation of Incident Control
Section 10 Stage 7 of Contingency Plan - The structured debrief following Plan implementation.
Section 11 Stage 8 of Contingency Plan - How lessons can be learned from incidents.
Section 12 Stage 13 of the Contingency Plan – Lessons learned
Section 13 The Diversion Route Document (DRD).
Section 14 Management of the Plan.
Section 15 Plan Management

1.2.2 Tactical Diversion Route Document (DRD)

The Diversion Route Document (DRD) contains details of Tactical 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 at 7.6.4 of the Network Management Manual (previously issued as AMM 71/06).
The contents of the DRD are specified in **Section 13** in this document.

1.2.3 Box of Reference

This box contains Major Stakeholder Contingency Plans and other reference information that the Tactical Management Team may require to manage an incident on or off the strategic network.

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

A.

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:

- the Service Provider
- the RCC
- the Highways Agency's National Crisis Management Team (CMT)

These Plans allow for the management of incident response to be escalated from the Service Provider to the RCC and to the CMT 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 management.

1.6 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, repairing damaged infrastructure and reopening the network. Particular attention is drawn to objectives relating to informing the public and safeguarding the environment.

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

1.7 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

1.8 Contingency Plan Escalation Procedure

1.8.1 Introduction

The Contingency Plan is implemented when the Service Provider's standard Incident Response procedures are unable to contain an incident or its effects, to the extent that any of the common **Incident Objectives** are threatened.

The Contingency Plan will be implemented in circumstances when the Service Provider's Standard Incident Response procedures are unable to stabilise a situation and the situation is likely to deteriorate further and become out of control without tactical or strategic intervention.

Figure 1.1 shows a high level overview of the escalation procedure. It shows how incident response is escalated from Bronze through Silver to Gold Levels. Triggers for implementing the Contingency Plan (at various levels) are shown in red.

Bronze (Operational Management by the Service Provider)

The incident is managed by the Service Provider using Standard Incident Response procedures.

Silver (Tactical Management by the Service Provider)

The Service Provider mobilises the Tactical Management Team and sets up the Tactical Management Room to manage the incident.

Gold (Strategic Management by the Service Provider)

The Service Provider mobilises the Senior Management Team and sets up Gold Command.

Gold (Strategic Management by the HA RCC)

Strategic management of the incident passes to the RCC. Details of how they operate can be found in the RCC Contingency 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)

Gold (Strategic Management at a national level by HA's National Crisis Management Team (CMT))

Strategic management of the incident passes to the CMT. Details of how it operates can be found in the National Crisis Management Plan

1.8.2 Gold, Silver and Bronze

It should be noted that Silver level command by an RCC and Gold level by the CMT in this context is relative to the Service Provider's and may not necessarily require Gold level command in absolute terms within either organisation. This might be more appropriate for, say, a crisis within the Highways Agency not involving the Service Provider. Equally, an RCC, for example, would probably be operating at no higher than Silver level command within its own Contingency Plan, but would be providing Gold level command for the Service Provider.

Figure 1.2 illustrates this point, and shows how a Gold-Silver-Bronze command structure can be provided in different circumstances with different organisations at different levels of control within their own Contingency Plans.

1.9 Interface with Regional Control Centre (RCC) Contingency Plans

The Plan is consistent with the HA's XXX Region – Regional Control Centre Contingency Plan dated XXX.

The RCC Plan adopts the same procedures and terminology, and embodies the actions specified for RCC in this Plan.

1.10 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 effects of the incident. Plan holders' names, contact details etc are given in **Appendix A** of this Plan.

1.11 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, 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.

1.12 Incident Definitions

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

Figure 1.1: High Level overview of escalation procedure

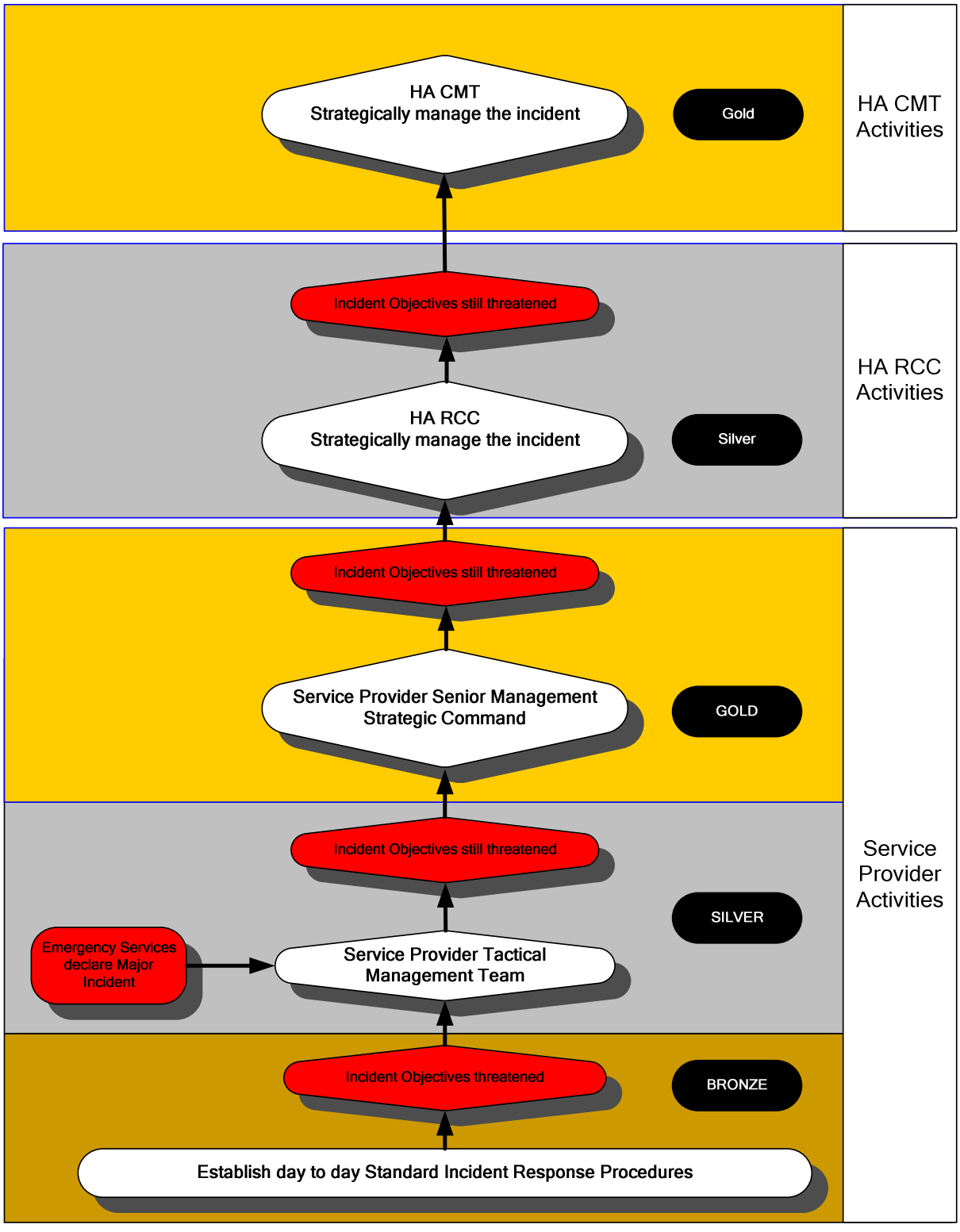


Figure 1.2: Relationship between Service Provider (SP), Regional Control Centre (RCC) and Crisis Management Team (CMT) levels of Incident Command

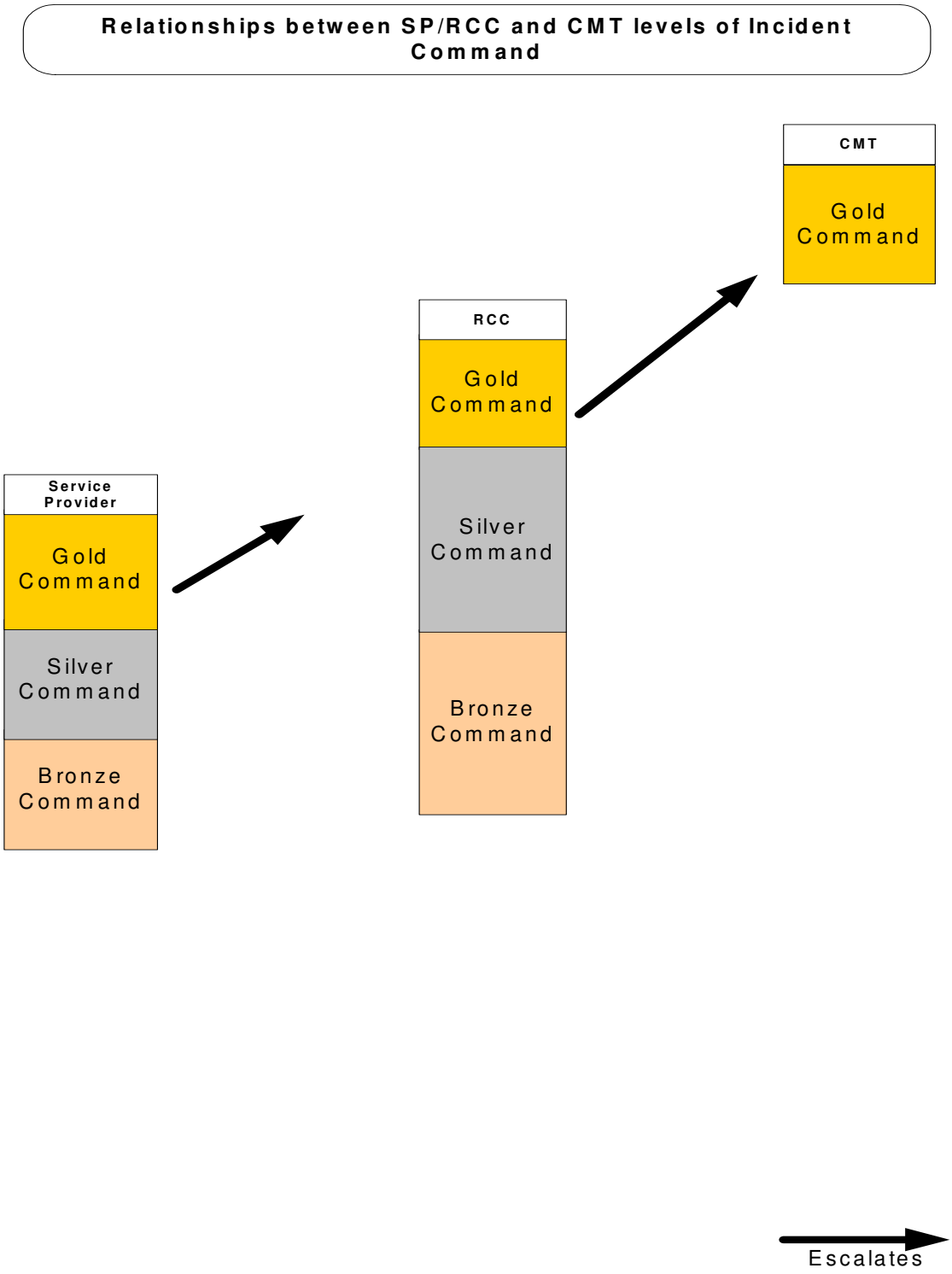


Figure 1.3: Service Provider Area Map
A map showing the roads and boundaries of the Service Provider's HA Network Area is to be included here, also showing the RCC responsible for each part of the network.

2.0 KEY STAGES OF PLAN

2.1 Introduction

Implementation of the Contingency Plan comprises a number of different stages at different levels of control (Bronze, Silver and Gold).

The figures in this section show different ways in which the Plan can be implemented. They illustrate:

- "Bottom Up" Plan implementation when implementation of the plan is triggered by events within the Service Providers Area.
- "Top Down" Plan implementation. When implementation of the plan is by external events imposed on the Service Provider.

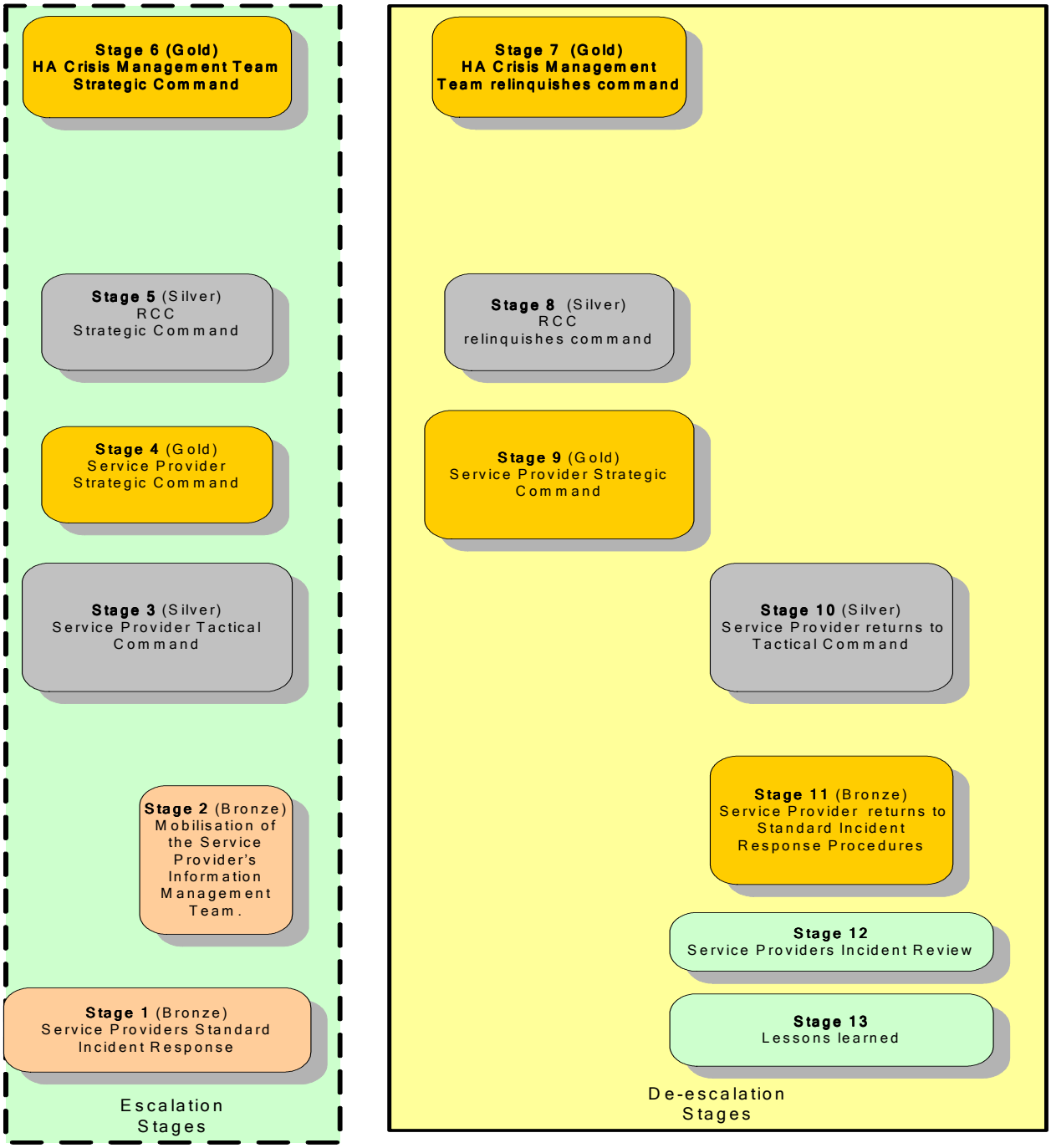
2.2 "Bottom-Up" Plan Implementation

Figure 2.1 (following) shows the key stages of Contingency Plan implementation.
There are 6 escalation stages and 4 de-escalation stages, although some stages appear in both procedures. The decision to escalate or de-escalate (at each stage) depends on whether the incident objectives (**section 1.8**) are being threatened. Execution of the ten individual stages is explained in more detail in **sections 4 to 11**.

The individual stages of the Plan can be applied in different sequences, as explained below.

Figure 2.2 Sequence A
Figure 2.3 Sequence B
Figure 2.4 Sequence C
Figure 2.5 Sequence D
Figure 2.6 Sequence E
Figure 2.7 Sequence F

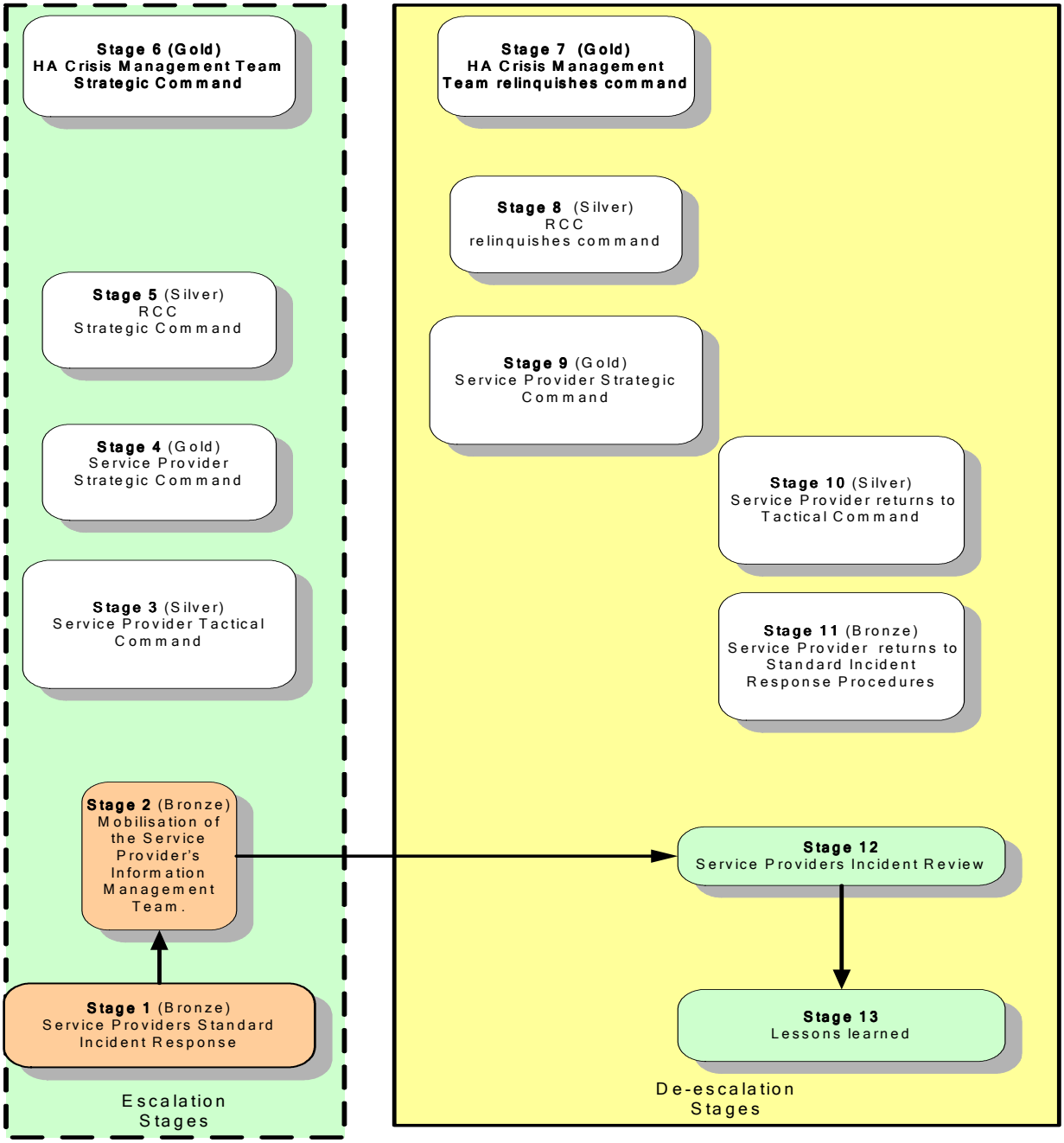
Figure 2.1: High Level diagram showing the different stages of mobilisation and de-escalation



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

The stages of Plan implementation above 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 six alternative sequences to implementing the Contingency Plan. In each case, the corresponding de-escalation stages are also included.

Figure 2.2: Sequence A

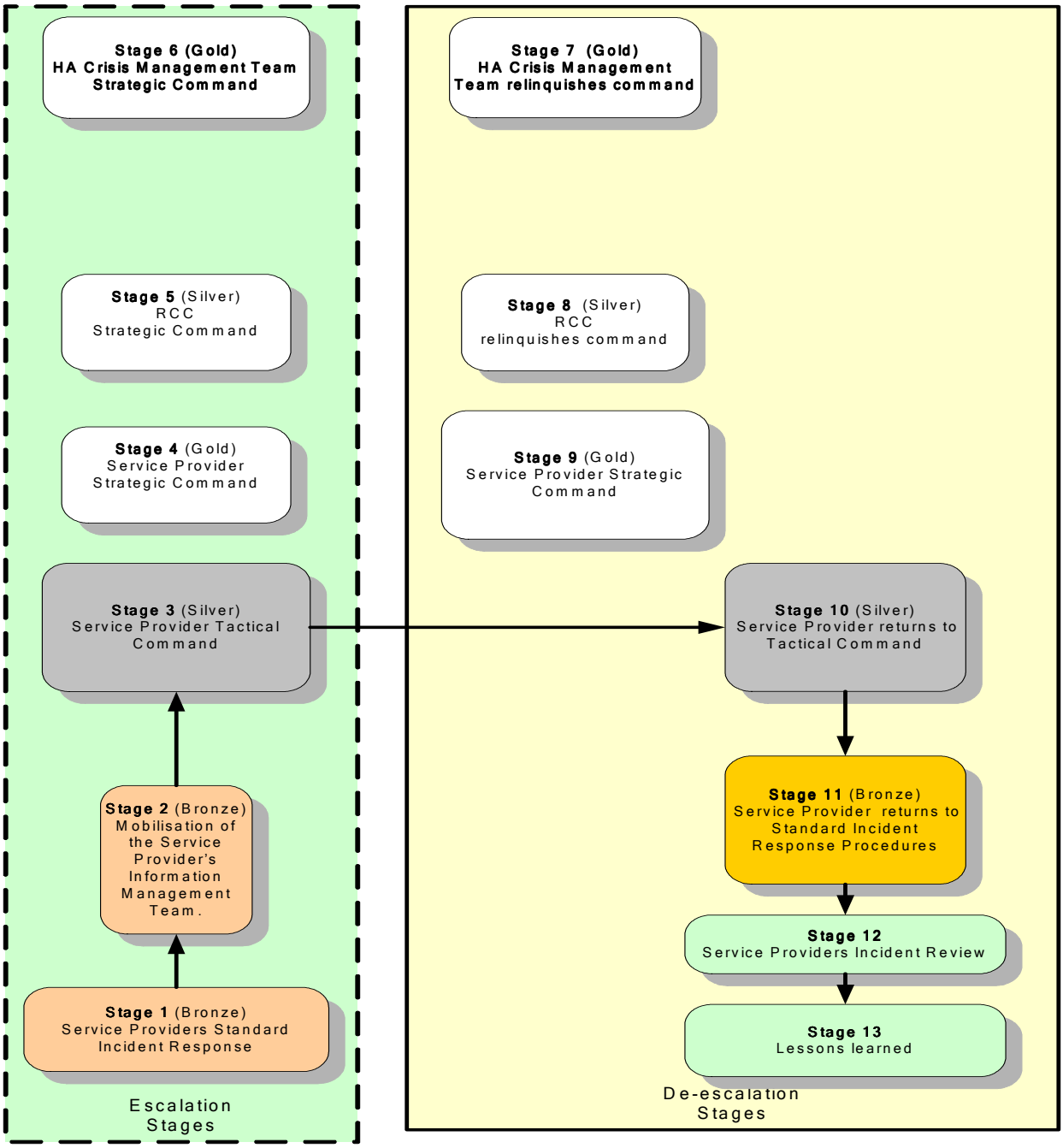


2.3.1 Sequence A Bronze (Stages 1, 2, 12 and 13)

(Mobilisation of Service Provider's Information management Team (IMT))

Service Provider's Standard Incident Response Plans are able to deal with incident at an operational level, but there is a need to enhance the communications transmitted to the HA, media and stakeholders. The Plan is partially implemented to mobilise the Service Provider's IMT only.

Figure 2.3: Sequence B

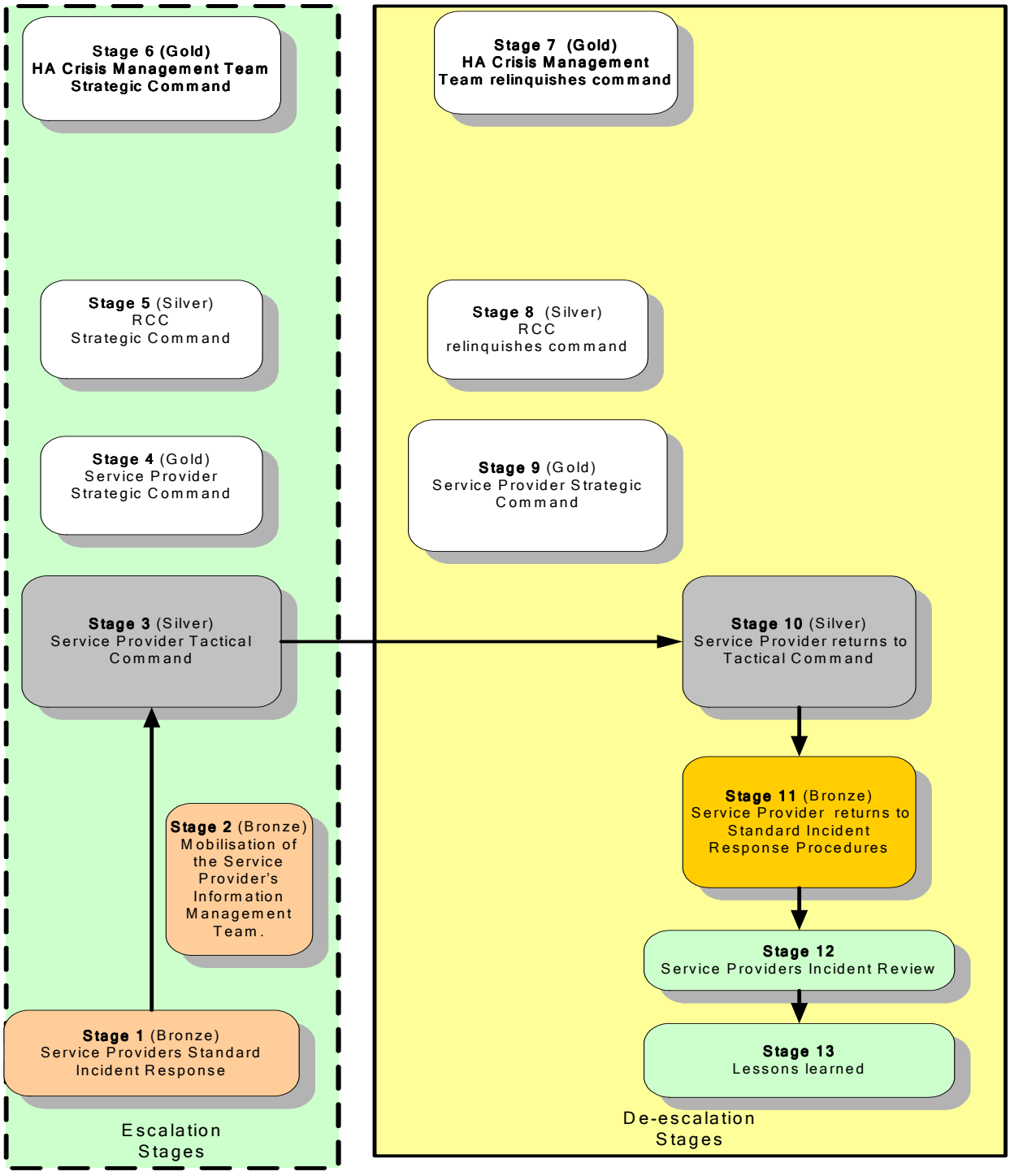


2.3.2 Sequence B Silver (Stages 1, 2, 3, 10, 11, 12 and 13)

(Service Provider Tactical control)

This shows the incident escalating to Service Provider tactical control as the situation deteriorates further. The IMT can alert others of the need to implement Stage 3.

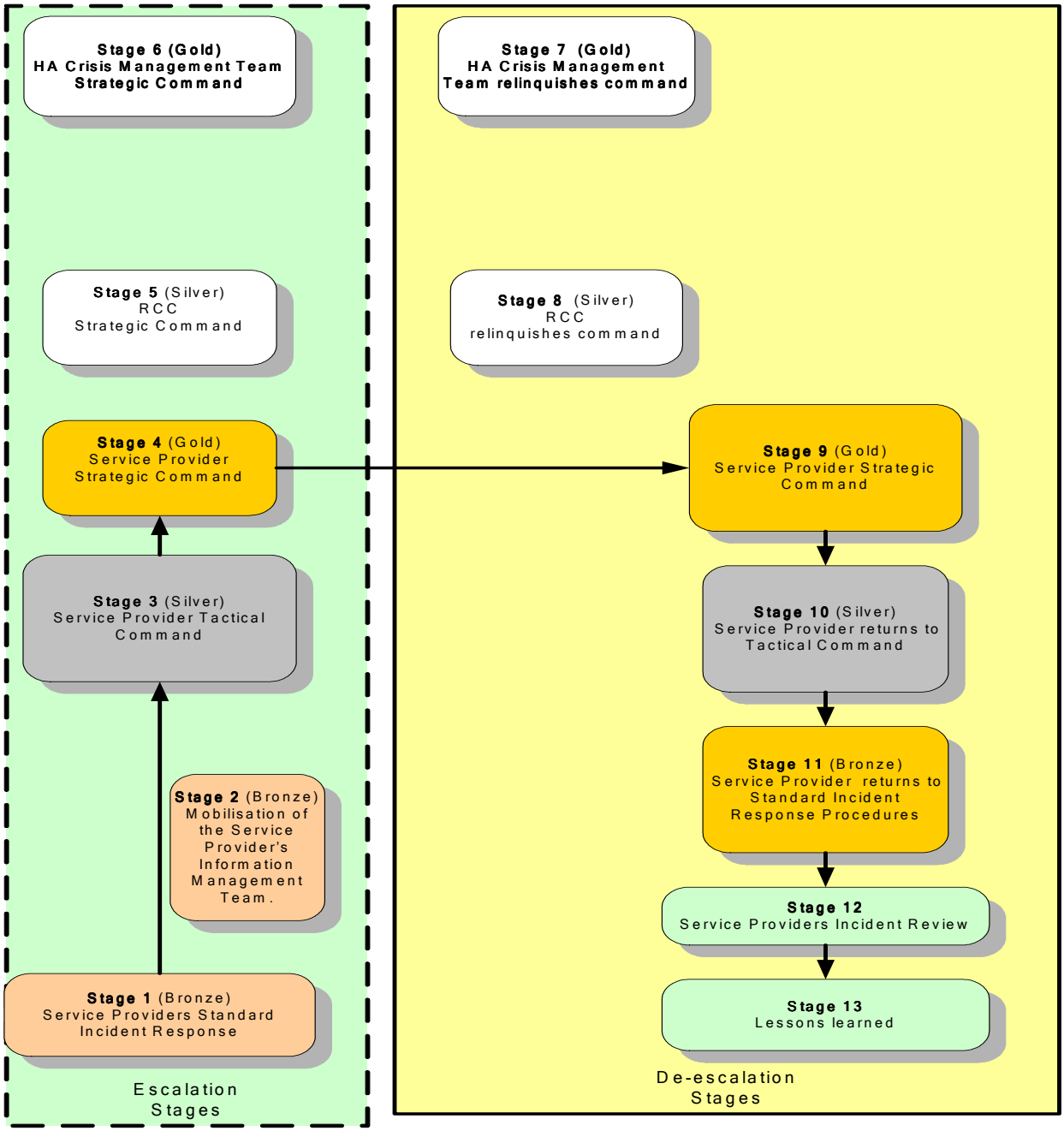
Figure 2.4: Sequence C



2.3.3 Sequence C Silver (Stages 1, 3, 10, 11, 12 and 13)
(Service Provider Tactical Control)

The sequence shows escalation directly to Service Provider tactical command, bypassing Stage 2 of the plan.

Figure 2.5: Sequence D

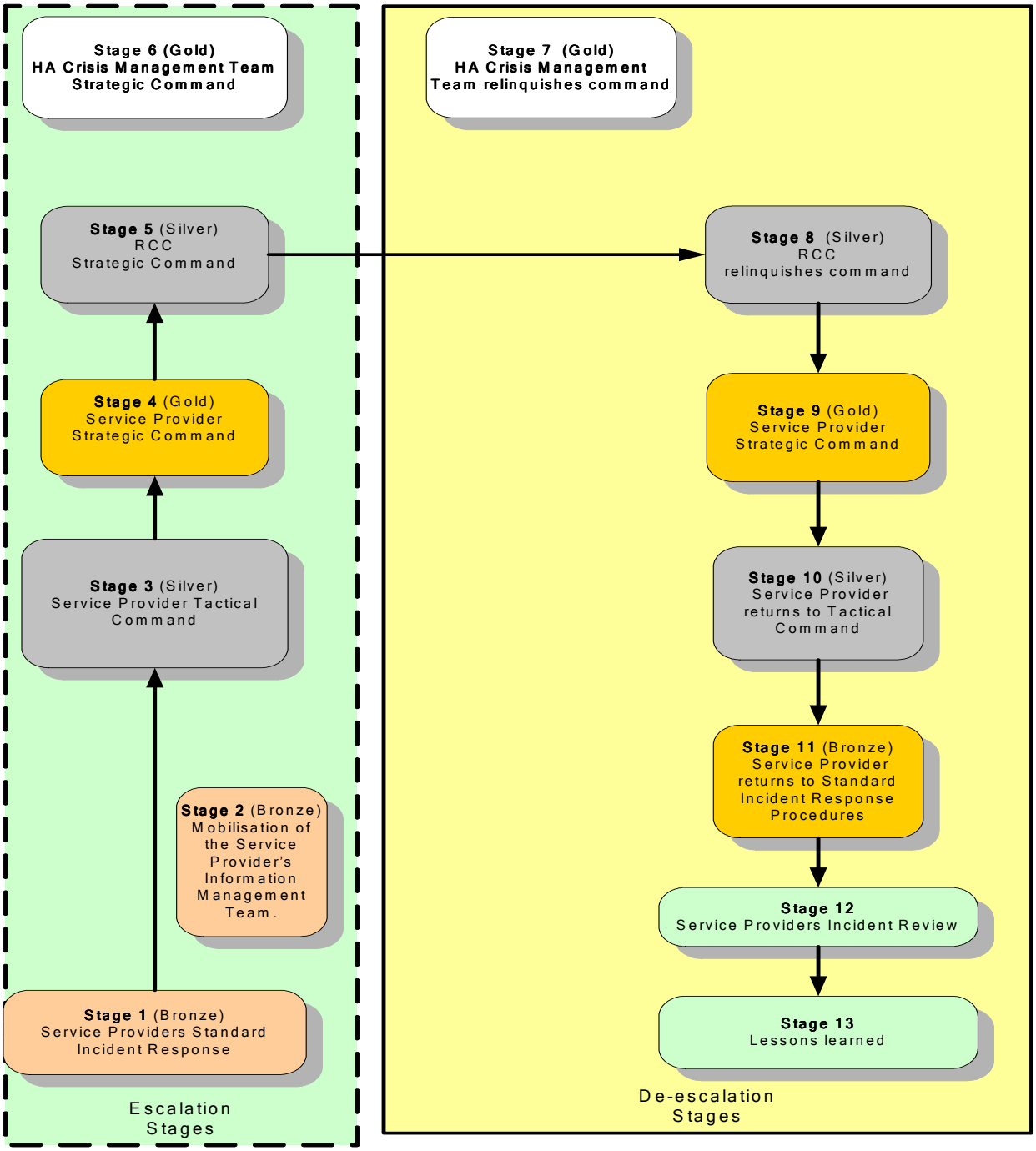


2.3.4 Sequence D Gold (Stages 1, 3, 4, 9, 10, 11, 12 and 13)

Service Provider Strategic Command

The sequence shows escalation to the Service Provider strategic command. A partial implementation of the Plan (Stage 2) could be included in the sequence if the incident develops more slowly. When the Service Provider decides that strategic command of the incident is no longer required, the Service Provider returns to tactical command Stage 3.

Figure 2.6: Sequence E

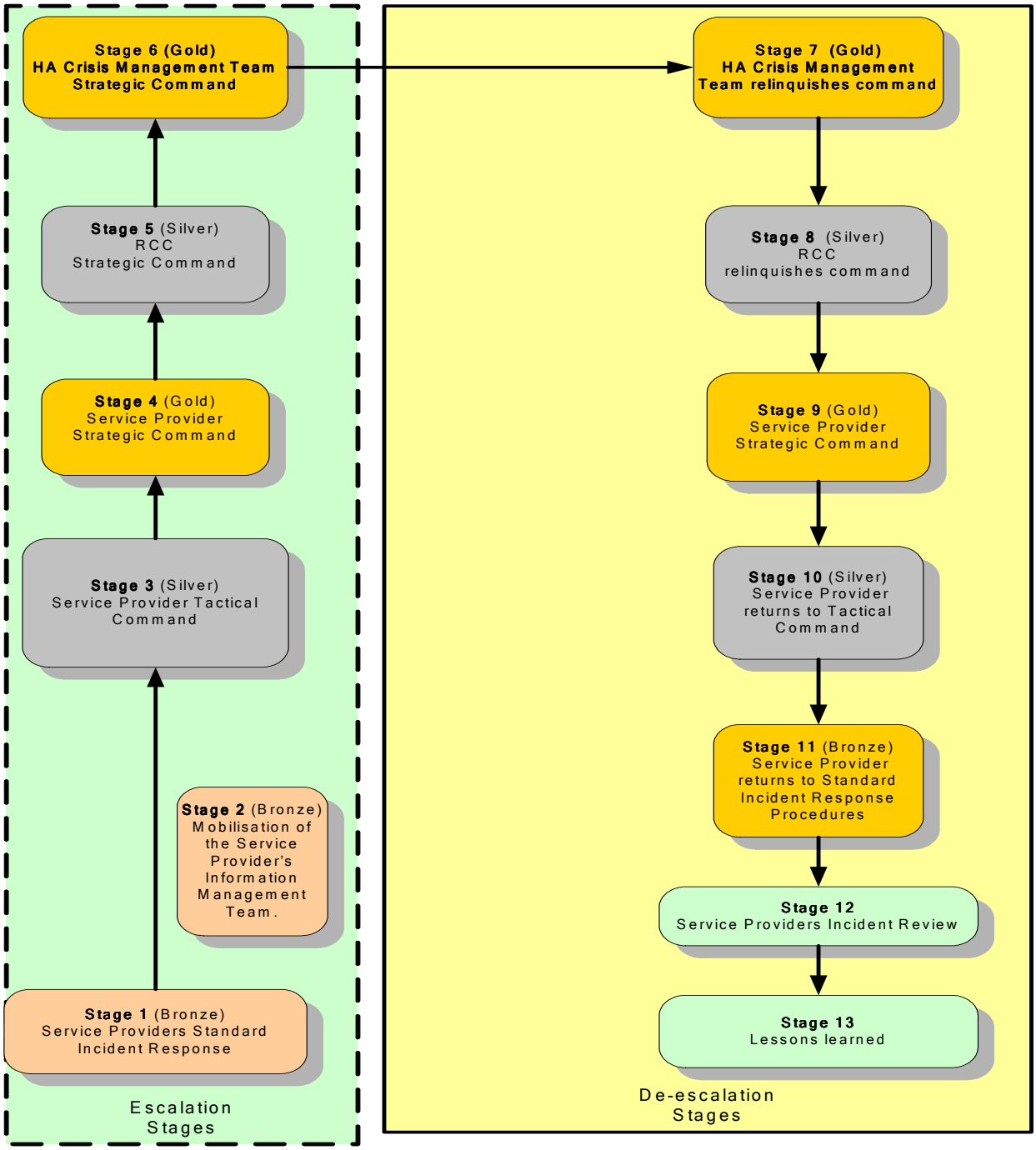


2.3.5 Sequence E Silver (Stages 1, 3, 4, 5, 8, 9, 10, 11, 12 and 13)

HA RCC Strategic Command

This sequence shows escalation up to the HA RCC Silver command. Again, a partial implementation of the Plan (Stage 2) could be included in the sequence if the incident develops more slowly. When the HA RCC Team relinquishes strategic command of the incident, the Service Provider regains strategic command and Stage 9 is implemented which has the same functions as Stage 4.

Figure 2.7: Sequence F



2.3.6 Sequence F Gold (Stages 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13)

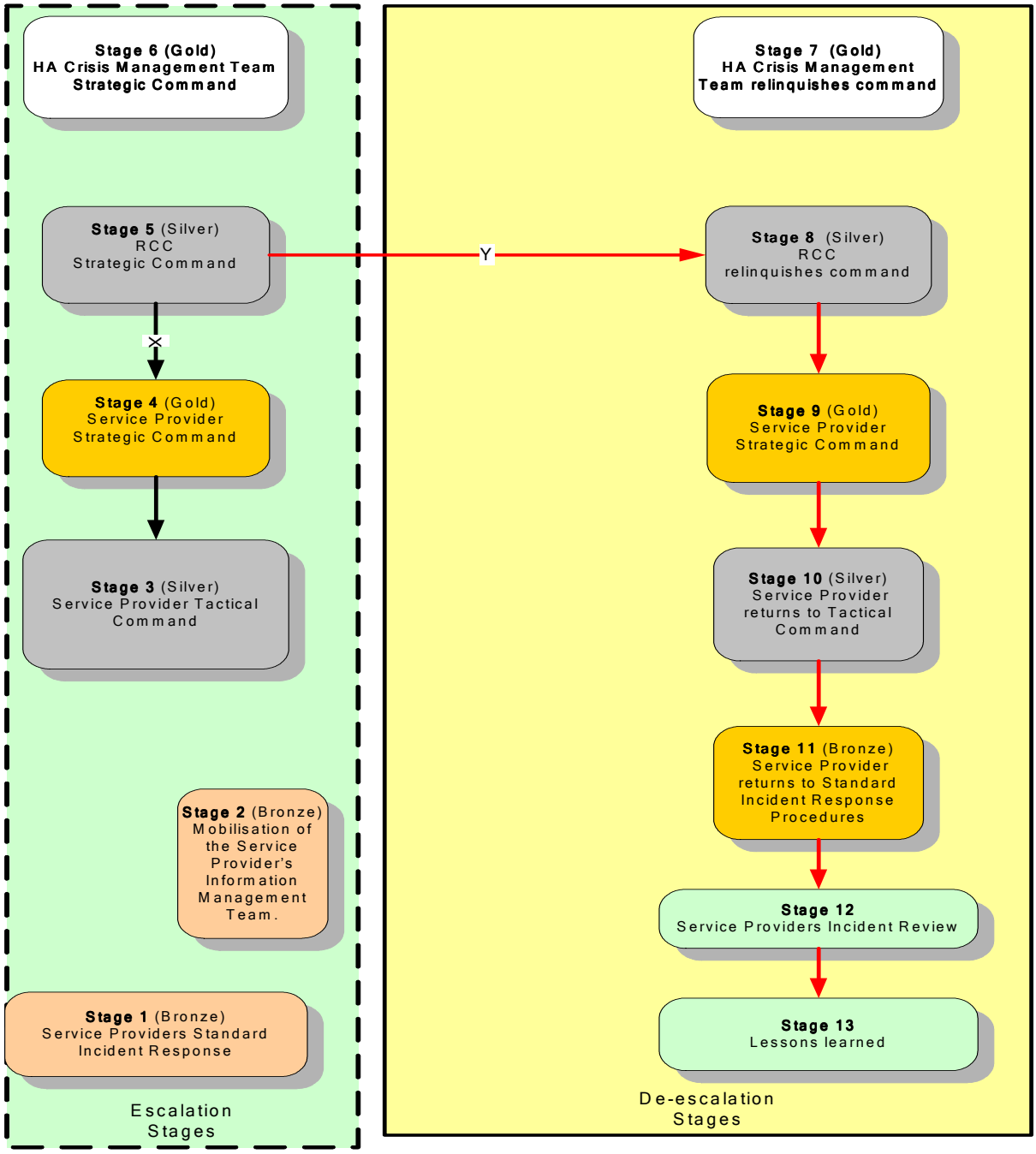
HA CMT Strategic Command

This sequence shows escalation up to the HA CMT Gold command. Again, a partial implementation of the Plan (Stage 2) could be included in the sequence if the incident develops more slowly. When the HA CMT Team relinquishes strategic command of the incident, the HA RCC regains strategic command and Stage 8 is implemented which has the same functions as Stage 5.

2.4 "Top-Down" Plan Implementation by RCC

The stages of Plan implementation above refer to "Top Down" Plan escalation triggered by events outside of the Service Provider's Area. 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 2.8: "Top-Down" Plan Implementation by RCC



2.5 "Top-Down" Plan Implementation RCC

In other circumstances, 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.

2.5.1 Escalation: Sequence X: RCC Silver (Stages 5, 4 and 3)

This sequence shows how the RCC implements the Area Contingency Plan and instructs the Service Provider to set up Gold Command.

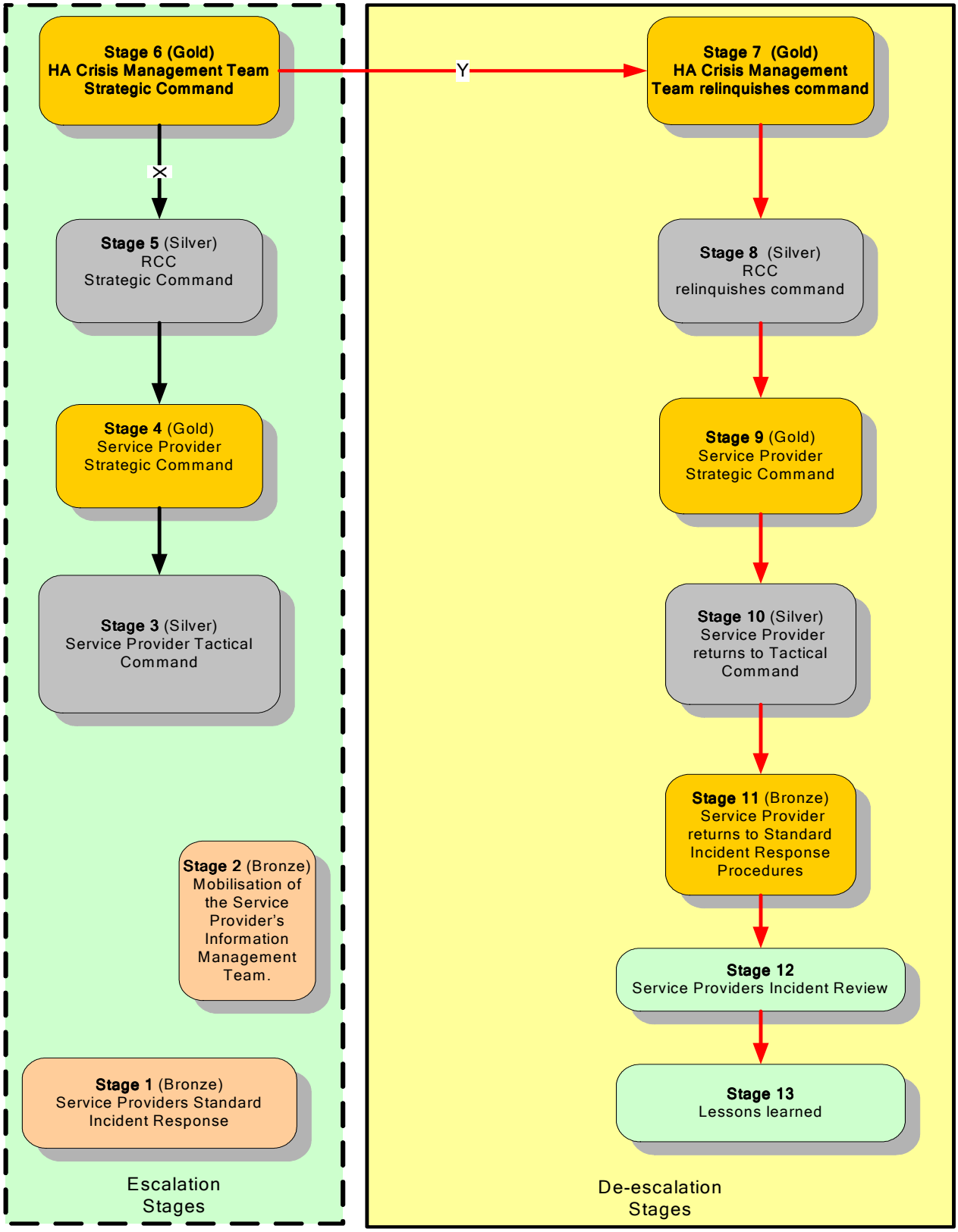
2.5.2 De-escalation: Sequence Y: RCC stands down Gold (Stages 8 to 13)

This sequence shows RCC closing down Silver command and the de-escalation process.

2.6 "Top-Down" Plan Implementation by the HA Crisis Management Team

In this situation, implementation of the Plan is instructed by the HA Crisis Management Team, set up in response to a Civil Emergency or similar.

Figure 2.9: "Top-Down" Plan Implementation by the HA Crisis Management Team



2.7 Key Sequences to HA National Crisis Management Team (CMT) implementing the Plan

2.7.1 Escalation: Sequence A: HA CMT Gold Control (Stages 6, 5, 4 and 3)

This sequence shows how the HA Crisis Management Team (CMT) implements the Contingency Plan. They pass strategic decisions down to the RCC who interprets these at a strategic level for the Area concerned. The RCC instructs the Service Provider to set up Gold command.

2.7.2 De-escalation: Sequence B: HA CMT Gold stands down (Stages 7 to 13)

This sequence shows how the HA CMT closes down its Gold command and hands strategic control of the incident to the RCC. The Service Provider retains tactical command of the incident. As the situation further eases, the RCC closes Gold command and leaves the Service Provider in tactical command.

3.0 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the following players who may be involved in an incident are briefly explained in this section.

- HA Area Team
- Regional Control Centre (RCC)
- Service Provider

The roles of other parties e.g. Police, Traffic Officer Service are explained in further detail in the HA document named Standard Incident Management Framework (SIMF)

3.1 Highways Agency (HA) Area Team

3.1.1 Role

The HA Area team's role in the Contingency Plan is to safeguard the Agency's interests at a area level. This may involve providing specialist advice to the RCC, 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.

3.1.2 Responsibility

To authorise temporary variations for the Service Provider for items outside of their contract
To give Specialist advise to the RCC if requested

3.2 HA Regional Control Centre (RCC)

3.2.1 Role

The regional control centres are the centres for all communications regarding incidents on the Strategic network. They manage Traffic Officer involvement in incidents, liaise with the Emergency services and Service Providers, and manage HA's response to the incident at operational, tactical and strategic levels.

3.2.2 Responsibility

Specific responsibilities of the RCC include :

- Manage Traffic Officer involvement in incidents
- Co-ordinate the responses of emergency services and other service providers
- Monitor and manage traffic on the Strategic network
- Display messages on variable message signs (VMS)
- Take strategic control of the incident when required

3.3 The Service Provider

3.3.1 Role

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

3.3.2 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

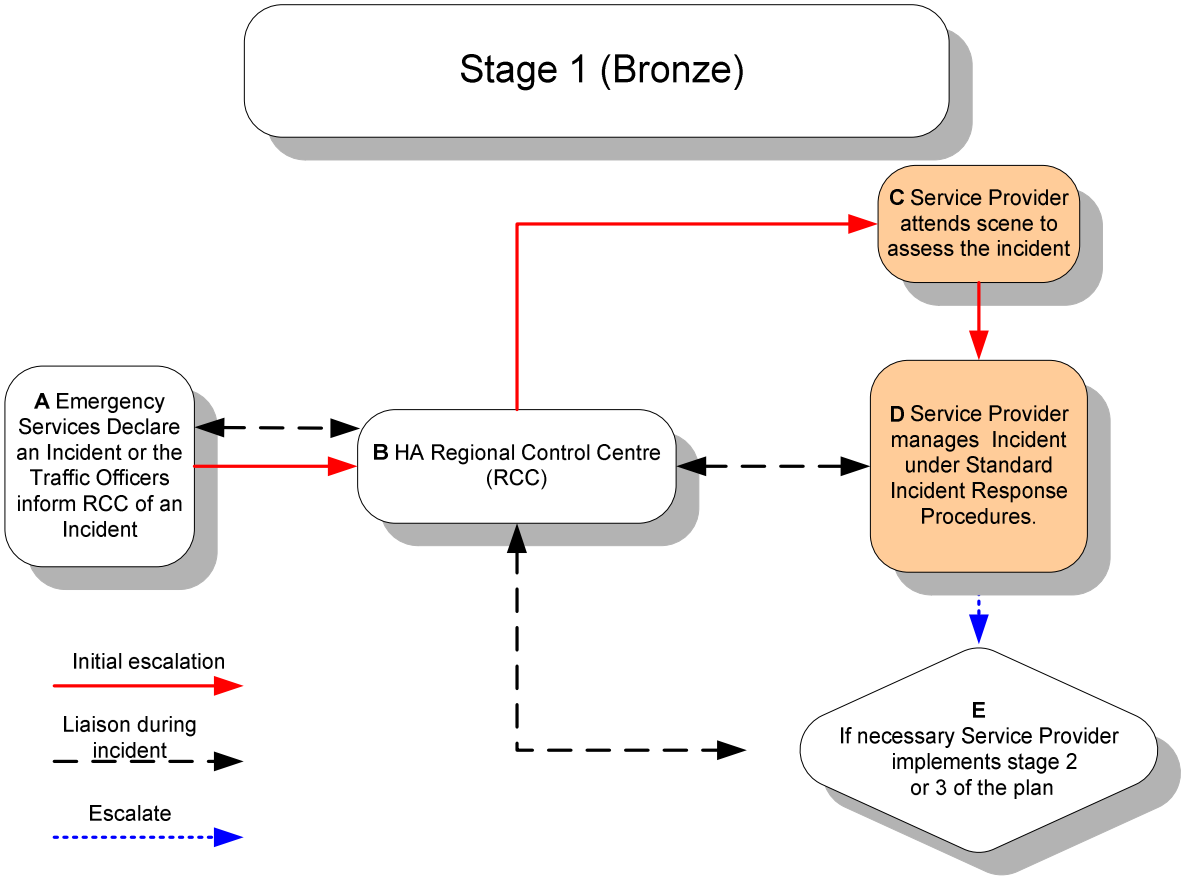
4.0 STAGE 1: SERVICE PROVIDER'S STANDARD INCIDENT RESPONSE (BRONZE)

4.1 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 1.6** are threatened.

Figure 4.1: Service Provider's Standard Incident Response Procedures



4.2 Box A

Police or Emergency services contact the RCC and inform them of an incident on the Strategic Network. A Traffic Officer contacts the RCC and informs them of an incident on the Strategic Network.

4.3 Box B

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

4.4 Box C

The Service Provider sends an Incident Support Unit (ISU) to attend the incident and make an initial assessment of the further response required.

4.5 Box D

The Service Provider sends the necessary resources to the scene of the incident and makes the necessary response (eg temporary signing, repairs to the infrastructure etc.). The Service Provider reassesses whether the incident can be managed under Standard Incident Response Procedures and whether any of the incident objectives are threatened.

4.6 Box E

If any of the incident objectives are threatened, the Service Provider will escalate the incident response to Stage 2 or 3. The escalation procedures are explained in **Section 5** (escalation to Stage 2) and **Section 6** (escalation to Stage 3).

4.7 Process Flow Charts

Include a process flowchart in Appendix F to explain Stage 1, showing the actions of each team or player and the lines of communication between them .The Service Provider column could be split in to separate columns for individual Service Provider teams. This will amplify Figure 4.1 and enable individuals to better understand the actions they have to take and who they need to communicate with. It may be helpful to cross refer to existing process flow charts describing Standard Incident Responses.
An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider.
Introduce the flowchart here and highlight any points which Plan holders should have drawn to their attention.

5.0 STAGE 2: MOBILISATION OF THE SERVICE PROVIDER'S INFORMATION MANAGEMENT TEAM (IMT)

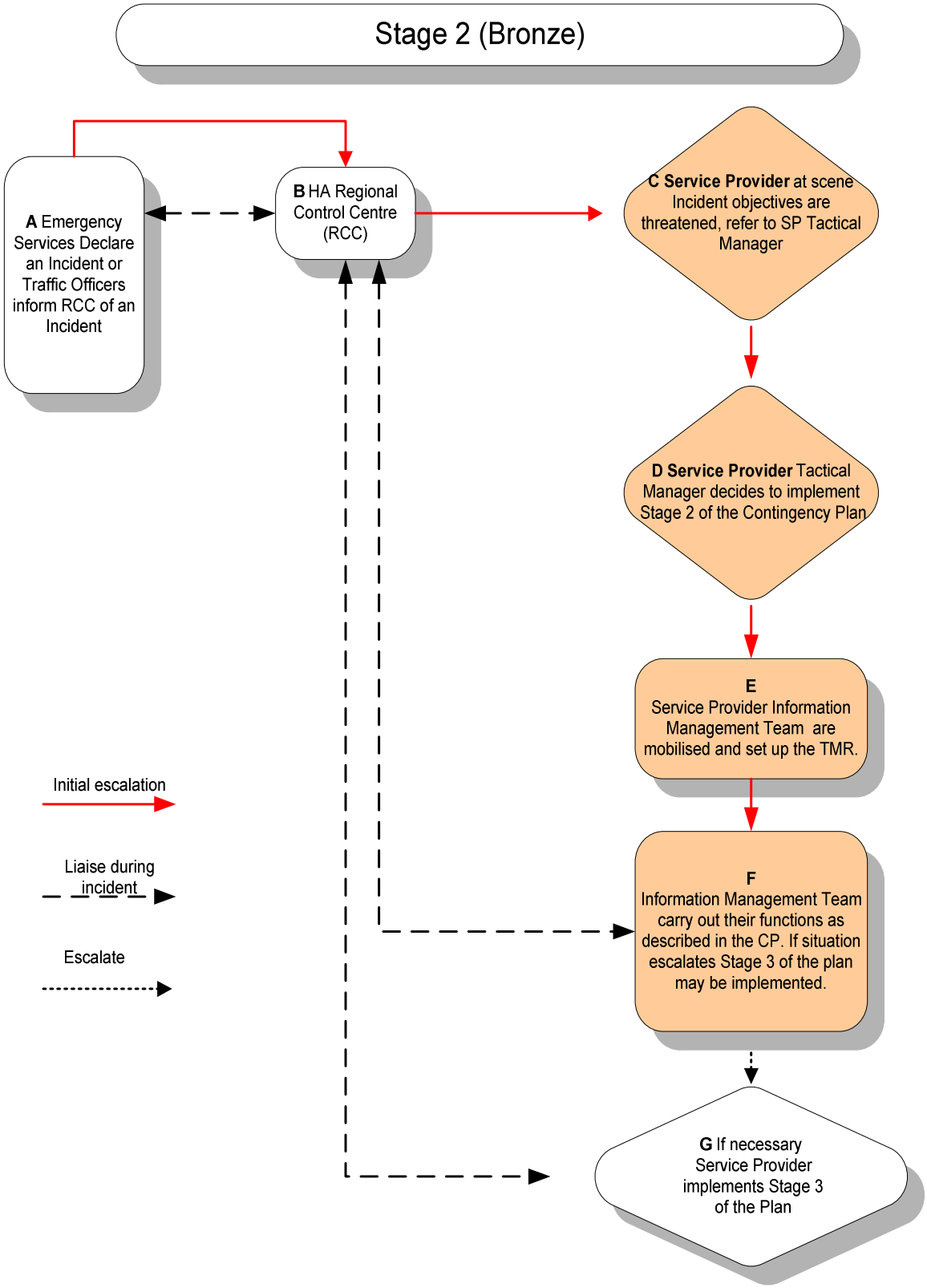
5.1 Introduction

Mobilisation of the IMT (only) is needed where incident objectives are threatened but the operational response is straight forward and does not require tactical management. In these circumstances, the Plan would be "partially" implemented.
The IMT will attend the Tactical Management Room (TMR) and carry out the following duties:

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

Figure 5.1 (on the following page) shows how Stage 2 is mobilised, key actions, and lines of liaison during the Stage. The key actions are explained in the succeeding sections.

Figure 5.1: Partial Mobilisation of the Service Providers Information Management Team



5.2 Box A

Police or Emergency services contact the RCC and inform them of an incident on the Strategic Network. A Traffic Officer contacts the RCC and informs them of an incident on the Strategic Network.

5.3 Box B

The RCC contacts the Service Provider's 24/7 control centre and informs them that there is an incident on the network and that the Traffic Officer or Emergency Services requires assistance.

5.4 Box C

Service Provider's staff at the scene update the Service Provider's 24/7 Control Centre of the events at the incident. If the Incident Objectives are threatened, the Tactical Manager is advised.
Explain:

- *How staff on site decide to contact the Tactical Manager*
- *who they contact*
- *How they contact the Tactical Manager*

5.5 Box D

The Service Provider's Tactical Manager assesses the situation and decides to implement stage 2 of the Plan.
Explain how the decision is then made to escalate to Stage 2, including:

- *how the need to escalate is identified*
- *who authorises the escalation*
- *what criteria influence the decision*

5.6 Box E

The Information Management team is mobilised, goes to the TMR and sets up operations.
Explain how this is done:

- *who is in the Information Management Team*
- *how they are mobilised*
- *how the Team sets up the Tactical Management Room (if not already fully functional)*

Details of the TMR are given in Section 6.

5.7 Box F

The Information Management Team carry out their functions in the TMR.

Explain how this is done:

- *how they decide which Stakeholders to contact*

- *how they obtain information re. the incident*
- *how they monitor media output*
- *how they make contact with RCC and stakeholders and maintain contact*
- *how they keep Service Provider Senior Management briefed (see Section 6)*
- *what information they have at their disposal in the Box of Reference(see section 15)*

5.8 Box G

If the situation deteriorates, the Information Management Team contacts the Tactical Manager and advises the situation.
Explain how this is done:

- *how a deteriorating situation is identified*
- *who the Information Management Team contacts*

The Tactical Manager then decides whether to escalate the Service Provider response to Stage 3, as described in Section 6.

5.9 Process Flow Charts

Include a detailed process flowchart in Appendix F to explain Stage 2, showing the actions of each team or player and the lines of communication between them. .The Service Provider column could be split in to separate columns for individual Service Provider teams. This will amplify Figure 5.1 and enable individuals to better understand the actions they have to take and who they need to communicate with.

An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider. Highlight any points which Plan holders should have drawn to their attention.

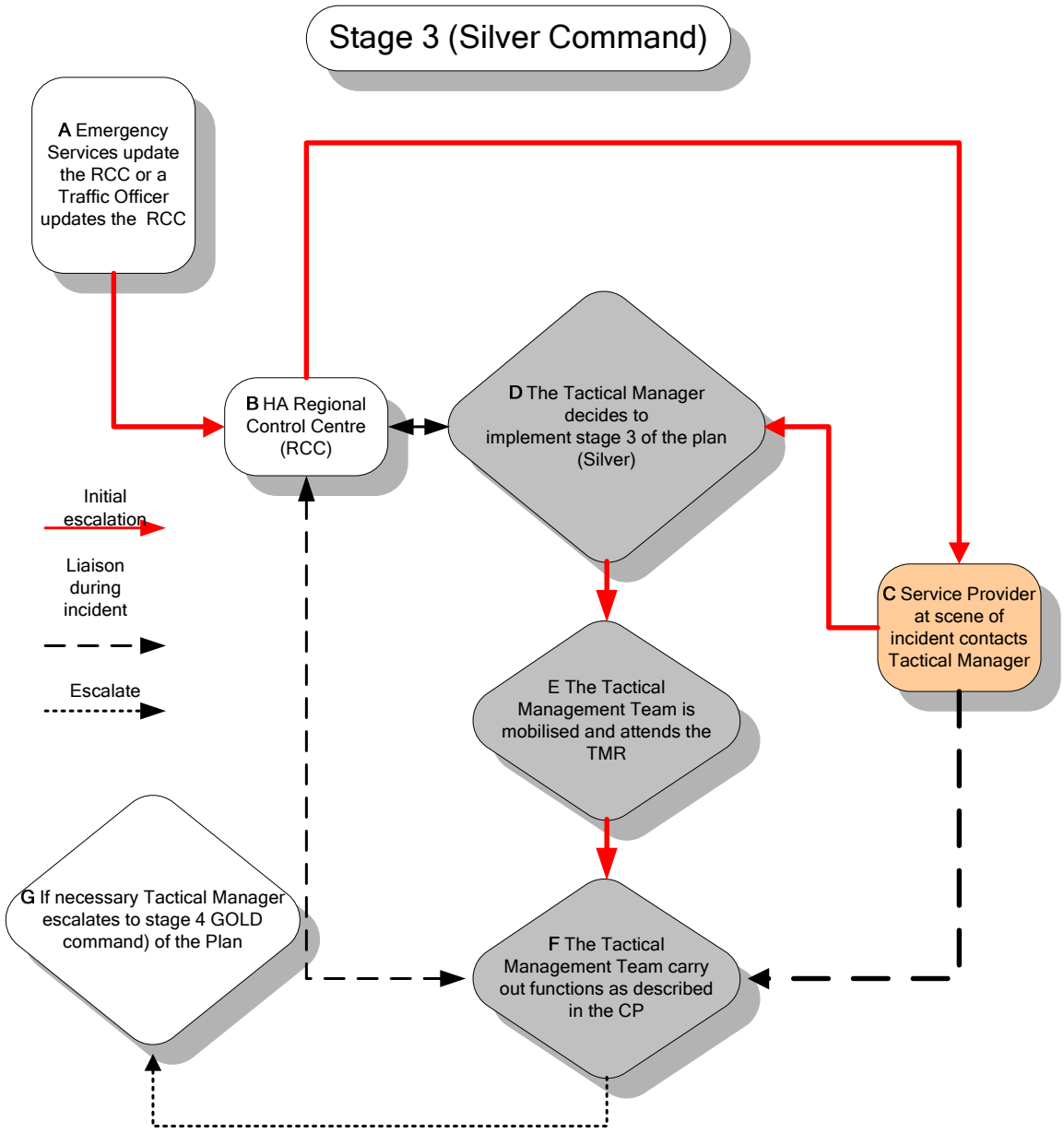
6.0 STAGE 3: SERVICE PROVIDER TACTICAL COMMAND (SILVER)

6.1 Introduction

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

Figure 6.1 shows how Stage 3 is mobilised, key actions, and lines of liaison during the Stage. The key actions are explained in the succeeding sections.

Figure 6.1: Full Mobilisation of the Plan (Silver)



6.2 Escalation to Stage 3

Escalation from Stage 2 to Stage 3 is described in **Section 5**. This Section describes escalation directly from Stage 1 (Standard Incident Response procedures) to Stage 3.

6.2.1 Box A

Police or Emergency services contact the RCC and inform them of an incident on the Strategic Network. A Traffic Officer contacts the RCC and informs them of an incident on the Strategic Network.

6.2.2 Box B

The RCC contacts the Service Provide's 24/7 control centre and informs them that there is an incident on the network and that the Traffic Officer or Emergency Services requires assistance.

6.2.3 Box C

Service Provider's staff at the scene update the Service Provider's 24/7 Control Centre of the events at the incident. If the Incident Objectives are threatened, the Tactical Manager is advised.
Explain:

- *How staff on site decide to contact the Tactical Manager*
- *who they contact*
- *How they contact the Tactical Manager*

6.2.4 Box D

The Tactical Manager decides to escalate Service Provider response to Silver Command.
Explain how this is done:

- *who is authorised to approve the escalation*
- *what factors influence this decision*

6.2.5 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.

Explain how this is done:

- *how the team is mobilised*
- *who is involved in the team*
- *how the TMR is mobilised*

6.3 Silver Command

6.3.1 Box A

Police or Emergency services regularly update the RCC with information regarding the incident.
Traffic Officer regularly updates the RCC with information regarding the incident.

6.3.2 Box B

The RCC is informed that the Service Provider has mobilised its TMT and then liaises with the TMT.

6.3.3 Box C

The Service Provider at the scene of the incident regularly updates the Tactical Manager.

6.3.4 Box D

The TMT manages the incident at a tactical level in liaison with the RCC. Further details of the TMT and the TMR are given below.

6.3.5 Box G

The Tactical Manager will continually monitor the situation and if necessary, will escalate the response to Gold Command.
Explain how this is done:

- *What factors influence this decision*
- *Who the Tactical Manager contacts*
- *Who is authorised to approve the escalation*
- *What are the functions of the TMT in this scenario*

6.4 Tactical Management Team (TMT) and Tactical Management Room (TMR)

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.

6.5 Tactical Management Team (TMT)

6.5.1 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
- Be a forum within which tactical decisions can be made, in conjunction with the Emergency Services, local authorities, 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/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 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 Silver control if requested to act as a Tactical Adviser.

6.5.2 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.

6.6 TMT Structure

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

- Tactical Decision Team
- Information Management Team
- 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.5 lists other resources who may be called upon by the TMT (eg technical specialists).

Specify the minimum numbers of staff from each team to be included in the TMT.
The functions of each team are explained below.

6.6.1 TMT - Tactical Decision Team

This team is formed of staff who 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 Stage 3, and then to act as the Tactical Manager in the TMR.

6.6.2 TMT - Information Management Team

The functions of the Information Management team in a partial mobilisation are set out in Section 5. In a full mobilisation, they will be assisted by Admin staff with communicating with HA and local authorities on operational matters as required. The Information Management Team will be composed of individuals qualified to undertake these functions.

6.6.3 TMT - Administration Team

The Admin 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 (eg roadworks).
- provide admin support to all other members of the TMT including attending to the smooth running of IT and other facilities in the TMR.

6.6.4 TMT - 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 are 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.

6.7 TMT - Organisation

Explain

- *how the TMT is structured*
- *lines of communication within the TMT*
- *external lines of communication*
- *how is it ensured that there will be sufficient staff available in each sub-team to mobilise the whole TMT at all times*

6.8 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.

6.8.1 TMR - Location

Explain where the TMR is located and how it is accessed.

6.8.2 TMR - Facilities

The TMR offers the following facilities:
computers

phone lines

Magnetic display board

Printer

Box of Reference

Digital radio etc.

The list of equipment is whatever the Tactical Management Team (TMT) deem necessary to manage an incident, and should be modified accordingly.

6.8.3 TMR - Setup

If the TMR is not permanently set up for use by the TMT, this section should explain how the TMR is to be set up and equipment activated for use by the Information Management team (partial implementation) or the TMT (full implementation) when the Plan is mobilised.
If there is IT equipment to be used in the TMR then provision should be made for replacement of missing or defective equipment in order to ensure continuity of full operation. Support staff available on a 24/7 basis or, as a minimum, a box of IT spares should be considered.

6.9 Interface with other Service Provider Tactical Teams

This section should explain how the TMT interfaces with other Service Provider tactical teams that may be active at the same time e.g. TMT for Emergency Operational Plans, Winter Maintenance or Special Events.

6.10 Emergency Service Interfaces

Communication between the Area Team and the controlling Emergency Service will be:

LEVEL OF CONTROL	Emergency Service	Service Provider Team
Bronze	Officer in Charge on site	Service Provider staff on site
Silver (communication via RCC)	*Incident Control Room	Service Provider Tactical Management Team
Silver – Strategic (communication via RCC)	Gold Control (if established) or Incident control room	Service Provider Gold Command
* the Incident Control Room may or may not be on site.		

6.11 Service Provider Offices and Depots

Details are given in Appendix B.6

6.12 Process Flow Charts

Include a detailed process flowchart in Appendix F to explain Stage 3, showing the actions of each team or player and the lines of communication between them. .The Service Provider column could be split in to separate columns for individual Service Provider teams. This will amplify Figure 6.1 and enable individuals to better understand the actions they have to take and who they need to communicate with.

An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider.

Highlight any points which Plan holders should have drawn to their attention.

7.0 STAGE 4: SERVICE PROVIDER GOLD COMMAND

7.1 Introduction

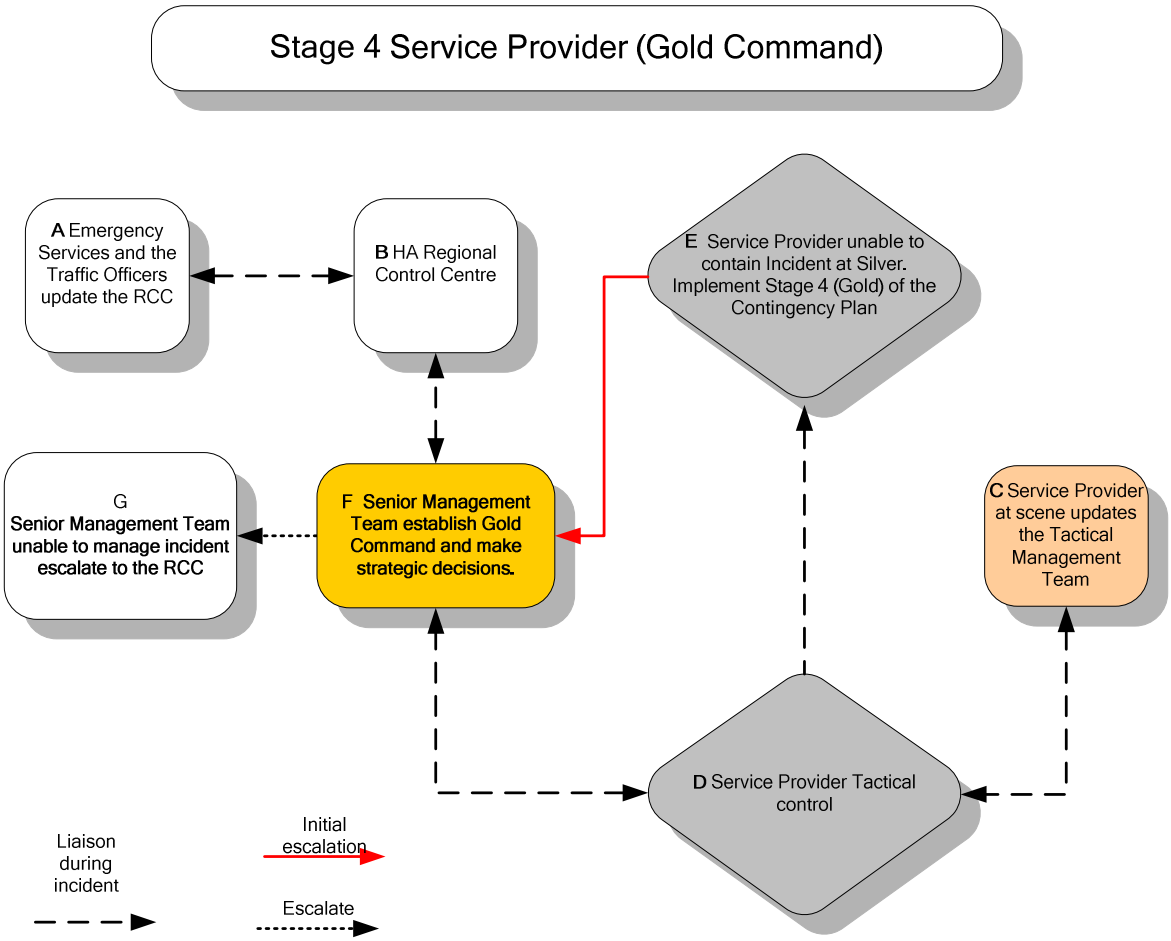
The Service Provider will escalate the plan to Gold level if the incident objectives are still threatened and the situation cannot be managed at a tactical level of command.
For example, this might arise if:

- 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 other adjacent areas.

Strategic decisions and control of the incident are passed to the Service Providers Senior Management Team. The Senior Management Team will then make the Strategic decisions concerning the incident whilst keeping the RCC informed of the situation.

Figure 7.1 (on the following page) shows how Stage 4 is mobilised, key actions, and lines of liaison during the Stage. The key actions are explained in the succeeding sections.

Figure 7.1: Service Provider Gold Command



7.1.1 Box A

Police or Emergency services regularly update the RCC with information regarding the incident. Traffic Officer regularly updates the RCC with information regarding the incident.

7.1.2 Box B

The RCC is informed that the Service Provider has mobilised its TMT and then liaises with the TMT.

7.1.3 Box C

The Service Provider at the scene of the incident regularly updates the Tactical Manager.

7.1.4 Box D

The TMT manages the incident at a tactical level in liaison with the RCC. Further details of the TMT and the TMR are given below.

7.1.5 Box E

The TMT unable to contain the incident at Silver command and therefore escalates the incident to the Senior Management Team to set up Gold Command.

7.1.6 Box F

Senior Management Team establishes Gold Command and makes strategic decisions.

7.1.7 Box G

Senior Management Team unable to contain incident and therefore escalates the incident to the RCC for them to manage.

7.1.8 Process Flow Charts

Include a detailed process flowchart in Appendix F to explain Stage 4, showing the actions of each team or player and the lines of communication between them. The Service Provider column could be split in to separate columns for individual Service Provider teams. This will amplify Figure 7.1 and enable individuals to better understand the actions they have to take and who they need to communicate with.

An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider. Highlight any points which Plan holders should have drawn to their attention.

8.0 STAGE 5: HA REGIONAL CONTROL CENTRE STRATEGIC COMMAND (SILVER)

8.1 Introduction

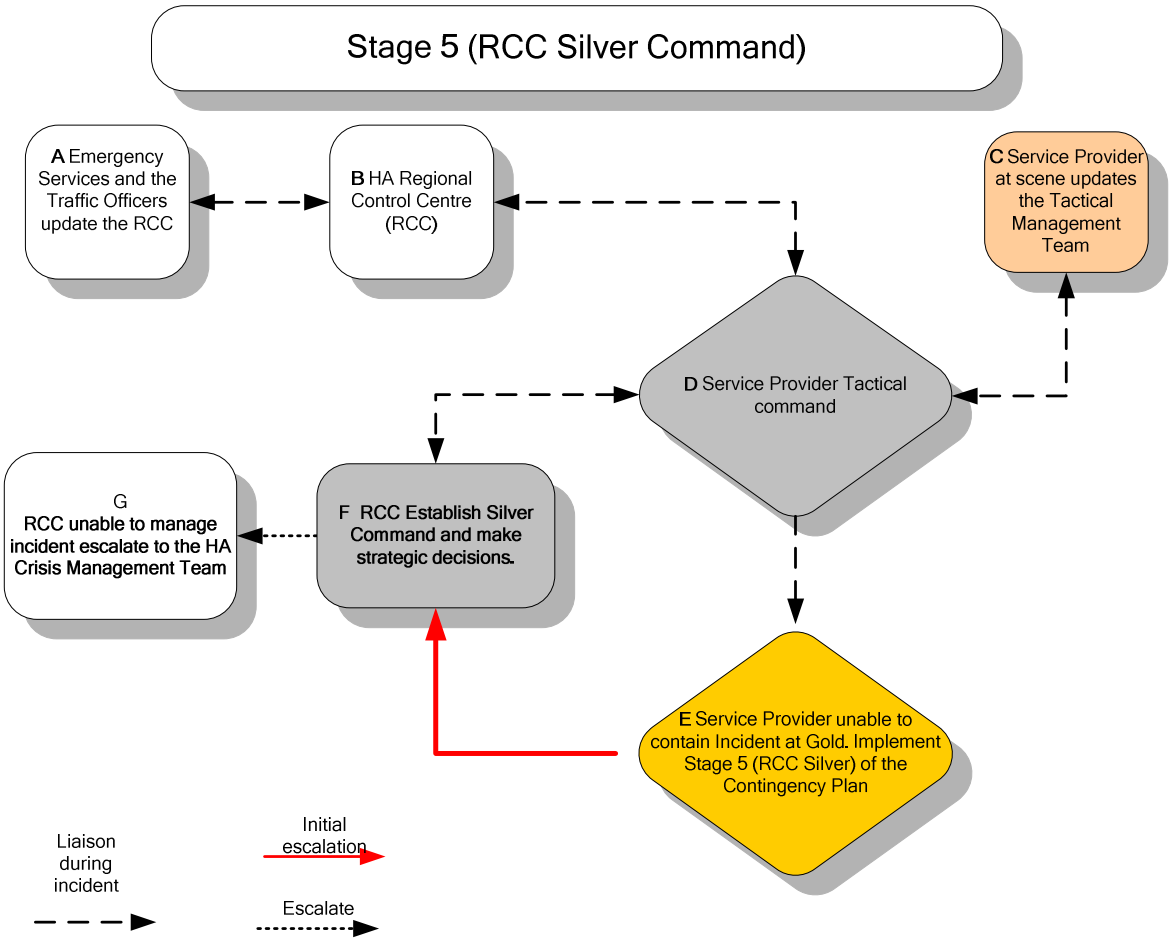
The Service Provider will escalate the plan to RCC (Silver level for them) if the incident objectives are still threatened and the situation cannot be contained at an Area level. For example, this might arise if:

- the Area does not have adequate resources and is unable to obtain them from Adjacent Service Providers
- disruption in the Area is threatening adjacent Areas
- regional wellbeing is threatened

Strategic decisions and control of the incident are passed to the RCC. The RCC will then make the Strategic decisions concerning the incident whilst keeping the relevant HA APM informed of the situation.

Figure 8.1 (on the following page) shows how Stage 5 is mobilised, key actions, and lines of liaison during the Stage. The key actions are explained in the succeeding sections.

Figure 8.1: Escalation to HA Regional Control Centre (RCC)



8.2 Escalation to RCC

8.2.1 Box E

Explain how this escalation takes place:

- *how the need for escalation is identified*
- *who the Service Provider contacts*
- *who authorises escalation*
- *what factors influence this decision*

8.3 RCC Silver Command

8.3.1 Box A

Emergency services contact the RCC and update them on the progress of the incident. Traffic Officer updates the RCC of the progress of the incident.

8.3.2 Box B

The RCC receives up to date information from Emergency Services and the Service Provider concerning the incident.

8.3.3 Box C

The Service Provider at the scene updates the TMT with information concerning the incident.

8.3.4 Box D

The TMT functions as in Stage 3, except that strategic decisions are made by Service Provider Senior Management Team Gold Command. The TMT will provide tactical advice to Gold Command as requested, and will make tactical decisions within the strategic framework defined by Gold Command.

8.3.5 Box E

The Service Providers Senior Management Team takes Strategic command of the incident. If they are unable to manage the incident they escalate to the RCC.

8.3.6 Box F

The RCC set up Silver Command to take strategic command of this incident.

8.3.7 Box G

If the RCC are unable to contain the incident at a Regional level they may decide to escalate command upwards to the National Crisis Management Team. This procedure is described in RCC Contingency Plan and the National Crisis Management Plan.

8.4 Process Flow Charts

Include a detailed process flowchart in Appendix F to explain Service Provider actions during Stage 4, showing the actions of each team or player and the lines of communication between them. This will amplify Figure 8.1 and enable individuals to better understand the actions they have to take and who they need to communicate with. Detailed actions for the HA APM and the RCC need not be shown, except for interfaces with the Service Provider team.
An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider.
Highlight any points which Plan holders should have drawn to their attention.

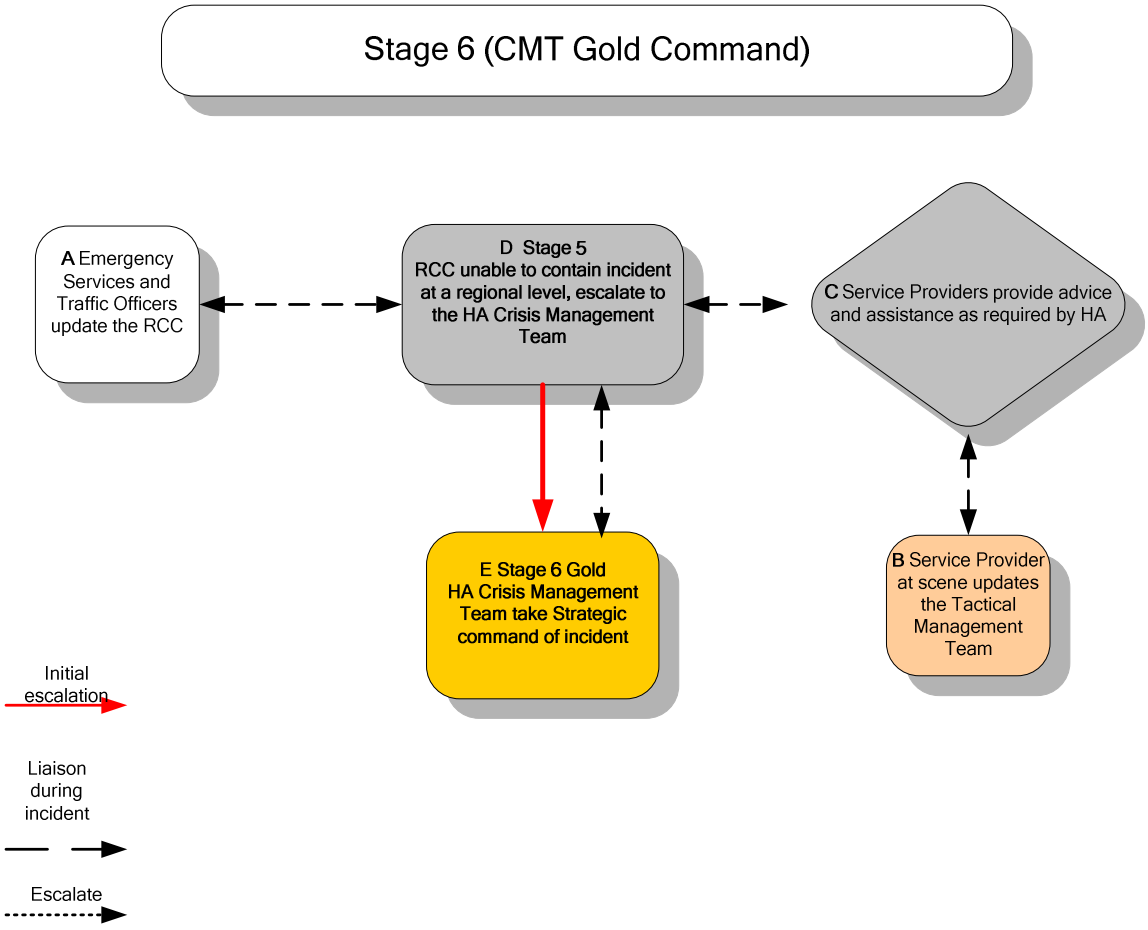
9.0 STAGE 6: HA CRISIS MANAGEMENT TEAM STRATEGIC COMMAND (GOLD)

9.1 Introduction

If the RCC is unable to contain the incident at a Regional level, then they will escalate the incident up to the HA Crisis Management Team (CMT). The HA Crisis Management Team will then make the Strategic decisions concerning the incident.

Figure 8.1 shows how Stage 6 is mobilised, key actions, and lines of liaison during the Stage. The key actions are explained in the succeeding sections.

Figure 9.1: HA Crisis Management Team



9.2 Escalation to HA Crisis Management Team

9.2.1 Box D

RCC decides that the incident or its effects cannot be contained at an Area or regional level and is of national significance. Strategic control of the incident is passed up to HA's National Crisis Management Team.

9.3 Gold Control

9.3.1 Box A

Police and Emergency services contact the RCC and update them on the progress of the incident. Traffic Officer updates the RCC of the progress of the incident.

9.3.2 Box B

The Service Provider's team at the scene update the Service Provider's Tactical Management Team of progress at the incident.

9.3.3 Box C

The Service Providers provide advice and assistance to the RCC, and provide tactical management of the incident within the strategic framework set by the Highways Agency.

9.3.4 Box D

The RCC liaises with the national Crisis Management Team and receive strategic direction. They interpret this strategic direction at a regional or Area level, and provide strategic instruction to the Service Providers.

9.3.5 Box E

HA's national Crisis Management Team takes strategic control of the incident (refer to National Crisis Management Plan).

9.4 Process Flow Charts

Include a detailed process flowchart in Appendix F to explain Service Provider actions during Stage 5, showing the actions of each team or player and the lines of communication between them. This will amplify Figure 9.1 and enable individuals to better understand the actions they have to take and who they need to communicate with. Detailed actions for the Crisis Management team will not be shown.
Detailed actions for the HA APM and the RCC need not be shown, except for interfaces with the Service Provider team.
An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider.
Highlight any points which Plan holders should have drawn to their attention.

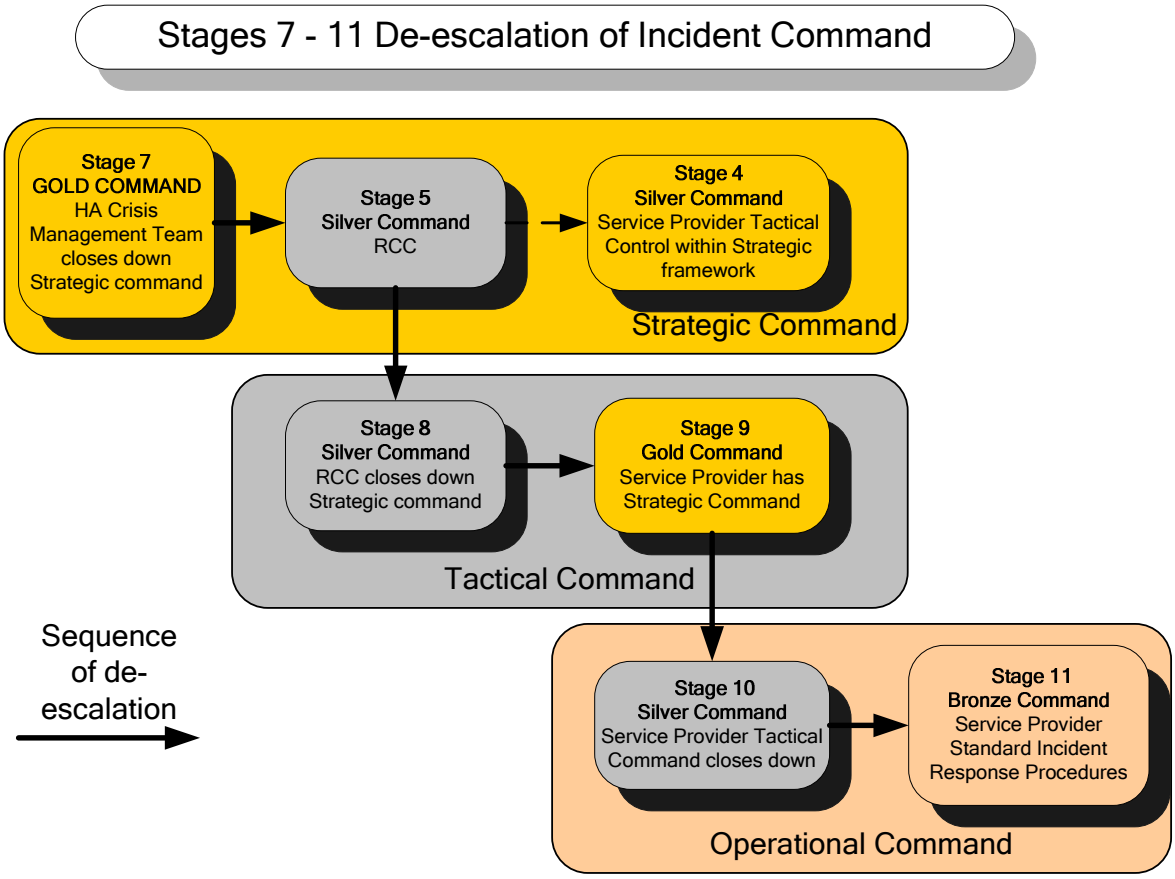
10.0 STAGES 7 - 11: DE-ESCALATION OF INCIDENT CONTROL

10.1 Introduction

As the threat from the incident recedes, command is successively passed back down from the HA Crisis Management team to the RCC, Service Provider Gold Command and finally to Service Provider Bronze command.

Figure 10.1 shows how Stages 7 to 11 are initiated, key actions, and lines of liaison during theses Stages. Each stage is explained in the succeeding sections.

Figure 10.1: De-escalation of Incident



10.2 Stage 7: CMT close down Command of Incident

HA Crisis Management Team decides that the situation no longer needs strategic command at a national level, and passes strategic command to the RCC.
The RCC manage the incident as per **stage 5** in this plan and follow procedures set out in the RCC Contingency Plan and the HA SIMF document.
The service provider will still be operating at Gold (Strategic Command) during the RCC strategic command of the incident.

10.3 Stage 8: RCC closes down Command of Incident

RCC decides that the incident no longer requires strategic command and passes command to the Service Provider. This is a reversion to **Stage 4** of the Plan, and the actions for that Stage are repeated.

10.4 Stage 9: Service Provider closes down Strategic Command of incident

The Service Provider decides that the incident no longer requires Strategic Command and command of the incident reverts to the Service Providers Tactical Command This is a reversion to Stage 3 of this plan.

10.5 Stage 10: Service Provider Command of Incident

The Service Provider decides that the incident no longer requires Tactical Command and command of the incident reverts to the Service Providers Standard Incident Response Procedures. This is a reversion to Stage 1 of this plan.

10.6 Stage 11: Service Providers Commands incident using Standard Incident Response Procedures

The Service Provider manages the incident using its Standard Incident Response Procedures as per Stage 1 of this plan.

10.7 Process Flowcharts

Include a detailed process flowchart in Appendix F to explain Service Provider actions during Stages 7 to 11, showing the actions of each team or player and the lines of communication between them. This will amplify Figure 10.1 and enable individuals to better understand the actions they have to take and who they need to communicate with. Detailed actions for the HA APM and the RCC need not be shown, except for interfaces with the Service Provider team.
An example of an appropriate style of process flowchart is shown in Appendix F of this Model Document, but this should be modified and expanded to suit the needs of each Service Provider. Highlight any points which Plan holders should have drawn to their attention.

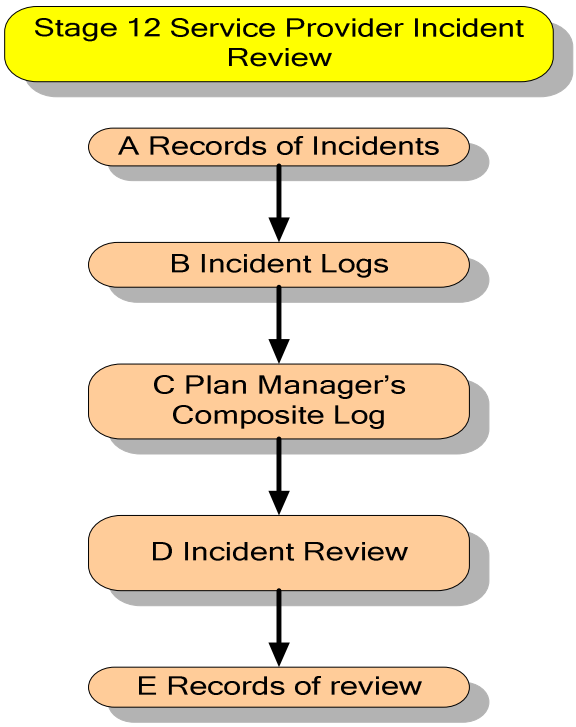
11.0 STAGE 12: SERVICE PROVIDER INCIDENT REVIEW

11.1 Introduction

The Plan format and content need to be reviewed after an incident requiring any stages of the Plan (above Stage 1) to be mobilised. The Service Providers incident review should be in line with guidance from the HA AMM 70/06 which offers guidance on Post Incident Cold Debrief Process. The following is a walk through agenda that the Service Provider should use as a guide.

Figure 11.1 shows the review process needed to achieve this.

Figure 11.1: Service Provider Incident Review



11.2 Box A

When a partial or full Contingency Plan has been implemented, records must be kept of:

- Communications
- Actions
- Decisions

Throughout, 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).

11.2.1 Records of Communications

All communications involving the relay of information and decision making 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
- Summary of response (if any)
- Next actions (if any) as a result of the communication
- Who will take these actions (if any)

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

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

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

11.2.2 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

11.2.3 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

11.3 Box B

Incident logs are summaries of the Records above, and must be completed by:
For the purposes of the Service Provider Incident Review, list the people, teams or organisations who should prepare Incident Logs.

Each log should contain the following information:

- Times and dates of specific communications, actions or decisions made

- Information relayed
- Actions taken
- Decisions made

11.4 Box C

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.

11.5 Box D

The Service Provider will arrange an internal Incident Review adopting the following procedure. Review of incident by key staff involved from:

- List the organisations that should be represented at the review.

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, 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).
- Overall, the 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 2 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.

11.6 Box E

Where an operational 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 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 anyway.

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 a 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.

12.0 STAGE 13: LESSONS LEARNED

12.1 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 HA/other operational procedures, then immediate feedback should be given to the HA so that they can share this with other Areas.

12.2 Personal Incident Debriefing

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

13.0 TACTICAL DIVERSION ROUTE DOCUMENT (DRD)

13.1 Purpose and functions of Tactical Diversion Routes

Diversion routes off HA's strategic network on Local Highway Authorities (LHA) roads are required for tactical diversion to assist incident management. These routes are shown in the DRD.

13.2 Contents of the Diversion Route Document

Explain the contents of the DRD and how this information is to be used – use AMM 71/06 as a guide.

13.3 Classification of Diversion routes

Diversion routes are subject to a formal HA classification (defined in AMM 71/06) to indicate their status in terms of whether they have been approved by Police, Local Authorities etc. These classifications are shown in the DRD.

13.4 2-way Traffic Diversion

If a link in the Service Provider's Area Network is closed in both directions then the relevant Police Force or Traffic Officer will decide if the approved diversion route is capable of accommodating traffic in both directions. If it is not, the Police or Traffic Officer may request (via the RCC) another diversion route from the TMT.

14.0 BOX OF REFERENCE

14.1 Introduction

The Box of Reference contains comprehensive information about the network for use during Tactical and Strategic control of incidents.
There are three Boxes:

- one stored in the Tactical Management Room (TMR)
- one stored at the RCC
- one held by the Service Provider's Contingency Plan Manager.

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.

14.2 Information in Box

The types of information stored in the Box of Reference are summarised below.
There are four types of documents stored in the box of reference:

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

These are explained in more detail below.

14.3 Diversion Route Document (DRD)

Tactical Diversion Routes for the Strategic Network (DRD)
Details of the DRD are given in section 14.

14.4 Major Stakeholder Emergency Plans

Copies of Major Stakeholder Emergency Plans within the Service Providers area should be stored in the Box of Reference. Contact with all Major Stakeholders should be made annually to obtain updated versions of these plans.
List here the Major Stakeholder Emergency Plans stored in the Reference Box.

14.5 Service Provider Operational Plans

Service Provider operational plans should be stored in the box of reference. These may be required by the TMT if they are to be implemented at the same time as the Contingency Plan..
List here the Service Provider Operational Plans included in the Reference Box.

14.6 Reference Information Document

The Reference Information Document stores information that may be required by the TMT when dealing with an incident. This document should store all information required by the TMT that is not otherwise easily accessible. If the information is easily accessible, then a file path name or web

address can be given for quick reference. Types of information that could be stored in this document are listed below.
Under each of the following headings, explain what information is contained in the RID and how it is referenced therein, or indicate how it can otherwise be accessed..

14.6.1 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 HA Network. These can be used for quick reference to check the layout of the Network at a given location.

14.6.2 Emergency Crossover Points

These may be used in Emergencies to enable the Traffic Officers or Police to turn traffic around.

14.6.3 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 network.

14.6.4 Emergency Access Points on Network

These are access points which the Emergency Services can use to gain access to the HA Network

14.6.5 Area Depot Locations

Maps and contact details of all the Service Providers depots on the Area

14.6.6 Stakeholder Contact Details

Contact names, addresses, telephone and e-mail addresses of all Major Stakeholders who may be affected by an incident on the HA network.

14.6.7 Sign Bin Inventory

Maps and lists of contents of all the sign bins on the HA network

14.6.8 Location of CCTV Cameras

A map showing the locations of the cameras and details of who operates the CCTV on the Service Providers network.

14.6.9 Business Continuity

Service Provider's Business Continuity Plan

14.6.10 Network Lighting

A map showing locations and types of Lighting on the HA Network

14.6.11 Location of Traffic Signals

A map showing locations and contact details of who operates the traffic signals on the HA Network

14.6.12 VMS Locations

A map showing locations and types of VMS on the HA Area Network

14.6.13 Major Works

Locations, dates and contact details of major works on the HA Network

14.6.14 External Events

Locations, dates and contact details of External Events impacting on the HA Network

14.6.15 Police Boundaries

A map showing locations and details of Police Boundaries on the HA Network

14.6.16 Emergency Services

Contact details of all relevant Emergency Services in the HA Area Network

14.6.17 Traffic Officer Boundaries

A map showing locations and details of Traffic Officer Boundaries on the HA Area Network

14.6.18 High Risk Weather sites

A map showing locations of all high risk weather sites on the HA Area Network

14.6.19 Hazardous sites adjacent to the Strategic Network

A map showing locations of all hazardous sites adjacent to the HA Area Network that would cause major disruption to the network.

14.6.20 Network Rail Bridges over the strategic network

A map or table showing locations of all Network Rail Bridges that run over or under the HA Area Network

14.6.21 Welfare

Contact details for welfare assistance if required by the Service Provider or HA Personnel

14.6.22 Financial Implications (Green Claims)

Contact details and procedures for financial claims involving incidents on the network.

14.6.23 Plant and Equipment

Types of Plant and equipment that may be required during of after an incident on the network and also contact details if required.

14.6.24 Specialist Contractors

Contact details and locations of specialist contractors that may be required to attend the scene of an incident.

14.6.25 Communication Systems

The types of communication systems used by the service provider should be explained in this section.

14.6.26 Liaison with Adjacent Areas

This section should contain contact information regarding details and procedures on how to contact and work with adjacent Areas.

15.0 PLAN MANAGEMENT

15.1 Plan Manager

Give details of the Plan Manager, including contact details

15.2 Plan Holders and Distribution

The plan should be distributed to all personnel who are involved in any procedure or process within the Contingency Plan. Include a list of plan holders in Appendix A. This list should include Traffic Officers, RCC's, Major Stakeholders such as the Local Authorities, Police Forces, Adjacent Service Providers and the HA Area teams.

All plan holders are listed in Appendix A of this document. Appendix A shows how the plan is to be distributed to each plan holder in the form of a

Hard Copy
CD Copy

15.3 Plan Updates

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

APPENDIX A PLAN HOLDERS

Below is an example of a heading for a list of Plan holders. The Plan holders should be individuals within such agencies that are involved in the incident or may be affected by the impact of the incident.
If further contact details are given elsewhere in another context e.g. in another Appendix or in the Box of Reference, please insert details in this table.

Further contact details in:	Copy Number	Name	Organisation	Position	E-mail address	CD/ Hard copy

APPENDIX B CONTACT DETAILS

B1 Tactical Decision Team

Name	Position	Contact information
Tactical Decision Team		
Person 1		Work: Fax: Mobile: **Home:** Email:
Person 2		Work: Fax: Mobile: Home Email:
Person 3		Work: Fax: Mobile: Home: Email:
Person etc		Work: Fax: Mobile: Home: Email:

B2 Senior Management Team

Name	Position	Contact information
Senior Management Team		
Person 1		Work: Fax: Mobile: **Home:** Email:
Person 2		Work: Fax: Mobile: Home Email:

Name	Position	Contact information
Senior Management Team		
Person 3		Work: Fax: Mobile: Home: Email:
Person etc		Work: Fax: Mobile: Home: Email:

B3 Information Management team

Name	Position	Contact information
Communication Team		
Person 1		Work: Fax: Mobile: **Home:** Email:
Person 2		Work: Fax: Mobile: Home Email:
Person 3		Work: Fax: Mobile: Home: Email:
Person etc		Work: Fax: Mobile: Home: Email:

B4 Administration Team

Name	Position	Contact information
Administration Team		
Person 1		Work: Fax: Mobile: **Home:** Email:
Person 2		Work: Fax: Mobile: Home Email:
Person 3		Work: Fax: Mobile: Home: Email:
Person etc		Work: Fax: Mobile: Home: Email:

B5 Service Provider other resources that may be required

Name	Position	Contact information
Other Resources		
Person 1		Work: Fax: Mobile: **Home:** Email:
Person 2		Work: Fax: Mobile: Home Email:
Person 3		Work: Fax: Mobile: Home: Email:

Name	Position	Contact information
Other Resources		
Person etc		Work: Fax: Mobile: Home: Email:

B6 Service Provider Area Offices and Locations

Name	Position	Contact information
Office 1		Work: Fax: Mobile: **Home:** Email:
Office 2		Work: Fax: Mobile: Home Email:
Depot 1		Work: Fax: Mobile: Home: Email:
Depot 2 etc		Work: Fax: Mobile: Home: Email:

B7 HA Area and Regional Contacts

Name	Position	Contact information
	Duty Press office	Work: Fax: Mobile: **Home:** Email:

Name	Position	Contact information
	RCC Network Operation Manager	Work: Fax: Mobile: Home Email:
	Area Performance Manager	Work: Fax: Mobile: Home: Email:
		Work: Fax: Mobile: Home: Email:

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 the local authority 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 mobilization and organization of the emergency services and supporting organizations, 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 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 for a period of 1 hour or more.
12. Suicide or attempted suicide resulting on the closure of lanes or carriageways.
13. Roadworks 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. The provision of welfare support.

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 contactor

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

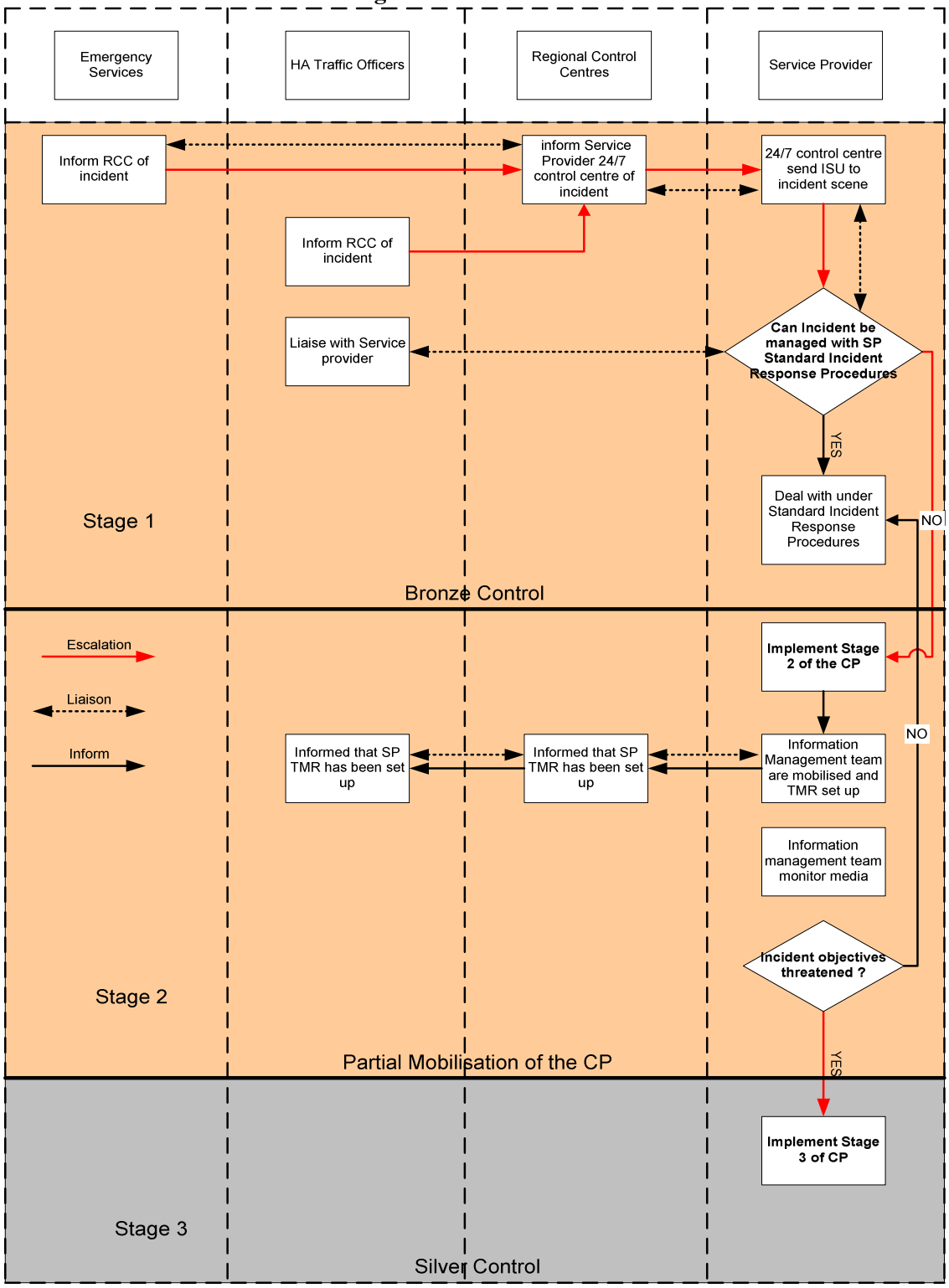
This is an example of a glossary but should be modified to suit the contents of the Service Providers own plan.

ACPO	Association of Chief Police Officers
AMM 70/06	Highways Agency "Area Management Memo"
Bronze Level Response	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
Control Centre	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
Diversion route	A pre-planned route to take traffic away from an incident site
ECP	Highways Agency "Emergency Contact Procedures"
Standard Incident Response Procedures	Service Provider established plans for dealing with routine Network incidents
Gold Level Response	Strategic Management of the incident by HA Area teams
HA Area Team	Highways Agency Area performance Managers 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
IMT	Service Providers Incident Management Team
NILO	HA National Incident Liaison Officer
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 Response	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”
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.
TO	Traffic Officer, from the Highways Agency Traffic Officer Service.

APPENDIX F EXAMPLE OF A PROCESS FLOW CHART

Figure F.1: Process Flow Chart



Annex 7.17.1 Identification of Canine Fatalities Form

Date:	
Time:	
Location:	

Colour	
Small (height to shoulder <30cm)	
Medium (>= 30 cm <45cm)	
Large (>45cm)	
Coat type (short, long or curly)	
Distinguishing marks	
Collar type/colour	
Identity Disc/ Owners Details	
Ear Tattoo Details	
ID Chip No	

Owner notified	
Police notified	
Local authority dog warden notified	
PetLog notified	
Nat. Dog Tattoo Reg. notified	

Contact Details

PetLog: www.thekennelclub.org.uk/caring/petlog.html

National Dog Tattoo Register: www.dog-register.co.uk/
Tel: 01255 552455
Email: tattoo@dog-register.co.uk

Annex 7.18.1 Rapid Re-opening of Running Lanes Following Diesel and other Hydrocarbon Spillages - Risk Example

This risk table gives the first consideration on the overall risk generated by a diesel incident following spillage from a Large Goods Vehicle involved in a serious injury incident.

Table Annex 7.18.1 Completed Risk Matrix Table

	Impact	**Low (1)**	**Medium (2)**	**High (3)**
Probability				
Low (1)		A	E	
Medium (2)			C	B
High (3)			D	

Risk

B. Spillage of diesel as a result of recovery
C. Excessive treatment of the pavement for the level of damage
D. Skid potential
E. Rutting
F. Binder loss leading to break up of pavement material

Overall risk figure:	A= 1x1	= 1
	B= 2x3	= 6
	C= 2x2	= 4
	D= 3x2	= 6
	E= 1x2	= 2
	Total figure	=19

A total figure of 19 indicates that options of no treatment, or absorbent and grit sand methodology, might not be appropriate.

Risk A

The potential for a future spillage from a diesel container has already been classified at the lowest possible level, therefore it cannot be reduced.

Risk B

Excessive treatment may score high if vehicles involved in an incident prevent a full consideration of the impact and effect of the diesel spillage on the pavement.

Risk C

Scoring risk C, skid potential, at 4, indicates concern over diesel on the pavement. If an absorbent is applied this may reduce the concern so that it may be reclassified, in a future assessment.

Risk D

Rutting may be a concern at the outset, but if no ruts are evident, then this risk score can be reduced. Rutting will take time to occur, unless the pavement has been extensively damaged, so a reduced risk score should not represent a reduction in the level of service provided to motorists. Monitoring should follow re-opening and treatment planned if rutting becomes evident.

Risk E

The diesel may not have been on the carriageway long and the potential for it to have affected the binder to any significant extent is considered minimal. However, if the diesel had collected in an existing defect location, such as a pothole, there is a potential for localised effects to be more severe and have an impact on the clearance of the diesel and re-opening of running lanes.

Annex 7.18.2 Rapid Re-opening of Running Lanes Following Diesel and other Hydrocarbon Spillages - Possible Treatment Options

In order of least time required to implement treatment and likely resultant delay to motorists:

- Nothing
- Grit sand
- Absorbent and grit sand
- Wash / jet wash
- Detergent and wash / jet wash
- Infra-red heating (still under testing)
- Plane and Pave
- Other