

Annex A

National Telecommunications Contingency

Consultation Action Plan

National Telecommunications Contingency Program

Table of Contents

0	Introduction to Action Plan	6
0.1	Background	6
0.2	Document Purpose	6
0.3	Three Primary Beliefs.....	6
0.4	Scope.....	7
0.5	Document Roadmap	7
Section 1:	Action Plan Overview	9
1.1	General.....	9
1.2	Definitions and Explanation	9
1.3	Action Plan Methodology	11
Section 2:	Critical Landscape	13
2.1	Impact to the general population.....	13
2.2	Crisis Scenarios and Emergency Conditions.....	14
2.2.1	General	14
2.2.2	Management Summary	14
2.2.3	Full List of Potential Scenarios and Critical Events	15
2.3	Critical Sectors and Organizations	16
2.3.1	Management Summary	16
2.3.2	Full List of Potential Critical Sectors and Organizations	16
2.4	Critical Telecommunications Services	17
2.4.1	Description.....	17
2.4.2	Management Summary	17
2.4.3	Full List of Critical Telecommunications Services	18
2.5	Critical Telecommunications Infrastructure	19
2.5.1	General Purpose and Scope	19
2.5.2	Full List of Potential Critical Infrastructure.....	19
Section 3:	Triggers.....	21
3.1	General.....	21
3.2	Triggers.....	21
3.2.1	Factors Invoking the NTC Action Plan	21
3.2.2	Trigger Analysis.....	22
3.2.3	Invocation Triggers	23

3.2.4	Planned Maintenance Outages	25
3.2.5	Trigger Reporting.....	26
Section 4: Action Plan Invocation		27
4.1	Purpose and Scope	27
4.2	Invocation Definition	27
4.2.1	What is the Invocation?	27
4.2.2	Purpose of Invocation	27
4.2.3	Carriers Definition of Invocation.....	28
4.2.4	General Comments.....	28
4.3	Decision-Makers and roles	29
4.4	Invocation Decision Making Method	29
4.4.1	Who Decides?	29
4.4.2	Communications	29
4.5	Invocation Process – Call Trees.....	31
4.5.1	What is a call tree?.....	31
4.5.2	What information do the callers provide?.....	31
4.5.3	Where is the call tree held?	32
4.5.4	What does the leadership team do?.....	32
4.5.5	Who will update the contact details and ‘call-tree’, and who will distribute?.....	32
4.6	Carriers’ Actions Timetable	32
4.6.1	Carriers’ Actions/Activities Timetable for the Resolution of Emergencies 32	
4.7	Invocation Routes and Methods	34
4.7.1	Phone number	35
4.7.2	Statement.....	35
4.7.3	Confidentiality	35
4.7.4	Security	35
4.7.5	Automated Information.....	36
4.8	Communications between Carriers and EETT.....	36
Section 5: Crisis Management and Action Plan.....		37
5.1	Purpose and Scope	37
5.1.1	Interests of the main actors	37
5.1.1.4	Carriers.....	38
5.2	Crisis Management Definition	38

5.2.1	Levels of Crisis Management/Action Plan	38
5.3	1st Level Carrier Actions	39
5.3.1	Immediate Carrier Response.....	39
5.3.2	Carrier internal staff during NTC	40
5.3.3	Crisis Relief Tool Initiation	40
5.3.4	Call Priority Initiation	40
5.3.5	Call Duration Control Initiation.....	40
5.3.6	Other Call Controls	41
5.4	2nd Level Actions After CMT Activation.....	41
5.4.1	CMT Tasks.....	41
5.4.2	CMT member role descriptions	42
5.4.3	CMT Members.....	44
5.4.4	Communications	45
5.4.5	Invoking Responsibilities.....	47
5.4.6	Crisis Management Preparation	49
5.5	Service/Business Resumption.....	50
5.5.1	NTC CMT Closure Decision Triggers.....	51
5.5.2	Closure	51
5.6	Detailed Trigger Specific Action Plans	52
5.6.1	Event, Service, Sector and Trigger Association	52
5.6.2	Trigger associated Action Plans.....	52
Section 6:	Reporting	76
6.1	Carrier Bi-annual Service Management Reports	76
6.1.1	Purpose.....	76
6.1.2	Metrics and Key Performance Indicators Report Contents	76
6.1.3	Periodicity	77
6.1.4	Governance	78
6.1.5	Communication and Feedback.....	78
6.2	CMT Problem Management Report	79
6.2.1	Background	79
6.2.2	Purpose.....	80
6.2.3	Report Data Content	80
6.2.4	Periodicity	81
6.2.5	Governance	81
Section 7:	Tools and Preparatory Activities.....	82

7.1	CMT Location Support	82
7.1.1	Carriers.....	82
7.1.2	EETT	82
7.2	Media and Carrier Communications	86
7.2.1	Carriers.....	86
7.2.2	EETT	87
7.3	Recovery Environments	88
7.3.1	Carriers.....	88
7.4	Reporting	97
7.4.1	Carriers.....	97
7.4.2	EETT	97
1	Appendix 1 - Bibliography	98
2	Appendix 2 - Acromyms.....	101

0 INTRODUCTION TO ACTION PLAN

0.1 BACKGROUND

The project can be summarized with the following statement:

“To provide a National Telecommunications Contingency environment, coupling the Telecommunications Service Providers committed to ensure minimal national disruption for telecommunications consumers and Critical Sectors / Organizations and the telecommunication service requirements in times of crises”

There is end-user/consumer value and socioeconomic benefits to Greece in the development of an integrated and ‘advanced’ telecommunications response to crises. The National Telecommunications Contingency Plan (NTC) is an initial attempt to establish this crisis response.

0.2 DOCUMENT PURPOSE

This document defines the requirements, processes and procedures which the telecommunications Carriers in cooperation with EETT will need in order to support a national telecommunications contingency plan.

The objective to this information is to be used as part of a national contingency plan in order to support and mitigate severe, prolonged, or damaging telecommunications disruption.

0.3 THREE PRIMARY BELIEFS

The action plan has been developed based on the foundation that in an emergence situation the continuity of telecommunications services is critical to the uninterrupted way of life, stability of society and sustained wellbeing of the population. The National Telecommunications Contingency Plan aims at maintaining these “Three Primary Beliefs” which are outlined below.

- Way of Life: A telecommunications failure detrimentally affects Greek way-of-life and the ability of the nation to continue in the same way as prior to the event. For example, major telecommunications disasters could impact goods delivery and therefore cause problems in people’s living.
- Stability: Government and social stability are affected by telecommunications services outages, resulting in a loss of confidence in the State apparatus and ability to react to events.
- Human Welfare: During telecommunications outages general public personal welfare and health are either placed at significant risk, or result in casualties which are considered intolerable for both the population generally and the Government.

0.4 SCOPE

The action plan has the following scope:

- It is concerned with any telecommunications outage or change to the current operating model, threatening the Three Primary Beliefs.
- The primary focus is on the telecommunication ‘users/consumers’ – either directly by being unable to use personal communications or indirectly through their need to contact Critical Sectors and Organizations such as emergency services (e.g. police, fire brigade, rescue teams, hospital services etc.) whose services have been impacted.
- It addresses any likely disaster scenario and subsequent impact upon the telecommunications infrastructure and services offered to the ‘users/consumers’.

What is considered out of scope is:

- The Carriers’ internal disaster recovery plans. It is assumed that Carriers have implemented sufficient resiliency for commercial reasons and have considered the consequences of insufficient protection. For the benefit of the Carriers this program suggests improvements for consideration (see Section 7: Tools).

0.5 DOCUMENT ROADMAP

This document contains besides the introduction (Section 0), seven more sections defining and describing the Action Plan). The context of the remaining six Sections is the following:

- Section 1 “Action Plan Overview”: an outline of the general process used as part of the national telecommunications contingency planning.
- Section 2 “Critical Landscape”: The crisis scenarios (i.e. emergency events) and an outline of those sectors and organizations, telecommunications infrastructure and services considered, and for which the Action Plan is designed to address.
- Section 3 “Triggers”: the technical trigger-points and measurements that are used to determine whether the National Telecommunications Contingency Action Plans are activated by the telecommunications Carriers, service providers and EETT.
- Section 4 “Action Plan Invocation”: an outline of the method for invoking the “national telecommunications contingency action plans” and the Crisis Management Team (CMT).
- Section 5 “Crisis Management and the Action Plan”: an outline of the actions activities, roles and responsibilities, communications, and tools used within the crisis management environment, as well as a definition of the disengagement point once the crisis is eventually resolved or has been reduced.
- Section 6 “Reporting”: an outline of the management reporting of events during the post-crisis period.
- Section 7 “Tools”: an outline of the tools and processes required to sustain, implement, support, modify, update the Action Plan to keep it relevant to any

lessons learned, changes in technology and services, changes in user emphasis etc.

SECTION 1: ACTION PLAN OVERVIEW

1.1 GENERAL

This Section includes:

- A set of definitions and explanations of the used terminology.
- An overview of the NTC Action Plan methodology.

1.2 DEFINITIONS AND EXPLANATION

Where appropriate, it is proposed that the Business Continuity Institute (BCI) terms and glossary are adopted as part of this programme. This can be found on:

<http://www.thebci.org/Glossary.pdf>

In addition, “this project.

Table 1: Term Definition and Explanation” below is a list of terms and definitions specific to this project.

Table 1: Term Definition and Explanation

Term Definition	Explanation
NTCP (National Telecommunications Contingency Program)	National Telecommunications Contingency Program: the initiative by EETT to establish a robust and highly integrated approach to crisis management planning and thinking within the Greek Telecom Sector.
NTC	National Telecommunications Contingency
NTC Action Plan	The detailed actions to counteract against telecommunications services outages upon the telecommunication networks and impact as a result of crisis or catastrophic event.
Internal Disaster Recovery Plan	A self contained set of activities that are activated in case of emergency. Within the scope of the NTCP, Disaster Recovery Plans refers to Carriers’ internal plans and actions.
Critical Telecommunications Services	The ‘Telecom Services’ offered by the Carriers – dialled services, mobile telephony, etc., prioritised and required to be available at a time of crisis. It is a prioritized list of a subset of the Telecommunications Carriers’ full service offering which is deemed “mission Critical” in support of the Critical Organizations and Sectors. Through a scoring mechanism, a short list has been created.

Term Definition	Explanation
Critical Organizations & Sectors	Critical Sectors and Organizations in the economy and the society in general – health services, fire prevention, ambulance service etc. – and for which the Critical Telecommunications Services will be prioritized and made available. It is a list of all the Organizations and Sectors deemed ‘Critical’ to the nation and which need the telecommunication services to be available in order for them to ‘survive’ and continue supporting the wellbeing of the general public and the socioeconomic backbone of the country.
Critical Telecommunications Infrastructure	The Carriers’ infrastructure which forms the foundation and supports proper operation of the Critical Telecommunications Services.
Crisis Scenarios	A ‘typical’ major incident that would precipitate an Emergency Condition and which would result in excessive telecommunications services demand or outages. It includes a list of proposed scenarios for which the NTC Action Plan is designed to assist. In developing the list we took also into account the feedback from the Carriers (given by answering a questionnaire issued on January 2005) in order to identify the best method for implementing a suitable contingency environment and which will support the further consultation, implementation and deployment recommendations.
Triggers	A list and description of metrics, and performance levels associated with the Crisis Scenarios, Critical Organization telecommunications needs, and Critical Telecommunications Services which once breached Invocation of the associated Action Plan is initiated.
CMT	The process by which a unified Crisis Management Team consisting of Carrier and EETT representatives comes together to address the crisis and manage the Action Plan.
Crisis Management	The steps and the procedures required to address the particular crisis. This is the heart of the Action Plan.
Reporting	<p>A set of crisis event reports designed to reduce the likelihood of a crisis and inform all stakeholders when one does occur. Reports are categorized as follows:</p> <ul style="list-style-type: none"> • Biannual Service Management Reports. They are reports submitted periodically in order to provide the ability of trend analysis and the prevention of possible emergency situations. • Problem Management Reports. They are reports that are issued after a contingency in order to promote the experience accumulation and any good practices for confronting emergencies.

Term Definition	Explanation
Tools	<p>A set of recommendations designed to:</p> <ul style="list-style-type: none"> a) Assist the Crisis Management Team to perform its duties. b) Assist the Crisis Management Team in communicating with the Media and the General Public. c) Introduce a set of processes, procedures and technical recommendations which can be used to reduce the likelihood of a crisis event or expedite resolution.

1.3 ACTION PLAN METHODOLOGY

The Action Plan is based on the process flow defined in Figure 1: NTC Process Flow. Which is further elaborated in subsequent chapters.

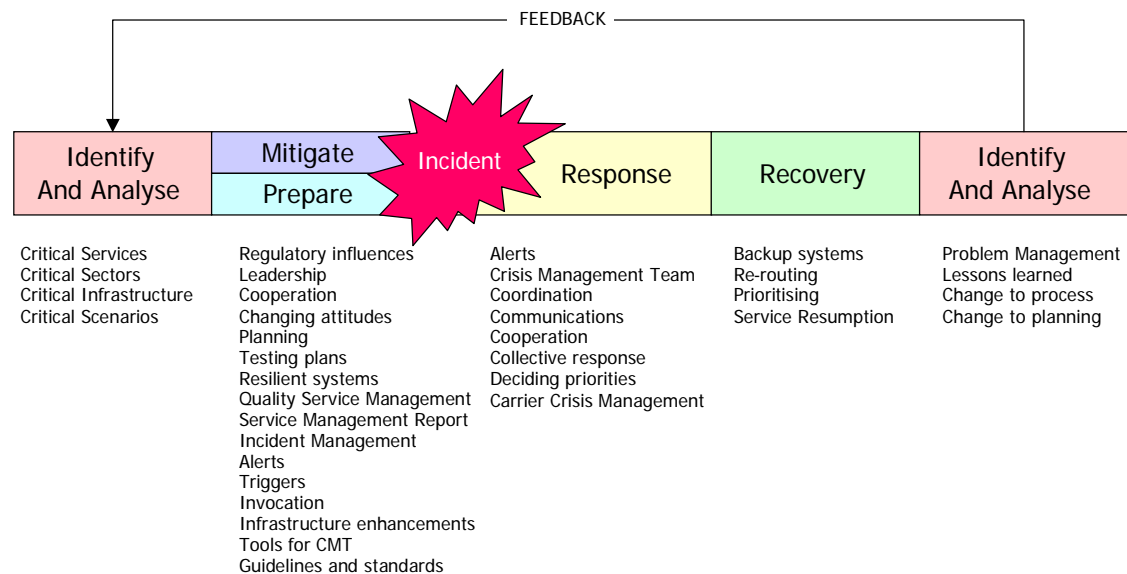


Figure 1: NTC Process Flow.

The initial Identification and Analysis presenting the Critical Telecommunication Services, Critical Sectors and Organizations, Critical Telecom Infrastructure and short listed Event Scenarios has been performed as described in Section 2: “Critical Landscape”. The identification of the critical landscape was used to define triggers for action once a problem or an emergency event associated with a critical landscape item developed. The trigger definition is described in Section 3: “Triggers”. The Identification and Analysis process is an ongoing process which will be performed by the Crisis Management Team after each Crisis Event in order to optimize and enhance the crisis management process and infrastructure resiliency. Based on the criticalities a set of Preparatory and Mitigating activities have been analyzed and documented as part of the NTC project. Upon a Crisis Event, the process depicted in Figure 2: Action Plan Process Flow will be initiated. Crisis Events breach a defined Trigger which in turn activates a set of “1st Level Actions” by the Carriers and the Activation of the Crisis Management Team. The Crisis Management engages in the resolution of the problem with a set of “2nd Level Actions”. Upon resolution of the problem the activities

associated with “follow-Up and Closure” are performed. The detailed Action Plan is presented in Section 5: “Crisis Management and Action Plan”.

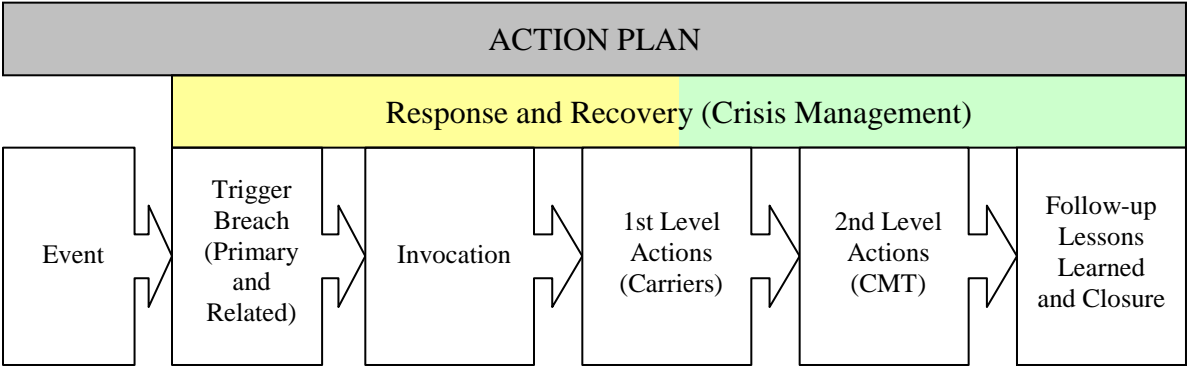


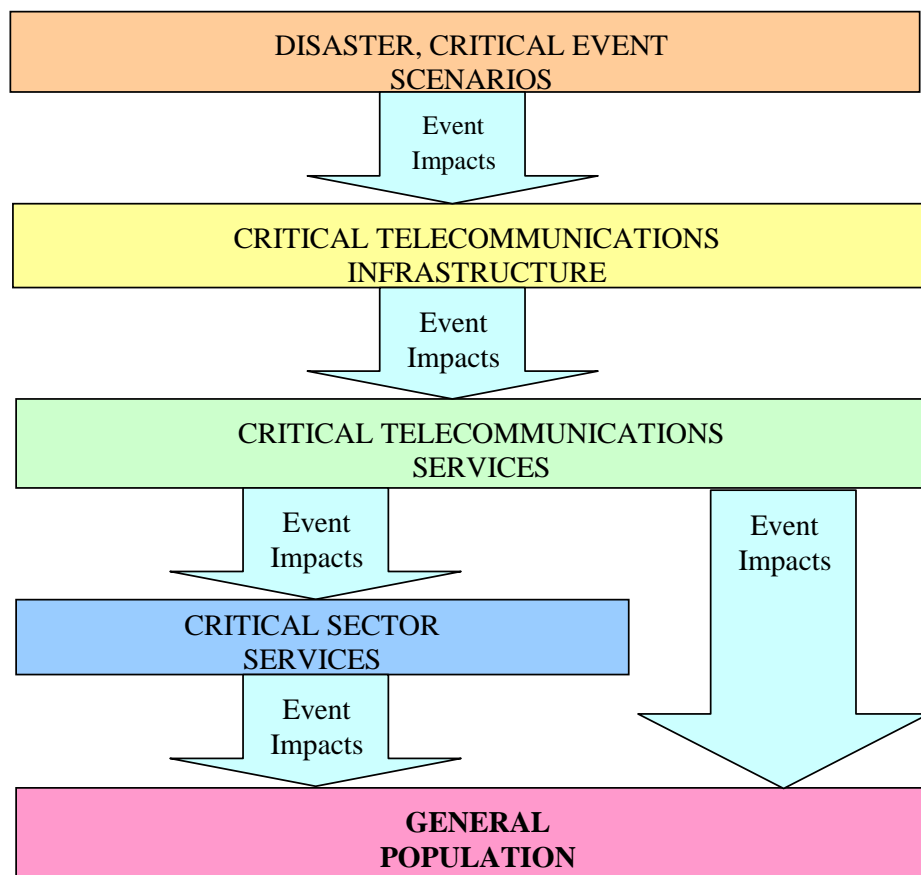
Figure 2: Action Plan Process Flow

SECTION 2: CRITICAL LANDSCAPE

2.1 IMPACT TO THE GENERAL POPULATION

The flow diagram below outlines the relationship between the short listed Disaster Event Scenarios and the impact to the telecommunications infrastructure and services and eventually the general public ‘end-users/consumer’. The impact to the end-user/consumer can be two fold. Directly due to the potential loss of his/her personal communications or indirectly through the loss of vital communications channels with critical sector organizations which can impact his/her health, wellbeing, financial state and established way of life.

Critical Event Impact Flow



2.2 CRISIS SCENARIOS AND EMERGENCY CONDITIONS

2.2.1 General

In reality, there is a plethora of possible scenarios and variances, some focussing on events, others focussing on equipment (for example “fire within a major telephone exchange” is an event, whilst “major telephone exchange failure” is the corresponding equipment focus).

The perspective of the scenarios is from the vantage point of “the national interest” an amalgamation of economic and industrial concerns together with people and health concerns.

The scope of this section is to list the many ‘event-driven’ scenarios; this can cover a wide spectrum of inter-related activities and consequences (for example an earthquake disrupts telephone exchanges, cabling, staff availability, etc.).

2.2.2 Management Summary

There are nearly 40 categories of scenarios that have been identified and developed further. Out of these categories the following 14 have been short listed and selected based on a scoring approach that has taken into account the probability and the impact to the way of life, stability and human welfare in Greece. They have been categorized as

- External to the telecommunication environment Crisis and Emergency Event Scenarios.
- Events which directly involve and impact the Telecommunications Infrastructure.

External Crisis and Emergency Event Scenarios

1. Chemical/Nuclear Incident (inside or outside Greece) – non fission explosion
2. Nuclear Incident (inside or outside Greece) – fission explosion
3. Earthquake
4. Inland Flooding
5. Coastal Flooding and Tsunami
6. Forest Fire and Scrub Fires
7. Acts Targeting Industrial and Commercial Centres
8. Virus and Malicious attacks on the Carriers
9. Sudden Income Changes (for a Telecommunications company)

Telecommunications Infrastructure Impact Scenarios

1. Infrastructure Component Failure
2. General Infrastructure Fires (e.g. fire in a major Telecom Carrier infrastructure)
3. Acts Targeting Physical Telecommunications Infrastructure
4. Acts Targeting Telecommunications Control and Command (NMS, TMN).

5. Capacity Management Failure

2.2.3 Full List of Potential Scenarios and Critical Events

The full list of scenarios that were analyzed and which will be continually assessed for inclusion within the action plan if situations change, is the following:

- 1 Infrastructure Component Failure
- 2 Neighbouring Countries Breaking Telecommunications Links
- 3 Technology and Skills Shortage
- 4 Chemical/Nuclear Incident (inside or outside Greece) – non fission explosion
- 5 Nuclear Incident (inside or outside Greece) – fission explosion
- 6 Sewage/Water Incident
- 7 Earthquake
- 8 Inland Flooding
- 9 Coastal Flooding and Tsunami
- 10 Storms, Heavy Weather and Hurricanes
- 11 Solar activity
- 12 Greek satellite Hellas Sat failure and other Space Liabilities
- 13 Disease and Epidemics (or pandemics)
- 14 Forest Fire and Scrub Fires
- 15 General Infrastructure Fires (e.g. fire in a major Telecom Carrier infrastructure)
- 16 Acts Targeting Physical Telecommunications Infrastructure
- 17 Acts Targeting Telecommunications Control and Command (NMS, TMN)
- 18 Acts Targeting General Facilities
- 19 Acts Targeting Population Centres
- 20 Acts Targeting Industrial and Commercial Centres
- 21 Electricity, Water and Utilities Interruption (part of supply chain)
- 22 Tactical Telecommunications Staff and Resource Shortages
- 23 Virus Attacks on Internet Services
- 24 Virus and Malicious Attacks on the Carriers
- 25 Military Infiltration
- 26 Espionage (military, political, or industrial)
- 27 Mobile and Radio Spectrum Interference and/or Jamming
- 28 Name Days and General High-Volume Dates
- 29 Capacity Management Failure
- 30 Loss of Carrier Interoperability

- 31 Poor Carrier-Carrier Cooperation/Coordination
- 32 Sudden Income Changes (for Telecommunications Sector)
- 33 Sudden Income Changes (major Telecommunication Carriers' clients)
- 34 Sudden Income Changes (for a Telecommunications company)
- 35 Competitive Industrial Espionage/Attacks
- 36 Long-term Investment Degradation
- 37 Medical Research Determining the Risk of Mobile Telephony to Health
- 38 Population Demographics (major demographic changes)
- 39 Holiday Seasonal Demographic Changes
- 40 Sports Events (Football matches, European Sports Events etc.).

2.3 CRITICAL SECTORS AND ORGANIZATIONS

This part outlines the Critical Sectors and Organizations Sectors for which Critical Telecom Services need to be provided, as part of a National Telecommunications Contingency process.

Critical Sectors and Organizations are those which impact the wellbeing, health and security of the general public. Should there be a telecommunications service interruption these Sectors and Organizations will be given priority over everything else.

2.3.1 Management Summary

The Critical Industries and Organisations of a nation require the telecommunication services to be available in order for them to 'survive' and continue supporting the public and the socioeconomic backbone of the country. Out of the 18 analyzed critical sectors and organizations, using a scoring approach that has taken into account the probability and the impact to the way of life, stability and human welfare in Greece, the following were selected:

1. Health: Primary-, secondary- and tertiary-care medical service, ambulatory services hospitals, etc., including special units such as burns, disease, etc.
2. Emergency Police, Fire, Ambulance and Rescue Services: National and regional related organizations.
3. Shipping and Harbour Control: The monitoring of shipping flow, the access into harbours, and the security and details associated with custom controls.
4. Civil Defence: The security, military, Government organizations requiring coordination of national, municipal, or regional recovery and control.

2.3.2 Full List of Potential Critical Sectors and Organizations

The full list of Critical Sectors and Organizations that were analyzed and which should be continually assessed for inclusion within the action plan is the following:

- 1 Food and Drink

- 2 Health
- 3 Drugs and Pharmaceutical
- 4 Utilities (Water, Electricity, and Gas)
- 5 Managed Transport
- 6 Internet Communications
- 7 Finance and Banking
- 8 Road Transport Management
- 9 Tourist Industry
- 10 Media
- 11 Country's Security (Police Operations and Criminal Security bodies)
- 12 Shipping and Harbour Control
- 13 Air-traffic Control
- 14 Civil Protection, Emergency Police, Fire and Rescue Services
- 15 Civil Defence
- 16 Social Security – Central Government
- 17 Dangerous Industries and Hazardous Substances
- 18 University Domains.

2.4 CRITICAL TELECOMMUNICATIONS SERVICES

2.4.1 Description

The list of telecommunications services listed in this section is the short list derived from the full list of services and deemed to be critical to sustaining the stated “Three Beliefs”, as well as supporting the Critical Sectors and Organizations during a Crisis event.

Triggers have been created which monitor the performance of these services as described in Section 3: “Triggers” and which once breached will initiate an Action Plan.

2.4.2 Management Summary

The critical telecommunications services selected for this Action Plan, based on a scoring approach that has taken into account the probability and the impact to the way of life, stability and human welfare in Greece, are the following:

1. Fixed Line Dialed (National and Local)
2. International Direct Dialling
3. Mobile Telephony (including SMS)
4. Satellite Telephony and Data (including Maritime emergency)
5. Internet Services Provision

6. Wireless Leased Lines
7. MAN/WAN Link Services
8. Data Services
9. Carrier Network Interconnects
10. Fixed Leases Lines
11. Disaster Recovery and Data Centre Sites
12. Emergency and Priority Services (E112, 100, 199, 166, etc.)

2.4.3 Full List of Critical Telecommunications Services

The full list of Critical Telecommunications Services that were analyzed and which should be continually assessed for inclusion within the action plan is the following:

- 1 Fixed Line Dialling (National and Local)
- 2 International Direct Dialling
- 3 Fixed Leased Lines
- 4 ADSL (Broadband)
- 5 ISDN (PRA BRA)
- 6 Mobile Telephony (including SMS)
- 7 MMS
- 8 Internet Services Provision (via dial-up, ISDN, ADSL, WiFi)
- 9 Data Services
- 10 Public Payphones
- 11 Customer Support Service
- 12 Carrier Retail Shop Outlets
- 13 Paging/Tetra Services
- 14 Carrier Network Interconnects
- 15 Wireless Leased Lines, LMDS
- 16 Satellite Telephony and Data (including Maritime emergency)
- 17 Disaster Recovery and Data Centre Sites
- 18 “Dark Fibre” (esp. as more critical data is communicated via this method)
- 19 PBX, etc. Maintenance and Support
- 20 MAN/WAN Link Services
- 21 Managed Capacity/Network Services
- 22 0800, 0845 and Premium Service
- 23 Directory Enquiries
- 24 Call Centre Services

- 25 Security Services (Home Monitoring, Burglar Lines)
- 26 Billing Service
- 27 Voice Mail
- 28 Message/Call Waiting
- 29 Emergency and Priority Services (E112, 100, 199, 166, etc)
- 30 3/4 digits Special Services (non emergency, information requests, etc.)
- 31 Services for Handicapped People
- 32 Number Portability, Carrier Pre-selection Service.

2.5 CRITICAL TELECOMMUNICATIONS INFRASTRUCTURE

2.5.1 General Purpose and Scope

This part describes the primary active and passive components, systems and sub-systems within the national telecommunications infrastructure (Main Systems). These main systems interconnect and interoperate in order to provide end-user/consumer, and telecommunications services including the defined Critical Telecommunications Services. Any major impact to this infrastructure will subsequently have an effect to the Critical Telecommunications Services. The requirement to identify the infrastructure systems and superimpose them on the Event Scenarios for failure will assist in raising awareness of the criticality of the infrastructure and of the need to strengthen and harden this environment. Additionally triggers have been developed which will initiate action once an infrastructure event breaches them.

2.5.2 Full List of Potential Critical Infrastructure

The full list of Critical Infrastructure that were analyzed and which should be continually assessed for inclusion within the action plan is the following:

- 1 Service Provider technical building facilities.
- 2 Network backbone nodes, digital switching systems.
- 3 Fixed Telephony Switching Systems.
- 4 Terrestrial Fibre Cable Systems.
- 5 Terrestrial Coaxial/Copper Cable Systems.
- 6 Submarine Cable Systems.
- 7 Submarine Cable Termination Stations.
- 8 Microwave Links, Towers and Masts.
- 9 Local Distribution that covers a large number of subscribers.
- 10 Mobile Switching Systems.
- 11 Mobile Telephony Transmission- Major Base Station Nodes.
- 12 Network Management Centres.

- 13 Data Centres.
- 14 Specialized Wireless Networks.
- 15 Space Satellite.
- 16 Satellite Earth Stations.

SECTION 3: TRIGGERS

3.1 GENERAL

This Section outlines the likely performance metrics and triggers that have been considered as part of a National Telecommunications Contingency (NTC).

These metrics have been produced by a combination of reviewing conditions used in other countries adapted in this report to reflect variances in culture, demographics and general social activities, the Consultant's experience and industry understanding, as well as knowledge of the Greek environment.

These triggers once breached will invoke the Action Plan and will activate the Crisis Management Team.

There are two general scope descriptions:

- Triggers within the telecommunications environment that can be measured and for which a breach of the conditions will be deemed sufficiently disruptive to the Greek society that immediate remedial action will be required.
- The analysis and definition of various measurements that will enable EETT to assess and provide guidance to the Carriers as to when and how a NTC crisis management function can be invoked in order to serve the interests of the Greek telecommunications user and consumer most effectively.

3.2 TRIGGERS

3.2.1 Factors Invoking the NTC Action Plan

The types of performance measures that gauge whether an invocation of the National Telecommunications Contingency Plan is required and which have been used to derive the Triggers are presented in "Table 2: Factors Invoking the NTC Action Plan". Using these measures, NTC invocation trigger points and measurement mechanisms have been determined which are specific for each short listed telecommunications industry External Crisis Event, impact to telecommunications infrastructure, impact to Critical Telecommunications Services, and impact to Critical Sector/Organization.

Table 2: Factors Invoking the NTC Action Plan

Factor	Description
Extend of telecom External Crisis	The level of the potential crisis, hazard, condition and it potential impact to the general population, telecommunications infrastructure, and level of uses of telecommunications services.
Quality	The quality of service being provided to the users and Critical Sectors and organizations. Quality can include items such as service degradation, congestion, multiple short-burst outages making service difficult (especially data), error rate, echo, etc.

Factor	Description
Historical / pre-empted	Trend analysis using service management information, including items such as capacity management (monitoring long-term trends nationally) and wider problem management tools (root cause analysis and investigating whether there is an opportunity to pre-empt a crisis).
User	The perceived and actual service disruption described by the users, even though the service may be performing within prescribed service levels.
Critical Sectors	The ability of the Critical Sectors to conduct their operation, based on the balance of 'resilience' agreed with the Carrier. The Critical Sector Industry members should aim to have a Disaster Recovery Plan and resilient infrastructure of their own.
Critical Infrastructure	The metrics provided by network monitoring devices that, when correctly configured and operated, will be able to assess in real-time any service degradation or interruption, and should also predict likely crises in advance, either by using modelling or by using early warning triggers

3.2.2 Trigger Analysis

There are four general categories of triggers:

- 1 Triggers associated with Crisis and Emergency events external to the telecommunications environment (i.e. Earthquake) which could cause excessive use of telecommunications service. It is noted that an event could cause the activation of a secondary related trigger.
- 2 Triggers within the telecommunications infrastructure which subsequently impact the defined Critical Telecommunications Services and thus the end-user/consumer (e.g. switching centre fires, fibre cuts, trunk group outages, backbone faults, base station outages etc.).
- 3 Triggers which are associated with specific defined Critical Telecommunications Services as perceived by the end-user/consumer (e.g. congestion of fixed/mobile telephony, no access to international dialling etc.).
- 4 Triggers related to the quality of service that is provided to critical Sectors and Organisations and which will impact the ability of the end-user/consumer to communicate with vital organizations such as ambulance, fire brigade, police etc.

Besides the invocation triggers that would result in activation of the specification actions there is a number of triggers that are designed to inform EETT that an event could evolve and there is a need for preparedness

Each Trigger is associated with a method of monitoring for breach and related actions /initiatives and to resolve mitigate the event as presented in "Table 6: Triggers and Action Plans".

3.2.3 Invocation Triggers

There are 26 Triggers which are categorized and relate to:

- External Crisis and Emergency Event Scenarios.
- Telecommunications Infrastructure Emergency Events.
- Outages and Impact to Critical Telecommunications Services.
- Impact to Critical Sectors and Organizations.

The full list of these Triggers is presented in “Table 3: List of the Triggers” and the associated actions are presented in “Table 6: Triggers and Action Plans”. These triggers are for unscheduled, unplanned, and un-mitigated service interruptions.

Table 3: List of the Triggers

Triggers	
1 a	The loss of infrastructure service capability equivalent to 300,000 user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute.
b	Over 10,000 originating and terminating calls are blocked for inter-carrier communications in any 30 minute interval
c	On two or more consecutive days, there are two or more instances where 10,000 user connections are interrupted for less than 30 minutes
2	A fission (nuclear) explosion, reported by the Government or media within the borders of Greece or within 1000 km of Greece
3	An earthquake of 6 on the Richter scale, reported by the Government or media within the borders of Greece or within 100 km of Greek territory, or above 5 Richter in any urban areas.
4	Flooding affecting any town over 5,000 people, reported by the Government or media
5	A forest or scrubland fire reported as threatening population centers, reported by the Government or media. Will cause a secondary trigger if it impacts telecommunications infrastructure.
6	Any fire in any switching station, cable termination centre, transmission centre, or other Carrier establishment where hardware needed to support telecommunication services is damaged. Will cause a secondary trigger if it impacts telecommunications services.
7	An actual terrorist act or perceived terrorist threat against telecommunications infrastructure, reported by the Government or media.
8	An actual terrorist act resulting in the loss of life or the closure of multiple businesses reported by the Government or media
9	Any unauthorized internal or external malicious attack on the Carriers affecting the ability to deliver service or to secure personal data records of consumers and businesses
10	Capacity on any element of the telecommunications infrastructure where traffic exceeds 90% of total possible traffic, in any single exchange, switching centre, transmission and connection centre, communications paths (e.g. cabling)
11	Any Carrier share-price drop of 30% in a week, or any operational financial loss, or any financial irregularities identified by auditors or other agents

Triggers	
12	Annual investment report and update via the Service Management report. Where EETT believes the investment profile may not be commensurate with the Three Primary Beliefs
13	Any medical-related announcement regarding mobile Carrier activity that is followed, within a week, by a 25% drop in call traffic volumes to and from mobile telephone users
14	Annual traffic report showing peak flows and problems
15	Any registered hospital telecommunications outage for more than 60 minutes
16	Any registered Fire, Ambulance and Rescue fixed or mobile telecommunications outage for more than 30 minutes
17	Any registered shipping and harbor control telecommunications outage for more than 60 minutes
18	<p>a Failure of international service resulting in 5,000+ failed international calls within a 30-minute interval (could be caused by routing difficulties, transmission, etc.)</p> <p>b Over 15,000 originating and terminating international calls are blocked for Inter-carrier communications in any 30 minute interval</p> <p>c The loss of infrastructure service capability equivalent to 150,000 international user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute</p>
19	<p>a The loss of 5,000 potential mobile telecom users brought about by a single incident, root-cause, or within a 30-minutes interval. To estimate the potential users the affected system capacity should be multiplied by a contention factor of 10. Thus an MSC which is capable of handling 500 simultaneous calls would potentially impact $500 \times 10 = 5,000$ users.</p> <p>b The loss of mobile infrastructure service capability equivalent to 150,000 user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute. The number of users is calculated as in the previous trigger point.</p> <p>c The concurrent total or partial loss of service for 4+ 'cells' (based around a mast) for a total of 30 minutes (i.e. 4 cells inactive due to the same root-cause during a 30 minute interval) brought about by a single incident or root-cause</p> <p>d Over 15,000 originating and terminating calls of mobile telephony are blocked for inter-carrier communications in any 30 minute interval</p>
20	Loss of Internet telecommunications connectivity to an ISP impacting more than 10,000 users for more than 30 minutes
21	The loss of or disruption to any service group affecting more than 30% of the subscribers using those services within any single switching exchange / transmission center.
22	A 90% utilization for any Carrier-Carrier interconnects lasting for a continuous period of 30 minutes or more.
23	Loss of a Carrier Data/Network Management Centre, or a Critical Sector Data Centre managed by the Carrier.

Triggers	
24	<p>a 100 failed attempts to access Emergency or Priority numbers (100, 166, 199, 112, etc.) in a duration, which needs to be agreed with the Emergency Service operator.</p> <p>b No ability to originate, terminate, or complete calls related to Emergency or Priority numbers for more than 30 minutes.</p>
25	Service interruption or serious downgrading of service for more than 30 minutes offered by Hellas-Sat
26	<p>a Deadly disease epidemic or pandemic that causes death in 50% of cases, or is likely to cause more than 50,000 deaths in Greece, that is either already within Greece or that will soon reach Greece</p> <p>b At least 200 user complaints to the offices of EETT within one working day, relating to any single telecommunications service or with reference to any single root cause</p> <p>c Carrier unable to collect and process a relevant trigger metric for a period of over 1 hour</p>

External Crisis Events would most likely result in network congestion due to the need of the end-user/consumer to communicate with loved-ones as well as Critical sectors and organizations but also could cause related secondary triggers to occur if the Telecommunications Infrastructure is impacted due to the External Crisis Event (i.e. earthquake would most likely cause extensive use of fixed and mobile telephony but could also impact the telecommunications infrastructure.). This relationship is presented in “Table 5: Event, Service, Sector and Trigger Association”.

The requirement is that when these triggers are set off, the Carriers are obliged and mandated to take the required action as described in the “1st Level Immediate”. Column of “Table 6: Triggers and Action Plans” and work with the CMT for actions associated with “2nd Level after CMT activation”.

It should be taken into account that the triggers generally, would be modified by the CMT over time depending upon the quantity and quality of data received, in order to achieve a real reduction in service interruption risk and a real improvement in quality of service.

As stated earlier the initial trigger points have been based on a combination of reviewing reporting trigger points and mechanisms used in other countries adapted in this report to reflect variances in local demographics, the industry-expert’s experience and understanding, as well as knowledge of the Greek reality. They are a starting point and will be further optimized out of any lessons learned.

3.2.4 Planned Maintenance Outages

During planned and scheduled maintenance, which could result to outages, it is recommended that a number of actions should be adhered to by the Carriers, in order to prevent the invocation of some of the chosen triggers that are presented above.

3.2.5 Trigger Reporting

The reporting of triggers that have been broken or that are modelled to be likely broken is a key facet of the whole quality improvement of the NTC Action Plan and the National Telecommunications Contingency Programme.

The Carriers should be capable of near-immediate reporting of ‘trigger’ activity. Mechanisms should be available where information required to obtain the trigger is monitored, collected and processed.

Bi-annually Released Service Management Report

The Carriers will submit a bi-annual report on the actual and modelled trigger infringements and the risk of infringed triggers. The eventual objective is the understanding of the risk, opportunities, and actual activity within the telecommunications networks on an ongoing basis. Detail structure of the report is presented in 6.1 “Carrier Bi-annual Service Management Reports”.

SECTION 4: ACTION PLAN INVOCATION

4.1 PURPOSE AND SCOPE

This Section outlines the invocation process needed to fulfil the requirements of the National Telecommunications Contingency and initiate action once a defined Trigger point is breached.

The scope of the Section is to detail:

- The different methods for invoking the action plan.
- The Crisis Management Team (CMT) and Carrier obligations for invoking.
- The testing requirements for invoking the action plan.
- The different types of invoking and communications between Carriers and EETT.

The invocation of the National Telecommunication Contingency Plan will be activated through one or more of the following:

- Pre-emption due to trend analysis (Service Management Report).
- Carriers breaching trigger-points.
- “Obvious crisis”.
- Monitoring and technical alerts.
- Media reports.
- Government requirements.
- EETT review of quality of service.

4.2 INVOCATION DEFINITION

4.2.1 What is the Invocation?

Invocation being described within this Section is the need for the Crisis Management facilities and the Crisis Management Team to become operational under EETT leadership, in order to expedite the recovery of telecommunications services to users due to a major incident.

4.2.2 Purpose of Invocation

The purpose of the invocation is to:

- Fulfil obligations as set out by the National Telecommunications Contingency Plan, determining and mandating that Telecommunications Carriers in cooperation with each other and EETT resolve major incidents as quick as possible.
- Initiate an organized, structured and cooperative approach in resolving telecommunications related crisis conditions.

- Ensure that the survivability of telecommunications services related to Critical Sectors such as police, fire and health services are given priority across all Carriers during a crisis event.
- Improve the quality processes within the Telecommunications Sector with lessons learned.
- Enable EETT to understand the holistic picture of any major incident, and to increase understanding as to how this is resolved, thus improving future incident resolution.
- Enable EETT to facilitate the Carriers' communication with other governmental crisis management organizations, when this is required.

4.2.3 Carriers Definition of Invocation

The Carriers most likely have their own escalation and crisis management invocation procedures – possibly with their own triggers, governance and disaster recovery processes.

For the purpose of the National Telecommunications Contingency action plan, the invocation in discussion here is for the management of a NTC Crisis Management Team (CMT) under the control of EETT and with participation by the Carriers. Any Carrier internal invocation and disaster recovery procedures will be managed and administered by the Carriers as they currently exist in harmony with the National Telecommunications Contingency Plan.

4.2.4 General Comments

Invocation of the action plan and the CMT depend on the threshold of the trigger points. With the aid of the Service Management report the triggers will be periodically adjusted so the action plan invocation occurs approximately once per 6 months.

The reason for every 6 months is that an invocation of the plan and the CMT has advantages and disadvantages:

The advantages are:

- A frequently invoked process is often easier to manage and more effective in dealing with incidents and crises, as the participants are experienced and of similar minds.
- A frequently invoked process will provide many 'lessons learned' actions and ideas to learn from – both at a technical level and also a human one.
- A frequently invoked process builds greater opportunities for Carrier cooperation and provides EETT with a platform for successful coordination.

There will be a tendency to elongate the time between invocations due to the cost of supporting a crisis management infrastructure, hence there will be a desire to improve quality to reduce the likelihood of an invocation. So in order to ensure 'frequent' invocations, the following actions are required:

- Lower the trigger thresholds in particular areas that are obvious weaknesses and which will begin to surface with the Service Management Report.

- Start to undertake more and more trend analysis of Carrier Incident Reports and Problem management reports (as an output of the biannual Service Management Report presented in 6.1 “Carrier Bi-annual Service Management Reports”), and therefore pre-empt any crisis at an earlier and earlier juncture.

4.3 DECISION-MAKERS AND ROLES

The following are general roles that will be mostly undertaken by EETT and will be established as part of the Crisis Management Team and processes:

Role	Description
NTC Leadership team	Three senior EETT staff with a specific responsibility for managing and coordinating the NTC Crisis Management Team. These people are the key decision-makers.
NTC Information Desk	Organisation/operation that provides a single number and 24x7 service capability, for recording crisis reports and contacting the required call-tree representatives in the event of a Crisis (which will initially include the NTC Leadership team).
NTC Administrator	Updates the call-trees and contact details, ensures that the Internet/extranet apparatus and data are active and up to date. This role could become the CMT scribe. Could come from EETT or a Carrier.
Carrier NTC Officer	Will report progress and communicate with the NTC Leadership team. Integral part of the CMT.

4.4 INVOCATION DECISION MAKING METHOD

4.4.1 Who Decides?

EETT having as its major duty the protection of the consumer in relation to telecommunications services will have the final decision to invoke the CMT or not.

Within EETT a leadership team of 3 senior officers will be appointed (as part of their operational duties) who have the remit of deciding the merits of a Crisis Management Team invocation. The name of this group will be:

NTC Leadership Team

These 3 staff will be contactable on a 24x7 basis in case of emergencies.

4.4.2 Communications

4.4.2.1 Who will alert the NTC leadership team?

The NTC Leadership Team will be alerted via the NTC Information Desk by the relevant Carrier, EETT, Government or the interested user (user from a Critical Sector or Organization) depending on the trigger breached.

The exact method of alerting the Leadership Team will depend upon:

- Time of date.
- Type of crisis and incident.
- Organization communicating the problem.

The alerting process for each member will follow the call tree information available at the NTC Information Desk. The Information Desk staff will use pre-established methods for contacting each member (i.e. mobile first, office number second, home number third).

4.4.2.2 What communications technology should be used?

In the Tools section of this Section there are a number of communications tools described which should help establish the best means of CMT communications. The team should decide ahead of time the best choice of establishing and maintaining communications in the event a crisis and make this available to the NTC Information desk.

4.4.2.3 How will they be alerted?

At least two means of communication should be used so as to make sure that all members have been contacted in case there is an impact of one of the choices due to the event. It is recommended that mobile telephony is used as the first choice and fixed telephony as an alternative. In the event of an invocation where mobiles or telephones are no longer available (as a result of the incident) a number of TETRA units should be made available at the Crisis management centre for distribution to the Crisis Management Team.

4.4.2.4 Who will they contact?

The Leadership Team and the NTC Information Desk must have access to a ‘call-tree’ in order to invoke and mobilise the required individuals and resources. Additionally each CMT member should have wallet cards which should be carried by each member at all times containing all member contact information. See EETT Invocation Process below.

4.4.2.5 Decision Point – Invoke or Not?

The primary driver which the Triggers were based on and which should be used to determine invocation is the potential detrimental affect in the Three Primary Beliefs (Table 4). This is not an empirical exercise, as the time to gather, analyse, and interpret the findings will result in delays and confusion.

Table 4: The Three Beliefs

Way of Life	Will the impact change the values and beliefs of the population and commerce – including the belief that the regulator acts to protect the consumer, maintains quality, and reduces risk?
Stability	Will there be a threat to the stability or civil order, or will the current Government or administration become affected?

Human Welfare	Will there be an increase in the loss of life or in injury, beyond what is reasonable due to the current event? (i.e. earthquake causing loss of life but loss of telecommunications could increase casualties due to non available Emergency Services e.g. police, fire brigade, EKAB, etc.).
---------------	--

The following broader questions will be asked and then answered by Leadership Team;

- What is the trigger point that has been breached?
- Are there any special circumstances that will readily resolve the incident?
- How many users affected, what's the impact, and for how long?
- How many Critical Sectors and Organizations affected, what's the impact, and for how long?
- What values will an invocation add, and how can invocation assist in the resolution?

4.5 INVOCATION PROCESS – CALL TREES

4.5.1 What is a call tree?

A call tree is a database of contact details, including who will contact whom. The fields within a call tree include:

- Contact name.
- Job title/role.
- Contact mobile/pager/phone number.
- Times that the contact is on-call.
- Date when details last updated.

4.5.2 What information do the callers provide?

The NTC Information Desk will require the following information:

- Caller's name and contact details.
- Organisation.
- Who is operating the Carrier CMT.
- Incident and trigger breached.
- Impact currently assessed on users.
- Suggested remedial action.
- Required supporting roles (from other Carriers and suppliers, etc.).

ACTION – The NTC Information Desk role will be assigned and the owner will be
PROPOSAL designated (EETT's responsibility).
1:

4.5.3 Where is the call tree held?

Call-tree information will be held in two basic media:

- Primarily on the WEB site, that is accessible as a secure extranet by the NTC Information Desk and NTC Leadership.
- Hard-copy held by the NTC Information Desk, NTC Leadership, and Carriers.

ACTION - An NTC administrator will be appointed to collect contact details for all
PROPOSAL NTC members (EETT and/or Carriers)
2:

4.5.4 What does the leadership team do?

The leadership team forms the CMT comprising of people with the roles outlined within the Crisis Management section 5.4.2 “CMT member role descriptions.” Agreement will be reached as to when to meet at the Crisis Management centre.

4.5.5 Who will update the contact details and ‘call-tree’, and who will distribute?

The NTC Information Desk will be responsible for updating at least once every six months. Additionally the Information desk will publish wallet cards with the contact information of each member and distribute it to all members.

4.6 CARRIERS’ ACTION - PROPOSALS TIMETABLE

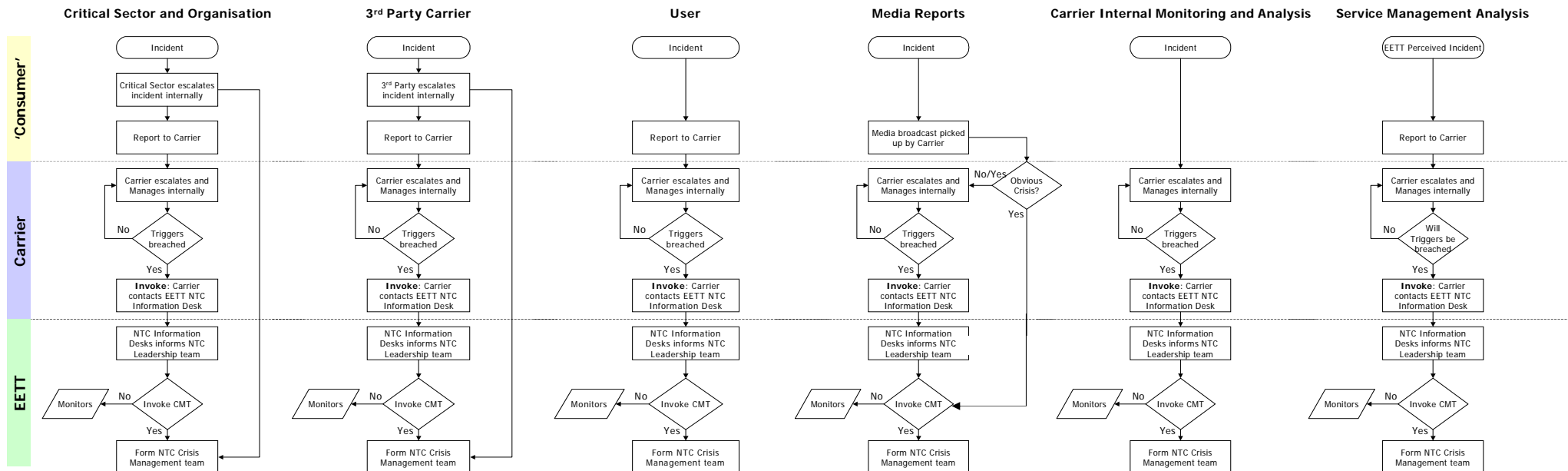
4.6.1 Carriers’ Actions/Activities Timetable for the Resolution of Emergencies

The following timetable associated with response to the crisis is required by the Carriers, and will be reported upon as part of the publicly available Service Management Report (see Section 6.1.5 Communication and Feedback):

Action/Activity	Timetable
Identifying the crisis affect upon any trigger (i.e. being able to determine whether a trigger has been breached).	Within 30 minutes of critical event.
<i>Once the affect of the critical event has been registered and modelled by the Carrier (i.e. within 30 minutes of a critical event), this will be known at the point at which the trigger has been breached. For the following steps activated, these have all been measured against the point at which the Carrier realises the trigger has been breached, or within 30 minutes – whatever is less)</i>	
Reporting the trigger breach by contacting EETT NTC Information Desk on +30 210 xxx xx xx	Within 15 minutes of breaching the trigger.

Action/Activity	Timetable
<p>Understanding and communicating the impact to the Leadership Team of EETT, by quantifying and qualifying all the following:</p> <ul style="list-style-type: none"> • The population area affected • The number of users affected • The type of the affect (services and infrastructure affected, etc.) • The affects on the Critical Landscape • The likely and expected duration of the outage • Whether the impact will increase, and if so, how 	<p>Within 60 minutes of breaching the trigger.</p>
<p>Diagnosing and communicating the crisis (i.e. the cause) to EETT by qualifying all the following:</p> <ul style="list-style-type: none"> • The current knowledge and understanding of the exact nature of the crisis • The root-cause of the incident 	<p>Within 60 minutes of breaching the trigger.</p>
<p>Understanding and communicating the recovery options to EETT, based around the immediate options (including viability of option, cost, recovery suitability) by qualifying all the following:</p> <ul style="list-style-type: none"> • Utilising the infrastructure of other Carriers • Utilising spare systems • Call control, routing and prioritisation • Alternative service provisioning 	<p>Within 120 minutes of breaching the trigger.</p>
<p>List the critical sectors and organisations affected, and their telephone services/details, and communicating to EETT:</p> <ul style="list-style-type: none"> • Organization • Contact details • Services/infrastructure offered • Priority services used 	<p>Within 120 minutes of breaching trigger.</p>

4.7 INVOCATION ROUTES AND METHODS



ACTION - PROPOSAL 3:

Form the NTC Information Desk, a 24x7 service desk, which will have a list of contact details of whom to contact, and the message to give them.

EETT will ensure that the Carriers and Government have the NTC Helpline contact details (NTC Information Desk).

The NTC Information Desk will have a list of questions to ask the caller – possibly a code.

The NTC Information Desk will collate Carrier Crisis Management team details from the Service Management Report, and use this as part of the call-tree

Once the trigger has been breached and the Carrier is required to contact the NTC Information Desk, attention should be given to the points that follow.

4.7.1 Phone number

A single phone number will be available on a 24x7 basis, with the phone number being widely known and publicised – this number covers both the users (Critical Sectors and Organisations) and the Carrier organisations. As an alternative a mobile telephone will also be available and publicised. These numbers will be part of the Carriers' priority list.

ACTION - EETT will have a suitable Crisis Management telephone number and call
PROPOSAL tree. In normal times the number will be forwarded to the EETT officer
4: responsible for Crisis Management

4.7.2 Statement

The Carrier must pass across the following details:

- Caller's name and contact details
- Organisation
- Who is operating the Carrier CMT.
- Incident and trigger breached
- Impact currently assessed on users
- Suggested remedial action
- Required supporting roles (from other Carriers and suppliers, etc.).

4.7.3 Confidentiality

A key facet of crises is the need to retain and sustain security and confidentiality.

In the event of a crisis where Carriers need to cooperate, the importance of 'confidentiality' between Carriers, as well as EETT is crucial to the success.

Decisions as to what information related to the crisis should be made available to the general public will rest with the CMT. Sensitivity to general public reaction is key.

4.7.4 Security

Secure access to the Crisis Management Team is a major concern and problem.

Agreement of the officers of the Carriers to gain access to the CMT and premises of EETT needs to be addressed upfront. Part of the biannual Service Management Report will be to detail the officers who will be involved in the National Telecommunications Contingency

ACTION - Carriers to define their CMT representatives and contact details in the
PROPOSAL biannual Service Management Report
5:

4.7.5 Automated Information

EETT through the Service Management Report and the invocation process and will have access to the general state of the Carrier services. In a longer term EETT in cooperation with the Carriers could investigate automated monitoring of some or all aspects of the National Telecommunications Crisis management process where feasible.

4.8 COMMUNICATIONS BETWEEN CARRIERS AND EETT

In Section “Section 7: Tools” there is a number of communications tools described, which should help establish the best means of communications between EETT and the Carriers. The team should decide ahead of time the best choice of establishing and maintaining communications. As a first choice mobile telephones should be utilized with fixed telephones as the back-up. These numbers should be part of the Carriers’ call priority scheme. Alternatively TETRA units can be made available at the Crisis Management Centre and can be picked up by the CMT members if fixed and mobile communications have been impacted.

SECTION 5: CRISIS MANAGEMENT AND ACTION PLAN

5.1 PURPOSE AND SCOPE

The scope of this Section is to provide the following details

- The actions which need to be taken to address the particular event and trigger breached.
- What the Carriers and the CMT are required to do, and by when.
- Roles and responsibilities.

5.1.1 Interests of the main actors

There are many stakeholders associated with the immediate and accurate resolution of Crisis and Emergency events and impacts associated with national telecommunications services. The development of the NTC action plan has considered the interest of the end-user/consumer from the point of view of all stakeholders.

5.1.1.1 *Government*

In the NTC the Government's interest is to serve the users, Critical Sectors and organizations, ensuring:

- Wealth and financial aspects are retained
- Population health and wellbeing are ensured
- Political and legal security is retained.

5.1.1.2 *EETT*

EETT supports the interests of the telecommunications users by ensuring:

- That the regulatory requirements are adhered to.
- That it identifies areas where aspects of the licence allocation contracts have not been adhered to.
- That it facilitates a quicker disaster recovery by enabling the Carriers to cooperate better.
- That the Carrier crisis management plans are current and relevant.

5.1.1.3 *Emergency Services- Critical Organizations*

The Emergency Services and Critical Organizations need to ensure that:

- The health, security and well being of the public are addressed.
- The economic viability of the country is retained.
- Lessons are learned about organizational responsibilities regarding contingency planning.

5.1.1.4 Carriers

In the NTC action plan the Carriers' interest is to serve their customers, Critical Sectors and organizations, ensuring:

- Legal exposure for each Carrier is minimised.
- They provide a robust and resilient service.
- Commercially they are seen as acting in the best interests of Greece and are therefore more likely to retain customers and revenues.
- Economically they are kept in business by reducing impact between dependent Carriers.

5.2 CRISIS MANAGEMENT DEFINITION

Crisis Management is the immediate response to a crisis utilizing an Action Plan, insofar as the correct team coordination and activities are completed in order to assess, repair/recover, and resolve major incidents.

The Carriers will identify the problem and issue and initiate remedial action in order to resolve the problem.

The members of a Crisis Management Team will be capable of discovering information as to the current state of affairs, and for motivating and managing the remedial action in order to close the incident in the quickest possible time.

The decision-making information-gathering process is similar for virtually all processes, and covers: What is the problem? What is the impact? How can we resolve it in the quickest possible way?

Crisis Management also includes the communications between the stakeholders, including legal entities, Carriers, and individual as well as business users.

5.2.1 Levels of Crisis Management/Action Plan

The NTC Action Plan has two levels pertaining to the resolution of the Crisis Event and any impact to the Telecommunications Infrastructure, Critical telecom Services and Critical Sectors/Organizations.

The "1st Level Immediate" addresses actions which the Carriers should perform immediately following the breach of a Trigger point as defined in 5.3 "1st Level Carrier Actions" and Table 6: Triggers and Action Plans. In addition the Carriers need to Invoke the NTC or Inform EETT as appropriate following the procedures defined in "Section 4:Action Plan Invocation".

The "2nd Level after CMT" addresses actions which the CMT should perform once the NTC is invoked and the CMT is activated as described in Section 5.4 "2nd Level Actions After CMT Activation" and Table 6: Triggers and Action Plans.

5.3 1ST LEVEL CARRIER ACTIONS

5.3.1 Immediate Carrier Response

The Carriers, upon a crisis condition and major incident which results in a breach of a Trigger, will:

- Engage the Carrier's internal crisis management staff and function.
- Initiate the Carrier's internal disaster recovery plans.
- Prepare, mobilise and be ready to engage the NTC process, by contacting the designated NTC Officer within the Carrier organisation.
- Initiate immediately Call Priority and Call Control mechanisms to provide priority to critical sectors communications requirement in the affected areas/regions as described in Section 5.3.4 "Call Priority Initiation" and 5.3.5 "Call Duration Control Initiation".
- For Mobile Carriers, initiate SMS broadcast alerting to instruct users in the impacted area/region as to the optimal use of the surviving telecommunication recourses.
- Be ready to alter Call Priority and Call Control parameters when and if instructed to do so by the NTC CMT, when a better understanding of the impact and extent of a crisis is established.
- Initiate CMT communications tools.
- Invoke the NTC Plan and engage the Carrier's representative with the other members of the CMT team.
- Where defined in "Table 6: Triggers and Action Plans" provide the necessary information to EETT.

The expectation is for the Carrier to have an internal crisis management team and function, and a series of internal recovery plans. The NTC crisis management process can over-ride the Carrier plans if necessary.

However, the Carrier has an obligation to recover the situation as planned by its own internal processes and disaster recovery plans **until informed otherwise by the NTC crisis management team**.

In parallel to NTC CMT activation and within the time limits defined in 4.6 "Carriers' ACTION - PROPOSALS Timetable" the following typical activities should be established:

- Understand the impact.
- Diagnose the problem.
- Understand the recovery options.
- List the critical sectors and organisations affected, and their telephone services/details.

5.3.2 Carrier internal staff during NTC

The Carrier responsibilities for their own crisis management staff in relation to the NTC will be:

- To provide the required recovery data to the NTC CMT via the Carrier's NTC Officer or otherwise.
- To attempt to recover the crisis in the best way possible, or otherwise instructed by the NTC CMT.
- To be actively communicating with the Carrier's support infrastructure.

5.3.3 Crisis Relief Tool Initiation

Upon trigger breaching the most likely impact to the telecommunications services will be an influx in activity due to an external event such as an earthquake, or congestion due to the unavailability of critical telecommunications infrastructure elements. In either case the telecommunications services will be impacted thus creating congestion for critical sector telecommunications services. In order to preserve the availability of these services Call Priority and Call Control mechanisms need to be implemented.

5.3.4 Call Priority Initiation

The Carriers immediately upon trigger breaching will evaluate the impact and will implement Call Priority as described in Section 7.3.1.1.7 "Priority in emergency situations" and 7.3.1.1.8 "Priority treatment of other Critical Industries and Sectors".

It is recommended that two levels of priority are established which can be initiated upon investigation of the impact and in coordination with EETT by both fixed and mobile Carriers.

Level A: Incoming (General public-to-agency) Critical Sector telephone services to Police (100), Fire Brigade (199), Ambulatory service (166) and general emergency (112) will be given the highest priority over all other calls in both the fixed and mobile networks for the impacted area/region. In the event of impact of the terminating facilities due to the disaster event, the responsibility for providing alternative terminating facilities resides with the critical sector agency (Police, Fire, Ambulatory services). Priority must also be provided to the CMT's telecommunication services.

Level B: Level A plus all incoming and outgoing calls to pre-defined Governmental, Public Safety, Military and Health sectors. The list of telephone numbers will be established upon consultation by EETT with the related sectors and will be made available to all Carriers.

After the initial and most likely immediate activation of Call Priority upon activation of the CMT the decision for alteration of Call Priority parameters will be transferred to the CMT.

5.3.5 Call Duration Control Initiation

The Carriers immediately upon trigger breaching will evaluate the impact and will implement Call Duration Control as described in 7.3.1.1.9 "Call Duration Control".

It is recommended that upon investigation and establishment of call congestion due to a crisis event, Carriers should implement Call duration Control to allow more general public members to use the surviving telecommunications services. Call Duration Control should not be implemented for the predefined Critical Sector numbers. The Carriers should impose primarily Call Duration Control to incoming calls to the impacted area/region, resorting to outgoing call control in extreme conditions. If variable duration call control mechanisms are available, Carriers should implement a control duration which will eliminate congestion while maximizing the call duration. If variable duration mechanisms are not available a **two minute call duration allowance** is recommended for calls intended for the stricken area/region.

Call Duration Control should be implemented across all switching centres equally if possible, avoiding discriminating against easy targets.

After the initial and most likely immediate activation of Call Duration Control and upon activation of the CMT the decision for alteration of Call Duration Control parameters will be transferred to the CMT.

5.3.6 Other Call Controls

Many modern telephone switches have many other call control mechanisms which can be used to control the amount of traffic in, out, as well as to certain destinations. These mechanisms include:

- Call Rate Control (i.e. allow 4 calls every 30 seconds per exchange).
- Call Percentage Control (i.e. 30% of calls allowed to transit).
- Call Blocking (calls not allowed to a specific destination).
- Call Gapping (Sets the upper limit of calls to a specific destination).

These call control mechanisms should be made available and used during a crisis event in cooperation between EETT and the Carriers.

5.4 2ND LEVEL ACTIONS AFTER CMT ACTIVATION

Immediately following the breach of a Trigger the Carriers will engage in resolving the problem as defined in section 5.3 “Carrier Actions”. In parallel, activation of the NTC will have taken place and engagement of the NTC CMT where appropriate.

The CMT will arrange to meet at the Crisis Management Command Centre and immediately upon activation work on the actions defined in “Table 6: Triggers and Action Plans” and Section 5.4.1 “CMT Tasks”.

5.4.1 CMT Tasks

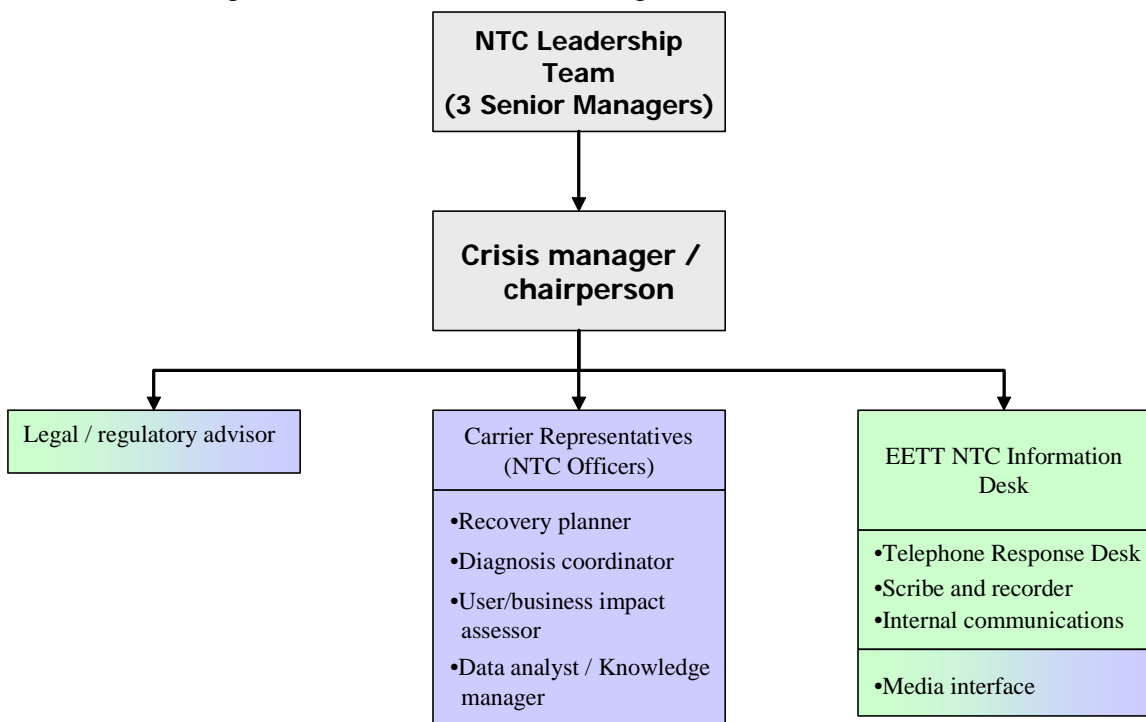
The key task and responsibilities of a Crisis Management Team are:

- Coordinate recovery.
- Be the single point of focus for recovery.
- Monitor response operations.
- Communicate, coordinate and pass information to all stakeholders.

- Consolidate damage assessments and provide status reports.
- Identify recovery and impact requirements.
- Prioritise requirements.
- Collate and analyse service metrics.
- Coordinate the allocation and use of resources.
- Ensure that the management and recovery activities are within the law.
- Provide a ready and trained response team to deal with any crisis.
- Coordinate activities between Carriers.
- Coordinate activities with relevant Government Agencies.
- Support coordinated interface with Media.
- Support coordinated announcement to the general public.
- Update WEB site.
- Issue Problem Management Report.
- Determine closure.

5.4.2 CMT member role descriptions

The Crisis Management structure is the following:



Once invocation occurs, the NTC leadership team described in the section 4.3 “Decision-Makers and roles” would have a role in Crisis Management. The key roles required for a Crisis Management Team are the following:

Role	Responsibilities	Who
Crisis manager / chairperson	Convenes CMT, in accordance with the NTC Leadership Team, schedules required meetings, but most importantly facilitates cooperation between Carriers to resolve issues to the benefit of the users and Critical Sectors and organisations. Liaises with Carrier senior management to ease any problems and completes actions.	EETT
Scribe and recorder	Ensures that the sequence of events is recorded; and decisions are logged.	EETT or Carriers
Data analyst and Knowledge manager	Obtains data from the media, Government, user service desk, other bodies, archives management information and metrics for analysis by Carriers and other specialists. Liaises with the Carrier CMT.	EETT or Carriers
Media interface	Updates website, compiles media broadcasts, contacts media, makes announcements, and communicates with the Carrier media group.	EETT or Carriers
Internal communications	Facilitates telephony or other communications methods with the Carriers and other stakeholders, including internal progress and status updates. Liaises with Carrier NTC officers.	EETT or Carriers
User/business impact assessor	Works with the various Carriers and other stakeholder organisations to determine the extent of any incident upon the general public or Critical Sectors and Organisations.	EETT or Carriers
Diagnosis coordinator	Works with the various Carriers and other stakeholder organisations to determine cause, and the 'damage' and issues being created by an incident. Liaises with Carrier NTC officers.	EETT or Carriers
Recovery planner	Works with the various Carriers and other stakeholder organisations to determine the recovery plans and options (including timescales etc.). Liaises with Carrier NTC officers.	EETT or Carriers
Legal and regulatory advisor	Advises the EETT Leadership Team, and also will provide advice and legal governance for certain decisions that may be required to bring the crisis to a speedier conclusion.	EETT
Telephone Response Desk	'Freephone' number for members of the public and Critical Businesses and the Carriers, works as a call centre taking faults, issues, information, etc.	EETT

ACTION – PROPOSAL 6: EETT and Carriers will appoint internal resources for each of the above roles, train and mentor to fulfil the responsibilities. A recommendation is for staff to be trained for multiple roles.

5.4.3 CMT Members

To fulfil the CMT roles mentioned above, the following sources of staff are required:

- At least one representative from within each Carrier organization to represent the Carrier during CMT activation (the Carrier NTC Officer). The representatives should be permanent members and not just assigned during a crisis. This will help maintain continuity and consistency.
- EETT staff, headed by a member who has the remit to chair and operate a CMT, including lawyer and media representatives (to provide leadership and advice to the team, and to reflect the regulatory views).

5.4.3.1 *CMT Member Role Profiles*

In addition to being good communicators and resourceful in obtaining information in difficult circumstances members of the CMT will have the following profile.

Role	Member Profile
Crisis manager / chairperson	<ul style="list-style-type: none">• Senior manager, experienced in team meetings and working under pressure• Leadership and guidance are key skills• Knowledgeable of regulatory requirements and the Telecommunications Sector and Services
Scribe and recorder	<ul style="list-style-type: none">• Diligent and resourceful recorder of information• Knowledgeable of meeting formats and adept at interpreting the nuances used in meeting conversations
Data analyst and Knowledge manager	<ul style="list-style-type: none">• Resourceful at gathering disparate data from multiple organisations• Awareness of the types of data required and the priority in obtaining them• Good at cataloguing and interpreting data from multiple sources, well organised• Computer skills to input information and manage the Emergency Management Database system described in the Tools section.
Media interface	<ul style="list-style-type: none">• Engaging and adept media relationship manager• Knowledgeable of different media outlets and how to engage with them
Internal communications	<ul style="list-style-type: none">• Thorough understanding of personal communications, and self-starter capable of seeking out difficult information• Mature and easy to communicate with
User/business impact assessor	<ul style="list-style-type: none">• Aligned to the requirements of the general population and the Critical Sectors (i.e. can engage with the user-community)
Diagnosis coordinator	<ul style="list-style-type: none">• Technical understanding of the Telecommunications Industry
Recovery planner	<ul style="list-style-type: none">• Technical understanding of the Telecommunications Industry
Legal and regulatory advisor	<ul style="list-style-type: none">• Knowledgeable of the regulations and laws governing the telecommunications Industry

Role	Member Profile
Telephone Response Desk	<ul style="list-style-type: none"> • Articulate and pleasant manner, able to react under pressure • Diligent and organised

5.4.3.2 *Carrier Membership Attendance*

Each Carrier must assign an officer of the company, who is responsible for attending the EETT NTC Crisis Management Team meetings.

This role is called **Carrier NTC Officer**.

This officer can be called upon at any time, and will be expected to act in the following role:

- To have direct access to the main board of directors and senior officers of his/her organization, and is comfortable about talking frankly to them about the activities required of the Carrier.
- Is empowered to discuss and make agreements for his/her organization, with or without verbal consent from the main board or senior officers.
- Is expected to negotiate with other Carriers to resolve issues in the best interests of the general public.
- To undertake a specific role in the framework of the CMT.

ACTION - Carriers to identify their internal officers responsible for undertaking the **PROPOSAL** role of Carrier NTC Officer
7:

5.4.4 Communications

5.4.4.1 *Media*

TV and broadcasting are an integral part of the public relations and general information release by EETT, the Carriers, etc.

The key element here is for a 'common-front' to be presented by the Telecommunications Sector. It is important for NTCP to be seen to offer a common and integrated response.

CMT representatives with media management abilities will deal with Media communications issues presented by major incident.

Additional requirements will be:

- A common and consistent line of communications and message.
- An up-to-date bulletin offering real value to the media.
- Information broadcast as to:
 - Start time
 - Cause
 - Impact and extent
 - Recovery status

- Recovery players
- Probable service resumption time
- What EETT and the Carrier want the users to do
- Confirmation that problem management will be undertaken.
- EETT and the Carriers seen to be driving events – being pro-active and NOT reactive.
- Information is the same as in other updated media outlets, such as the Internet and EETT/Government website.

ACTION – The CMT will have media-trained staff who can/will interface with the
PROPOSAL Carrier media staff to offer a single message.
 8:

5.4.4.2 Web-based

With the disruption of telecommunications services during period of crises, it is becoming increasingly important to provide Internet-based information.

The CMT will provide a crisis management bulletin update, including an English translation.

The bulletin will include the same information as mentioned above, plus, a dynamic map showing the areas affected, to include a service incident matrix, providing details of the Carriers and the Critical Services affected (e.g. mobile telephony, etc.).

ACTION - EETT will introduce a NTCP Web site as described in section 7.1.2.3
PROPOSAL “WEB Site” for the EETT and NTCP staff to place news/metrics updates
 9: etc.

5.4.4.3 Public Warning

The general public will require information as to the extent of the crisis and to what steps it should take in order to avoid further deterioration of the telecommunications infrastructure.

A Public Warning and Information Dissemination system is described in section 7.2.1.1 “Public Warning and Information Dissemination Systems”, which can provide the vital link between the Crisis Management Team and other Government disaster support organizations and the general public should be considered.

CMT should use this system to provide a crisis management bulletin and updates through Radio and TV stations in cooperation with other Government organizations.

The information should be consistent with what is available in the web and provided to media.

ACTION – EETT will introduce an Emergency Warning and Information
PROPOSAL Dissemination System to communicate with the general public
 10:

5.4.4.4 Communications To Government

EETT will report directly to the Government Department of Transportation and Telecommunications and any other relevant Government Agencies.

5.4.5 Invoking Responsibilities

5.4.5.1 *Pre-Invocation*

The general process for identifying crises and alerting these to EETT and the subsequent invocation of a Crisis Management Team is the following:

Originating 'Trigger'	Method for identifying and Invocation Process
Carrier Identification	Escalation through Carrier Incident Management process and referral back to the 'Trigger' section as to what is and is not covered. Upon identification that a problem exists, the Carrier then has 30 minutes to inform the EETT NTC CMT.
Media Identification	Broadcast widespread incidents such as earthquake etc. through the TV channels, which is then identified by any or all stakeholders, and then invocation can be generated.
Government Identification	Instruction and command by the Government, contacted directly to the directorate of EETT and/or the Carriers to engage together in order to resolve an actual or impending calamity.
EETT Identification	Suitable analysis and information about the ability of the Carriers to fulfil their service obligation could result in the activation of the Crisis Management Team, with the objective of pre-emption.

ACTION – PROPOSAL 11: EETT will broadcast the Invocation details to the stakeholders upon receipt and identification of an invocation

5.4.5.2 *Overview*

Once the decision to invoke the CMT has been taken, the following process is suggested:

1. Crisis manager / chairperson alerted
2. Crisis manager / chairperson gathers key CMT members at the CMT Situation Management Centre (defined in Tools section)
3. Establish communication facilities (teleconference bridge facilities as described in Crisis Management Team Communications in Tools section).
4. Sets expectations and remind the team what their roles are
5. Identify current status, options, and risks
6. Communicates with stakeholders
7. Device a list of obvious questions
8. Get answers to list of obvious questions

5.4.5.2.1 Triggers

One or more of the triggers outlined in Section 3: “Triggers” and “Table 6: Triggers and Action Plans” have been breached.

5.4.5.2.2 Crisis Manager’s/Chairperson’s Initial Directives for action

Below is a series of ‘scripts’ for CMT activity, based around an indicative timescale:

“Immediately”

For	Request
Scribe- Recorder	Record the reason for invocation, log the decisions made by the CMT, and draw up a timeline of events
Internal Communications	Ensure ready communications with Carrier and stakeholder teams – initially contacting the Carriers and engaging their Crisis Management Teams; keep a list of all contacts and organise any recorded messages.
Media Interface	Contact the media groups within the Carriers, and liaise with main media organizations as and when required. Review press releases from Internal Communications
Crisis manager	Directs the CMT members to complete their duties and return periodically to update the remaining members

“Within the first 30 minutes ...”

For	Request
Telephone Response Desk	Established with a remit of collating any incoming messages from Carriers, CMT members or other stakeholders
Data analyst	Contacts the Carriers and retrieves the metrics etc. relating to any incident (for example, how many telephone exchanges are out of action?” etc.)
Diagnosis coordinator	Contacts the Carriers and ascertains the current issues and incident status. Reviews Government and media information to assess wider issues

“Within the next 30 minutes...”

For	Request
Diagnosis coordinator	Contacts the Carriers and ascertains the nature of the fault, its likely location, time to fix, and options available to clear fault without knowing the full source-root cause
User/business impact	Investigate the impact of the incident upon the users, including number affected, regions, types of Sectors and organisations, etc.

“Within the next 60 minutes...”

For	Request
Recovery planner	Contacts the Carriers and ascertains the options available to recovering the environment and restoring service, including the likely timescales, impact, and cost
Crisis manager / chairperson	Intervene in order for other Government agencies to assist the Carriers with problem resolution if required. (i.e. clear of roads, resolve power problems, urgent equipment transport etc.)

“Within the next 60 minutes...”

For	Request
Legal and regulatory advisor	Details the legality of the recovery options and the current situation, advises accordingly

Obviously these timescales and tasks may vary; however, they represent a guide as to the sequence of events.

5.4.6 Crisis Management Preparation

The following are required to be available prior to invoking:

1. Telephone directory – EETT and Carriers
2. The Information and Crisis Management Command Centre with required facilities (see Tools section)
3. Appropriate Crisis Management Team Communications (see Tools section)
4. Teleconference bridge number and access
5. List of obvious questions
6. Documentation Templates for use by the CMT
7. The post consultation document
8. Pre-arranged security arrangement for external CMT members
9. Carrier Crisis Management Plans
10. Availability of the Emergency Management System.
11. The chosen Public Warning and Information Dissemination System (see Tools section)

5.4.6.1 *Use of Crisis Management Command Centre*

The proposed primary and secondary NTC command centres to be used by the CMT in times of crises are:

Location	Address	Telephone	Priority
EETT designated Office			
Alternate location at a Carrier's facility			

5.4.6.2 Carrier Questions

Answers to the following questions are required by the CMT in order to coordinate a response to a crisis and should be provided by the relevant Carrier within the allocated time frame described in section 4.6 “Carriers’ ACTION - PROPOSALs Timetable”:

High-level

1. What’s the problem, how widespread?	<i>Diagnostic/Media</i>
2. What’s the user (general public/Critical Sector) impact?	<i>Impact</i>
3. What are the commercial repercussions on the Carriers?	<i>Impact</i>
4. When will the service be resumed?	<i>Diagnostic</i>
5. What’s this going to cost?	<i>Impact</i>
6. What alternatives/options do we have – do we have spare equipment we can utilise? What about loaned equipment from other Carriers?	<i>Recovery</i>
7. What risks/costs are associated?	<i>Impact</i>
8. What do you recommend?	<i>All</i>
9. What decision do you want us to make?	<i>All</i>
10. What can we do to assist?	<i>All</i>

Tactical

1. What are our options?
2. What happens if we can’t identify problem?
3. Can we share services between Carriers?
4. What are the priority services and numbers?
5. What spare hardware is available?
6. What priorities can be arranged?
7. What services can be pre-empted?
8. How can we reduce congestions?
9. What are the metrics for failure?
10. What decisions do you want made?
11. What are the lessons to be learned from this?
12. How do we receive data from Carriers?
13. What penalties will be incurred for poor performance?

5.5 SERVICE/BUSINESS RESUMPTION

Service resumption, both as part of the operation of counter-measures and work-around, and also as part of the final resolution and return to normal operation of a crisis or major incident, is a key component.

The business resumption phase can be best described as the **response and recovery** of the service required to conduct a survivable user/Critical Sector and Organisation operating model.

The following decisions and requirements need to be met by the CMT.

5.5.1 NTC CMT Closure Decision Triggers

Once the CMT has been engaged, the triggers for disengagement or continuing with the CMT are different from the original event triggers (this is to avoid the anomaly which will determine that 5,000 users affected cause an invocation of the CMT, but should a reduction of 1 result in CMT disengagement?).

This is because the root-cause may not have been resolved and that continued disruption may still occur.

The Carriers desire to be continually engaged within the CMT process will also depend upon:

- The legal sensitivity towards an organization's (or its directors) liability in managing and mitigating crises.
- The organizations' corporate sensitivity and responsibility.
- The regulatory fines for Carriers not covering obligations stemming from their license of the applied regulations.
- The intensity of the original cause (an earthquake that destroys much telecommunications infrastructure may result in years of service degradation).

Correspondingly the point to disengage will be determined by the following:

- Will a continued and an indefinite root-cause affect the 3 Primary Beliefs? If not, then it will primarily be an issue of commercial concern for the Carrier(s) involved.
- Will the continued engagement of the NTC CMT reduce the impact of the incident, or reduce the eventual ramifications arising from the incident?
- Will a permanent 'working-party' offer better value? (Especially in the case of long-term incidents such as earthquakes, etc.). If so, establish another leadership body to manage the continued incident.
- Will the continued engagement of the NTC CMT add any value to any of the stakeholders?

Summarising, will the Three Primary Beliefs be affected?

Way of Life	Will the way of life be detrimentally altered any further? Will the duration of the incident pose any further longer-term implication?
Stability	Has civic stability been reaffirmed?
Human Welfare	Will there be any further human impact beyond what is reasonable, and can the NTC CMT assist in lessening the extent?

5.5.2 Closure

Closure of a crisis and associated CMT can only be achieved if the 3 primary beliefs are not longer in jeopardy. The closure of a Crisis or Crisis Management Invocation will be reached only when the Problem Management Report described in section 6.2 "CMT Problem Management Report" has been produced. Within this report the agreements

between the Carriers and any other parties involved will be mentioned (e.g. if one Carrier enables another to use their infrastructure).

The final arbiters as to the closure of the Crisis Management Team invoked by triggers will be the Chairperson of the CMT, who has been empowered by the three NTC Leadership Team members.

5.6 DETAILED TRIGGER SPECIFIC ACTION PLANS

As discussed in previous sections each Crisis Event, Critical Infrastructure element problem, Critical Telecom Service problem or Critical Sector/Organization impact will cause a Trigger and subsequent Actions to resolve the problem. Table 6: Triggers and Action Plans presents the Action Plan details of each trigger.

5.6.1 Event, Service, Sector and Trigger Association

Each particular Event has a primary trigger which once breached will initiate the Action Plan process. Depending on the extent of the Event, related Triggers can also be breached. As an example an earthquake of the trigger magnitude 5 Richter (Trigger 3) most likely will cause excessive use of fixed and mobile telecommunications activity and thus defining the primary Trigger action activity.

If telecommunications infrastructure is destroyed or impacted, related triggers will also be breached. Associated action activities for these Triggers are described in the appropriate trigger. In this case one of the tasks of the Crisis Management Team is to identify the root cause of multiple triggers and prioritize actions accordingly. “Table 5: Event, Service, Sector and Trigger Association” presents the relationship between Crisis Events, Telecommunications Critical Services/Sector Impact and the associated Primary/Related Trigger.

5.6.2 Trigger associated Action Plans

Once the Trigger is breached, the process depicted in the Figure 2: Action Plan Process Flow is initiated. The actions associated with each Trigger breached are summarized in Table 6: Triggers and Action Plans. Each triggered action presents:

- the trigger monitoring mechanism,
- the probable impact of the breach,
- any proactive activities which could have prevented the breach or minimized the impact,
- the 1st Level immediate actions which need to be performed mostly by the Carriers,
- the 2nd Level actions which will be performed by the Crisis Management team once activated, and
- the follow-up and closure of the crisis and the action plan.

The table also contains actions to triggers which require actions on behalf of the Carriers and information submission to EETT but no activation.

References to appropriate sections of this document are included for more detail.

Table 5: Event, Service, Sector and Trigger Association

	TRIGGER																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
External Crisis and Emergency Event Scenarios																										
1. Chemical/Nuclear Incident (inside or outside Greece) – non fission explosion		P								R					R	R		R	R	R	R	R	R	R		
2. Nuclear Incident (inside or outside Greece) – fission explosion		P								R					R	R		R	R	R	R	R	R	R		
3. Earthquake	R	R	P							R					R	R		R	R	R	R	R	R	R		
4. Inland Flooding	R			P						R					R	R		R	R	R	R	R	R	R		
5. Coastal Flooding and Tsunami				P						R					R	R		R	R	R	R	R	R	R		
6. Forest Fire and Scrub Fires	R				P					R					R	R		R	R	R	R	R		R		
7. Acts Targeting Industrial and Commercial Centers								P															R			
8. Virus and Malicious attacks on the Carriers									P																	
9. Sudden Income Changes (for a Telecommunications company)											P	P	P													
Telecommunications Infrastructure Impact																										
1. Infrastructure Component Failure	P									R					R	R		R	R	R	R	R		R		
2. General Infrastructure Fires (e.g. fire in a major Telecom Carrier infrastructure)	R					P				R					R	R		R	R	R	R	R	R	R		
3. Acts Targeting Physical Telecommunications Infrastructure	R						P			R					R	R		R	R	R	R	R	R	R		
4. Acts Targeting Telecommunications Control and Command (NMS, TMN)	R						P			R					R	R		R	R	R	R	R	R	R		
5. Capacity Management Failure										P																

	TRIGGER																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Critical Services Impact																										
1. Fixed Line Dialed (National and Local)														P							P					
2. International Direct Dialling														P				P			P					
3. Mobile Telephony														P					P		P					
4. Satellite Telephony and Data (including Maritime emergency)														P							P				P	
5. Internet Services Provision														P						P						
6. Wireless Leased Lines																					P					
7. MAN/WAN Link Services																					P					
8. Data Services																					P					
9. Carrier Network Interconnects																						P				
10. Fixed Leases Lines																					P					
11. Disaster Recovery and Data Centre Sites																							P			
12. Emergency and Priority Services (E112, 100, etc.)																								P		
Critical Sectors Impact																										
1. Health															P											
2. Emergency, Police, Fire, Ambulance and Rescue																P										
3. Shipping and Harbour Control, Immigration																	P									
4. Civil Defence																										P
Various																										P

	TRIGGER																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
NOTE:	P	Primary trigger for specific Scenario, Critical Telecom Service and Critical Sector.																								
	R	Related trigger which could be breached due to specific Event Scenario																								

Table 6: Triggers and Action Plans

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
1a	The loss of infrastructure service capability equivalent to 300,000 user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute.	Carriers to monitor, record and process in real-time the required network and infrastructure statistics which, when processed, will derive the trigger points. These type of statistics are based on Network Management Systems (NMS) and not on user reported calls	Loss of user, interconnect connectivity, (due to possible loss of local loops, concentrator, switch, trunk groups, cable, microwave link, fiber etc)	Verify that the top 10 components of a Carriers network have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup systems and services such as mobile telephone exchanges, mobile cellular base stations, etc. Alternate routing abilities National or regional broadcast messages to land and mobile services informing users as to how to use telecom resources in a crisis.	Invoke NTC Action Plan	Activate Carrier internal Disaster Recovery plans. Activate call control mechanisms to reduce congestion and share resources. Activate call priority for defined Critical Services.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Update of WEB site. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review possible resilience improvements and Carrier future cooperation arrangements where required.
1b	Over 10,000 originating and terminating calls are blocked for inter-carrier communications in any 30 minute interval				Invoke NTC Action Plan			
1c	On two or more consecutive days, there are two or more instances where 10,000 user connections are interrupted for less than 30 minutes				Inform EETT			

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
2	A fission (nuclear) explosion, reported by the Government or media within the borders of Greece or within 100 km of Greece	Carriers and EETT to monitor in real-time news broadcasts	Public panic and excessive use of telecom resources. Possible loss of telecom infrastructure.	User education on telecomm services use in the event of a disaster, distribution of information leaflets.	Invoke NTC Action Plan	Activate call control and call duration mechanism and share resources if required. Activate call priority for defined Critical Services if required.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, monitor for subsequent triggers. Update WEB. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review inter-Agency cooperation.
3	An earthquake of 6 on the Richter scale, reported by the Government or media within the borders of Greece or within 100 km of Greek territory, or above 5 Richter in any urban areas.	Carriers and EETT to monitor in real-time news broadcasts	Public panic and excessive use of telecom resources. Possible loss of infrastructure resources. Emergency situation requiring special telecom service provisioning.	Mobile base stations and mobile public telephones available for deployment to stricken areas. User education on telecomm services use in the event of a disaster, distribution of information leaflets. Telephone exchanges to be build to an earthquake-proof specification, with backup generators etc.	Invoke NTC Action Plan	Activate call control mechanisms to reduce congestion and share resources if required. Activate call priority for defined Critical Services if required.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, monitor for subsequent triggers. Deploy mobile base stations and public telephones if required. Update of WEB site. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review inter-Agency cooperation. Review Impact to infrastructure and suggest improvements.

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
4	Flooding affecting any town over 5,000 people, reported by the Government or media	Carriers and EETT to monitor in real-time news broadcasts	Public panic and excessive use of telecom resources, possible loss of infrastructure resources. Emergency situation requiring special telecom service provisioning.	Mobile base stations and mobile public telephones available for deployment to stricken areas. User education on telecomm services use in the event of a disaster, distribution of information leaflets. Telephone exchanges away from potential flood areas.	Invoke NTC Action Plan	Activate call control mechanisms to reduce congestion and share resources if required. Activate call priority for defined Critical Services if required.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, monitor for subsequent triggers. Deploy mobile base stations and public telephones if required. Update of WEB site. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review inter-Agency cooperation. Review Impact to infrastructure and suggest improvements.

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
5	A forest or scrubland fire reported as threatening population centers, reported by the Government or media. Will cause a secondary trigger if it impacts telecommunications infrastructure.	Carriers and EETT to monitor in real-time news broadcasts	Public panic and excessive use of telecom resources. Possible loss of telecom infrastructure.	User education on telecomm services use in the event of a disaster, distribution of information leaflets. Verify that the top overhead network links have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup links and services and mobile cellular base stations. Alternate routing abilities. Place protection around telecommunications assets in regions likely to experience intense fires (forest or otherwise, such as major oil storage works etc.)	Inform EETT	If no impact to telecom infrastructure monitor the event. If congestion occurs activate Carrier internal Disaster Recovery plans. Activate call control mechanisms to reduce congestion and share resources. Activate call priority for defined Critical Services.	EETT will monitor the situation and the information provided by the Carriers. If necessary NTC will be invoked and CMT will be activated. Update of WEB site.	Depends on the extend of the event and possible impact to telecommunication infrastructure. Review telecommunications needs of responding agencies (Fire, Police).

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
6	Any fire in any switching station, cable termination centre, or other Carrier establishment where hardware needed to support telecommunication services is damaged. Will cause a secondary trigger if it impacts telecommunications services.	Carriers to monitor telecommunications facilities environmental conditions.	Loss of connectivity and services, (due to possible loss of local loops, concentrator, switch, trunk groups, cable, microwave link, fiber etc)	Verify that the top 10 components of a Carriers network have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of environmental monitoring (Fire, Smoke detection). Existence of backup systems and services such as mobile telephone exchanges, mobile cellular base stations, etc. Alternate routing abilities. National or regional broadcast messages to land and mobile services informing users as to how to use telecom resources in a crisis.	Inform EETT	Activate Carrier internal Disaster Recovery plans. Activate call control and call duration mechanism to reduce congestion and share resources. Activate call priority for defined Critical Services. Deploy available backup systems.	EETT will monitor situation and activate CMT if appropriate. Upon activation CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Coordination for inter-carrier equipment and resource sharing where applicable. Mitigation of legal issues. Coordination with Government Agencies where appropriate. Update of WEB site.Interface with media.	CMT to document crisis and resolution. Review possible resilience improvements and Carrier future cooperation arrangements where required.

			Actions (Crisis Management)					
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
7	An actual terrorist act or perceived terrorist threat against telecommunications infrastructure, reported by the Government or media.	Carriers and EETT to monitor in real-time news broadcasts	Potential for telecom infrastructure impact resulting in other triggers being breached.	Carrier premise security enhancement, bomb proofing, manhole protection etc.	Invoke NTC Action Plan	Carriers to increase security alert at all facilities. Prepare for disaster recovery activation.	CMT Activation. Monitor situation. Liaison with Government Agencies and interface with Carriers.	Issue Problem Management Report, Lease with Related Government agencies to review interaction during event.
8	An actual terrorist act resulting in the loss of life or the closure of multiple businesses reported by the Government or media	Carriers and EETT to monitor in real-time news broadcasts.	Potential for excessive network activity. Potential for business telecommunications services disruptions.	Carriers should have Business Customer support centers and processes. Carrier premise security enhancement, bomb proofing, manhole protection etc.	Inform EETT	Prepare to support Business Customers disaster recovery plans such as circuit and connectivity switch over to alternate data centers, telephony traffic to chosen call centers and any other activity chose by the businesses impacted. Carriers to increase own security alert and prepare for disaster recovery activation.	EETT will monitor situation and will invoke NTC if necessary. Liaison with Government Agencies and interface with Carriers.	Issue Problem Management Report, Lease with Related Government agencies to review interaction during event.

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
9	Any unauthorized internal or external malicious attack on the Carriers affecting the ability to deliver service or to secure personal data records of consumers and businesses	Carriers to monitor IT systems.	Potential for telecom services impact and personal data breach.	Curriers should have proper information security policy for staff and customers, fire walled systems, DMZ zones etc. Perform annual systems penetration tests.	Inform EETT	Carriers to identify, deactivate and patch breached system.	Carriers to identify extend of breach, confirm data validity, remedy accordingly. Interface with media.	N/A
10	Capacity on any element of the telecommunications infrastructure where traffic exceeds 90% of total possible traffic, in any single exchange, switching centre, communications paths (e.g. cabling)	Carriers to monitor in real-time the capacity of the networks, with appropriate alerts, and ability to report on changes over a 1 year period.	Potential for network congestion and user outages.	Capacity planning, mechanisms for reallocating resources such as bandwidth, trunk capacity, systems processing. Mechanisms and processes for call management (Call Priority, Call Duration Control, Rate Control, Call Percentage Control, Call Blocking Control, Call Gapping)	Inform EETT	Activate call control mechanisms to reduce congestion and share resources if required. Activate call priority for defined Critical Services if required.	EETT will monitor situation and activate CMT if appropriate. Upon activation CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Coordination for inter-carrier capacity issues.	If CMT is activated, issue Problem Management Report, document resolution, review workaround and agree on enhancements for future problem avoidance.

			Actions (Crisis Management)					
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
11	Any Carrier share-price drop of 30% in a week, or any operational financial loss, or any financial irregularities identified by auditors or other agents	Carriers and EETT to monitor in real-time news broadcasts	Potential for business collapse and user services impact.	N/A	Inform EETT	N/A	EETT will monitor situation and activate CMT if appropriate. If CMT is activated review potential customer risk.	N/A
12	Annual investment report and update via the Service Management report. Where EETT believes the investment profile may not be commensurate with the Three Primary Beliefs	Carriers to deliver an annual investment report to EETT, detailing the total investment in infrastructure and the planned changes in infrastructure, over the next 5 years	Impact in infrastructure survivability, resiliency, capacity. Potential for service level deterioration.	Infrastructure, technology investments in line with revenues, customer levels, industry refresh trends, and technology trends.	Service Management Report (See Section 6.1)	Carriers to prepare and submit report bi-annually.	EETT will monitor situation provide guidance and statistics when and where appropriate.	EETT will award excellence when appropriate.

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
13	Any medical-related announcement regarding mobile Carrier activity that is followed, within a week, by a 25% drop in call traffic volumes to and from mobile telephone users	Carriers and EETT to monitor public news broadcast. Create new or enhance existing Telecom Leadership Forum consisting of representation of the Carriers and EETT	Potential for impacting mobile usage and industry survivability.	Instructions on proper use of mobile technology. Publicizing of relevant studies and reports.	Telecoms Leadership Forum	Carrier participation in Leadership Forum and establishment of common approach.	EETT will participate in Telecom Leadership Forum and will monitor situation providing guidance and information when and where appropriate. Interface with media.	N/A
14	Annual traffic report showing peak flows and problems	Carriers to monitor traffic statistics	Identification of potential issues and trends which could impact services.		Service Management Report	Carriers to prepare and submit report bi-annually.	EETT will monitor situation provide guidance and statistics when and where appropriate. Interface with media.	N/A

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
15	Any registered hospital telecommunications outage for more than 60 minutes	Carriers to report to EETT Emergency user complaint. The organization/Sector holding the priority number has an obligation to report outages to EETT as part of the arrangement of being made 'a priority service'.	Impacting the wellbeing of the general public.	Carrier review of hospital telecommunications, and suggest recommendation for resilient service implementation and back-up solutions where appropriate.	Invoke NTC Action Plan	Identify problem area. Network prioritization of impacted service. Rerouting of relevant traffic in coordination with impacted hospital.	CMT Activation. CMT decisions on call prioritization parameter modifications. Coordination between involved carriers, coordination with impacted hospital, coordination with relevant Government Agency where appropriate. Interface with media. Interface with media.	Issue Problem Management Report. Identification of root problem, and coordination with impacted hospital for alternative and back-up solutions where appropriate.
16	Any registered Fire, Ambulance and Rescue fixed or mobile telecommunications outage for more than 30 minutes	Carriers to report to EETT Emergency user complaint. The organization/Sector holding the priority number has an obligation to report outages to EETT as part of the arrangement of being made 'a priority service'.	Impacting the wellbeing of the general public.	Carrier review of emergency agency telecommunications, and suggest possible recommendation for resilient service implementation and back-up solutions where appropriate.	Invoke NTC Action Plan	Identify problem area. Network prioritization of impacted service. Rerouting of relevant traffic in coordination with impacted emergency agency.	CMT Activation. CMT decisions on call prioritization parameter modifications. Coordination between involved carriers, coordination with impacted emergency agency, coordination with relevant Government Agency where appropriate. Interface with media.	Issue Problem Management Report. Identification of root problem, and coordination with impacted emergency agency for alternative and back-up solutions where appropriate.

Trigger		Trigger Monitoring	Resulting in	Actions (Crisis Management)				Follow-Up
				Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	
17	Any registered shipping and harbour control telecommunications outage for more than 60 minutes	Carriers to report to EETT any Shipping and Harbour control complaint. Emergency user complaint	Impact to the general public established way of life and national economic wellbeing.	Carrier review of agency telecommunications, and suggest possible recommendation for resilient service implementation and back-up solutions where appropriate.	Invoke NTC Action Plan	Identify problem area. Network prioritization of impacted service. Rerouting of relevant traffic in coordination with impacted agency.	CMT Activation. CMT decisions on call prioritization parameter modifications. Coordination between involved carriers, coordination with impacted agency, coordination with relevant Government Agency where appropriate. Interface with media.	Issue Problem Management Report. Identification of root problem, and coordination with impacted agency for alternative and back-up solutions where appropriate.

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
18a	Failure of international service resulting in 5,000+ failed international calls within a 30-minute interval (could be caused by routing difficulties, transmission, etc.)	Carriers to monitor and process call statistics and in real-time	Failure of incoming and outgoing international traffic	Verify that the top network elements associated with international traffic have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup systems and services such as mobile telephone exchanges, etc. Alternate routing abilities.	Invoke NTC Action Plan	Activate Carrier internal Disaster Recovery plans. Activate call control mechanisms to reduce congestion and share resources. Deploy available backup systems.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Update of WEB site. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review possible resilience improvements and Carrier future cooperation arrangements where required.
18b	Over 15,000 originating and terminating international calls are blocked for Inter-carrier communications in any 30 minute interval				Invoke NTC Action Plan			
18c	The loss of infrastructure service capability equivalent to 150,000 international user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute				Invoke NTC Action Plan			

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
19a	The loss of 5,000 potential mobile telecom users brought about by a single incident, root-cause, or within a 30-minutes interval. To estimate the potential users the affected system capacity should be multiplied by a contention factor of 10. Thus an MSC which is capable of handling 500 simultaneous calls would potentially impact 500x10=5,000 users.	Carriers to monitor and process call statistics and in real-time	Failure of mobile telecommunications services.	Verify that the top network elements associated with mobile services have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup systems and services such as transportable mobile telephone exchanges, base stations etc. Alternate routing abilities.	Invoke NTC Action Plan	Activate Carrier internal Disaster Recovery plans. Send SMS to users and inform them about call restrictions. Activate call control mechanisms to reduce congestion and share resources. Activate Critical Services priority mechanisms. Deploy available backup systems such as transportable base stations.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Coordinate between Carriers for resource sharing. Coordinate between carriers for Critical Sector service restoration where appropriate. Update of WEB site. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review possible resilience improvements and Carrier future cooperation arrangements where required.
19b	The loss of mobile infrastructure service capability equivalent to 150,000 user minutes within any 30-minute interval that comprises of 2 or 3 separate instances. A user minute is an outage of 1 user access for 1 minute. The number of users is calculated as in the previous trigger point.				Invoke NTC Action Plan			

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
19c	The concurrent total or partial loss of service for 4+ ‘cells’ (based around a mast) for a total of 30 minutes (i.e. 4 cells inactive due to the same root-cause during a 30 minute interval) brought about by a single incident or root-cause				Invoke NTC Action Plan			
19d	Over 15,000 originating and terminating calls are blocked for inter-carrier communications in any 30 minute interval				Invoke NTC Action Plan			
20	Loss of Internet telecommunications connectivity to an ISP impacting more than 10,000 users for more than 30 minutes	Carriers to inform EETT about ISP complaint. ISP can also inform EETT directly.	Loss of Internet access to public users.	Carrier review of ISP telecommunications arrangements, and suggest possible recommendation for resilient service implementation and back-up solutions where appropriate.	Invoke NTC Action Plan	Identify problem area. Network prioritization of impacted service. Rerouting of relevant traffic in coordination with impacted ISP.	CMT Activation. CMT decisions on network prioritization parameter modifications. Coordination between involved carriers, coordination with impacted ISP. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review possible resilience improvements. Review connectivity with ISP and suggest alternatives and improvements.

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
21	The loss of or disruption to any service group affecting more than 30% of the subscribers using those services within any single switching exchange / transmission center	Carriers to monitor traffic and network statistics.	Loss of telecommunication service such as fixed, wireless leased lines, WAN/MAN services, Data service, satellite services etc.	Verify that the associated components of a Carriers network have suitable resilience. Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup systems and services. Alternate routing abilities. Work with customers using services to suggest resilience and back facilities.	Invoke NTC Action Plan	Activate Carrier internal Disaster Recovery plans. Activate network control mechanisms to reduce congestion and share resources where appropriate. Deploy available backup systems.	CMT Activation. CMT decisions on resource allocation, network control parameter modifications, restoration coordination, and remedial actions. Coordination with key impacted users. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Review possible resilience improvements. Review connectivity with key impacted users and suggest alternatives and improvements.

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
22	A 90% utilization for any Carrier-Carrier interconnects lasting for a continuous period of 30 minutes or more.	Carriers to monitor traffic statistics.	Impact to alternative carrier services	In coordination with Alternative carrier perform capacity planning, introduce mechanisms for reallocating resources such as bandwidth, trunk capacity, systems processing. Mechanisms and processes for call management (Call Priority, Call Duration Control, Rate Control, Call Percentage Control, Call Blocking Control, Call Gapping)	Inform EETT	In cooperation with impacted Alternative carrier activate call control mechanisms to reduce congestion and share resources if required. Activate alternative routing where available. Activate call priority for defined Critical Services if required.	EETT will monitor situation and activate CMT if appropriate. Upon activation CMT decisions on resource allocation, call control parameter modifications, restoration coordination, and remedial actions. Coordination for inter-carrier capacity issues.	Issue Problem Management Report. CMT to document crisis and resolution. Coordinate between carriers. Review connectivity architecture and suggest alternatives and improvements.

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
23	Loss of a Carrier Data/Network Management Centre, or a Critical Sector Data Centre managed by the Carrier.	Carriers to monitor environments	Loss of carrier data/network management and control. Loss of Critical Sector IT and telecom environments.	Carrier alternate data/network management facilities. For Carrier and Carrier managed Data Center environments deployment of environmental monitoring (fire/smoke detection, water detection etc). Deployment of proper air-conditioning, UPS power, generators. Resilient connectivity arrangements	Invoke NTC Action Plan	Activate Carrier internal Disaster Recovery plans. Activate alternate data/network management center.	CMT Activation. Assist impacted Carrier/Critical Sector with: Inter-carrier coordination/cooperation activities, assistance requirements from Government agencies, assistance requirements from public utilities. Interface with media.	Issue Problem Management Report. CMT to document crisis and resolution. Consolidate damage assessments and provide status reports. Review possible resilience improvements and Carrier future cooperation arrangements where required.

			Actions (Crisis Management)					
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
24a	100 failed attempts to access Emergency or Priority numbers (100, 166, 199, 112, etc.) in a duration, which needs to be agreed with the Emergency Service operator.	The Carriers to monitor and process call attempts. The Emergency Services operator to monitor call processing.	Impacting the wellbeing of the general public.	Carrier review of emergency agency telecommunications, and suggest possible recommendation for resilient service implementation and back-up solutions where appropriate. Have available call priority mechanisms for all Emergency and Critical sector calls.	Invoke NTC Action Plan	Identify problem area. Initiate call prioritization of impacted service. Rerouting of relevant traffic in coordination with impacted emergency agency.	CMT Activation. CMT decisions on call prioritization parameter modifications. Coordination between involved carriers, coordination with impacted emergency agency, coordination with relevant Government Agency where appropriate. Coordinate recovery activities. Monitor response operations. Communicate, coordinate and pass information to all stakeholders. Consolidate damage assessments and provide status reports. Ensure that the management and recovery activities are within the law. Interface with media.	Issue Problem Management Report. Identification of root problem, and coordination with impacted emergency agency for alternative and back-up solutions where appropriate.
24b	No ability to originate, terminate, or complete calls related to Emergency or Priority numbers for more than 30 minutes.				Invoke NTC Action Plan			

		Actions (Crisis Management)						
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
25	Service interruption or serious downgrading of service for more than 30 minutes offered by Hellas-Sat	Carrier to monitor satellite operation.	Loss of satellite delivered services	Verify that the associated components of a Carriers network have suitable resilience (alternate transponders, uplink earth-station etc.). Regularly reviewing Business Continuity plans, network topology and maintenance arrangements. Existence of backup systems and services. For critical services suggest to customers possible terrestrial alternate routing abilities.	Invoke NTC Action Plan	Identify root cause. Activate back-up, alternate path where available (alternate transponders, earth station etc)	CMT Activation. Coordinate recovery activities. Monitor response operations. Communicate, coordinate and pass information to all stakeholders. Consolidate damage assessments and provide status reports. Ensure that the management and recovery activities are within the law.	Issue Problem Management Report, Document problem and resolution.

				Actions (Crisis Management)				
Trigger		Trigger Monitoring	Resulting in	Proactive preparation	NTC Action Plan	1 st level-immediate	2nd level- after CMT meeting	Follow-Up
26a	Deadly disease epidemic or pandemic that causes death in 50% of cases, or is likely to cause more than 50,000 deaths in Greece, that is either already within Greece or that will soon reach Greece	Carriers and EETT to monitor in real-time news broadcasts	Public panic and excessive use of telecom resources, Emergency situation might require special telecom service provisioning.	User education on telecomm services use in the event of a disaster, distribution of information leaflets. Carrier staff immunization arrangements.	Invoke NTC Action Plan	Activate call control mechanisms to reduce congestion and share resources if required. Activate call priority for defined Critical Services if required.	CMT Activation. CMT decisions on resource allocation, call control parameter modifications, monitor for subsequent triggers. Update of WEB site. Interface with media.	Issue Problem Management Report, Document problem and resolution. Review emergency relief Government Agency requirements/cooperation.
26b	At least 200 user complaints to the offices of EETT within one working day, relating to any single telecommunications service or with reference to any single root cause	EETT will monitor complain activity	Possible service outage, or trigger point about to be breached.	N/A	Invoke NTC Action Plan		CMT Activation. CMT investigation of root cause and source of trouble. Coordination with Carriers to resolve user complains. Update of WEB site.	Issue Problem Management Report, Document problem and resolution.
26c	Carrier unable to collect and process a relevant trigger metric for a period of over 1 hour	Carriers to monitor trigger process.	Carriers unable to determine trigger breach	Resiliency in IT, network management systems. Documented processes for monitoring trigger points.	Inform EETT	Restore Capability	EETT will monitor situation through reports provided by the relevant Carrier.	Issue Problem Management Report, Document problem and resolution.

SECTION 6: REPORTING

6.1 CARRIER BI-ANNUAL SERVICE MANAGEMENT REPORTS

6.1.1 Purpose

The purpose of the Carrier Service Management Report is to:

- Provide clarity and transparency to performance.
- Display the metrics from which national analysis and problem management conclusions can be drawn.
- Identify structural issues regarding technical infrastructure, services etc.
- Justify decisions.
- Improve the service quality and set targets/incentives accordingly.
- Identify weaknesses in the network and alter investment strategies accordingly.
- For the Carriers to display a high degree of understanding in their own service management.
- Justify Government decisions.

6.1.2 Metrics and Key Performance Indicators Report Contents

The Service Management Report must contain the following minimum data:

Heading	Required Data and KPIs
Congestion (80-90% capacity utilization)	<ul style="list-style-type: none">▪ User accounts▪ Interconnects (state adjoining Carriers)▪ Bandwidth▪ International traffic▪ Mobile masts (number of cells experiencing congestion, location of these cells, etc.)▪ Areas where there is congestion (service, technical, demographic; and geographical)
Incidents	<ul style="list-style-type: none">▪ Services affected (and to what extent)▪ Infrastructure affected (and to what extent)▪ Critical Sectors and Organizations affected (and to what extent)▪ Emergency numbers affected (and to what extent)▪ Use of priority numbers and routing▪ Average time to resolve▪ Total number of concurrent incidents (per hour if possible)
Problems	<ul style="list-style-type: none">▪ Top 10 incident types▪ Mitigating action required to resolve top-10
Capacity	<ul style="list-style-type: none">▪ Total number of users per service▪ Average spare capacity per exchange▪ Available numbers versus used numbers

Heading	Required Data and KPIs
Availability	<ul style="list-style-type: none"> ▪ Availability of the Critical Services
Investment Appraisal	<ul style="list-style-type: none"> ▪ Capital investment planned every year for the next 5 years (nominally and as a percentage of current assets) ▪ Breakdown between replacement investment and upgrade / improvement investment
Business Continuity	<ul style="list-style-type: none"> ▪ Internal BCM Officer ▪ Carrier's NTC Interface Officer ▪ Number of internal Business Continuity invocations

The Service Management Report requirements will vary over time in order to deliver the correct value and reflect the current state. The requirements for updating the Service Management Report will be released by EETT according to section 6.1.3 "Periodicity" in the form of a 'questionnaire' that forms the basis of the service management report.

6.1.3 Periodicity

The reports will be released on 1st June (covering the period 1st November - 1st May) and 1st December (covering the period 1st May - 1st November) every year

The following indicative timetable is proposed:

Activity	Date
Year End Report	
EETT release 'questionnaire' to Carriers to cover period 1 st November 2005 - 1 st May 2006	30 th September 2005
Carriers respond with 'Service Management Report – Period: 1 st November 2005 - 1 st May 2006' to EETT	1 st June 2006
EETT to review questionnaire results for period 1 st November 2005 - 1 st May 2006	1 st June 2006 - 1 st August 2006
EETT to document questionnaire results for period 1 st November 2005 - 1 st May 2006	1 st August 2006 - 1 st September 2006
EETT publish 'Analysis of Telecommunications Services - Period: 1 st November 2005 - 1 st May 2006'	1 st September 2006
EETT to adapt new questionnaire for period 1 st November 2006 – 1 st May 2007	1 st September 2006
EETT release 'questionnaire' to Carriers to cover period 1 st Nov 2006 - 1 st May 2007	30 th September 2006
Year Beginning Report	
EETT release 'questionnaire' to Carriers to cover period 1 st May 2006 - 1 st November 2006	31 st March 2006
Carriers respond with 'Service Management Report	1 st December 2006

Activity	Date
– Period: 1 st May 2006 - 1 st November 2006’ to EETT	
EETT to review questionnaire results for period 1 st May 2006 - 1 st November 2006	1 st December 2006 - 1 st February 2007
EETT to document questionnaire results for period 1 st May 2006 - 1 st November 2006	1 st February 2007 - 1 st March 2007
EETT publish ‘Analysis of Telecommunications Services - Period: 1 st May 2006 – 1 st November 2006’	1 st March 2007
EETT to adapt new questionnaire to cover period 1 st May 2007 – 1 st November 2007	1 st March 2007
EETT release ‘questionnaire’ to Carriers to cover period 1 st May 2007 - 1 st November 2007	31 st March 2007

6.1.4 Governance

The governance of the Service Management Report is as follows:

- Every Carrier under licence of EETT must submit a report.
- The ultimate owner of the report within the Carrier organisations should be the highest-ranking officer.
- The report must be addressed to the Regulator (EETT).
- The report will be subject to review by EETT and there is the possibility of further investigations to understand the details behind the information.

6.1.5 Communication and Feedback

The general communications for the Service Management Report will be formed around the following four points:

- EETT will submit a biannual Service Management template and definition as to the requirements and boundaries of all the metrics and KPI’s (for example, “what is spare capacity per exchange?”).
- Carriers will submit the response to the ‘template questionnaire’ in the form of the Service Management Report.
- EETT will release a ‘Survey of Telecommunications Services’ 3 months after the Carriers submit their Service Management Report. This will be in confidence [i.e. no Carriers mentioned by name], and will show the ‘average’ performance (i.e. as a % of Carrier total capacity etc.).
- Lessons Learned as part of the CMT Problem Management reporting (see below) will also be referred to.

6.2 CMT PROBLEM MANAGEMENT REPORT

This Section outlines the traditional requirements for problem management, and then details how these need to be adapted to fit the requirements of a National Telecommunications Contingency environment.

The scope is to outline:

- The best practice for Problem Management.
- The Problem Management requirements for the National Telecommunications Contingency.

6.2.1 Background

6.2.1.1 *Approach to Problem Management section*

The considerations for the development of this section are:

- An understanding that by describing a best-practice approach, EETT can gain an additional insight into how the Carriers should be reducing the impact and frequency of incidents.
- An explanation as to how Problem Management can be best applied, and how this can most effectively be delivered, both as part of Carrier business-as-usual, and also as part of a crisis affecting service delivery to the Critical Organisations and industries.

6.2.1.2 *Problem Management Scope and Definition*

In ITIL terminology, a 'Problem' is defined as:

An unknown underlying cause of one or more incidents.

Problem Management is the method for cataloguing and analysing the root-cause of an Incident and for ensuring that the full extend of lessons learned are undertaken.

The output of a Problem Management process will be a set of recommendations and an action plan for reducing the impact and likelihood of incidents in future.

The purpose of the Problem Management process is:

- To formally close any major incident or crisis and satisfy the stakeholder that due diligence exists.
- To provide historical data to ensure that the same mistakes are not repeated.
- To ensure that the Carriers collate the correct data when resolving incidents/crises.

The Scope for EETT of the Problem Management process is:

- The assessment and root-cause analysis for any invocation of the NTC CMT or any trigger point at the conclusion of the crisis.
- The analysis of all Carrier Service Management Report, resulting in a trend analysis of incident performance, capacity management, and service levels to the users and Critical Sectors.

6.2.2 Purpose

The purpose of the CMT Problem Management Report is to:

- Provide the Carriers with better market information about crisis management.
- Stop similar root-causes arising again and causing incidents.
- Improve quality and speed of recovery for future crises.
- Improve resilience within the Carrier, Critical Sector and Organisation communities.
- Ensure that any legal aspects which may arise from a severe outage have a point of reference.
- Enable the creation of an improved telecommunications policy and regulation, allowing EETT and the Government to refine regulation accordingly.
- Provide international disaster management structure and telecommunications bodies with details of Greek crisis management capabilities and lessons learned.

6.2.3 Report Data Content

The report must contain the following data:

- Date/time and duration, from first report of incident, to when the NTC CMT was invoked, through to closure.
- Crisis name.
- Brief description of crisis.
- Trigger point.
- How the crisis manifested itself, along with a sequence of events.
- Impact on Critical Services, Critical Sectors and Organizations, and general public communities – including metrics relating to coverage, accounts affected, etc.
- Affect on the Carrier organisation.
- How crisis management evolved during the process, the decision process, etc.
- The stakeholders (including names) involved – customers/users, EETT staff, Carrier staff, etc.
- Relationship and interaction between stakeholders.
- Remedial action undertaken to ensure service resumption.
- Activities done well – activities done not so well.
- Cost of recovery, cost of outage.
- Conclusion and recommended alterations and action plan to further mitigate.
- Other information.

6.2.4 Periodicity

The reports should be released within 30 days of the service resumption following an invocation of the NTC CMT, or from informing EETT that there has been a breach of a trigger, or from the point that a trigger was breached.

6.2.5 Governance

The governance of the CMT Problem Management Report is as follows:

- The CMT will oversee the production of the report, liaising with the Carriers involved, and incorporating comments, etc. from some of the Critical Sectors and Organizations affected.
- The Carriers are expected to forward the information upon request to the CMT (based upon the list of Data Content mentioned above).

SECTION 7: TOOLS AND PREPARATORY ACTIVITIES

The information within this section outlines the required tools and operations to support the NTC Action Plan and Crisis Management environment.

7.1 CMT LOCATION SUPPORT

7.1.1 Carriers

There are no specific tool elements for the Carriers to have available for the CMT location, with the exception of a Call Tree.

7.1.2 EETT

7.1.2.1 Information and Crisis Management Command Centre (ICMCC)

A “Command and Information Centre” is required where the Critical Events can be managed and the CMT can use as their command centre.

During periods of no Critical Events this Centre could be used by NTC related personnel:

- To work on improving coordination procedures between all of the Carriers and organizations (Government and private).
- To manage public relationship as described in the “Public Awareness” section.
- To establish and update the WEB site.
- To improve the Emergency Management System.
- To perform as the permanent national clearing house for everything relating to public telecommunications disaster prevention and recovery.
- To manage the national public warning and information dissemination system described previously (testing, update etc.).

During instances of disaster events the situation centre should:

- Be the joint command, control and contact centre for all CMT activity.
- Be the interface point to the public with respect to telecommunications Disaster Recovery.
- Be the place of Public Warning and Information Dissemination System operation.
- Be the telecommunications environment interface to other Government crisis management agencies.

This centre should be established in a secure, resilient and hardened facility in order to survive potential impact from the specific event. It should incorporate the communications facilities described in the next section.

The following should also be available at the Centre at all times awaiting invocations.

- PCs, printer, software.
- Telephony access to Carriers as described in section 8.1 and below.
- The chosen communications tools for each CMT member (mobile, beeper, TETRA etc.).
- UPS power.
- Access to the Public Warning and Information Dissemination System.
- Access to the WEB site described below.
- This document.
- Access to the Emergency Management System described below.
- Access to call tree and other contact information.

ACTION – PROPOSAL 12: The Information and Crisis Management Centre will be established under the leadership of EETT, in cooperation with the Telecommunications Carriers and be available for invocation at all times.

7.1.2.2 Crisis Management Team communications

The importance of communications between CMT members, EETT, Carriers and other organizations during ICMCC activation after a disaster cannot be overstated. During either an alert or a mobilization, team members need to rapidly get in touch and stay in touch with each other. Considerations for team communications will include the following:

- Intra-crisis team communications, especially during infrastructure impact and loss of life events.
- Telecom Carrier crisis team communications, e.g., to coordinate logistics, inter-Carrier assistance, etc.
- Crisis team leader communication with ICMCC.
- ICMCC communication with other Government and civil authority incident command posts (e.g. fire department or emergency operations centre).
- Communication with the site of the of event: urban, suburban, rural.
- Communication with other Government and disaster support organizations.

Modality	Merits	Disadvantages
Pager	Can be used to alert and mobilize team. Can be used to pass text messages back and forth to individuals or entire team.	Useless for tactical communications. Useless for emergency communications.
Wired telephone	Most useful for mobilizing Crisis team for advanced warning of impending disaster (e.g. storm, etc.)	Team must use a “telephone tree” to contact team members. Takes time and, in an earthquake will most likely be unavailable. Numbers used could be included in suggested priority mechanism.

Modality	Merits	Disadvantages
Mobile telephone	<p>Tend to be ubiquitous (i.e. everyone has one)</p> <p>Portable</p> <p>It would be very useful if the mobile Carrier can set up to operate like a portable “2-way” radio and for a “party-line” where everyone on the call can hear what’s going on (extremely important).</p>	<p>In a major disaster wireless, like a wired phone, might be unavailable. Short battery life. Fragile. Team must use a “telephone tree” to contact team members. Takes time and, in an earthquake, might not be available (if the event itself doesn’t disrupt service, congestion might). Frequently, providers have a single “back-haul” route (i.e., no redundancy) to their switching centres - a significant liability for earth quake-prone locales. The numbers used could be put in the priority mechanism described in this section.</p>
Teleconference Bridge	<p>Easily available service. “Party-line” where everyone on the conference can hear each other with very good quality (extremely important). Can be used with wired and wireless telephones.</p>	<p>Depends on plain telephone service that might be impacted by the event. The numbers used could be put in the priority mechanism described in this section.</p>
CB hand-held radio	<p>Portable. Cheap, easily available. “Party-line” where everyone on the channel can hear what’s going on (extremely important). No licensing required. Relatively flexible with 40 channels available</p>	<p><i>Lots</i> of interference because of their ubiquitous-ness. The frequencies on which CBs operate carry very long distances (“skips”) during periods of moderate-to-high sun spot activity, contributing to their high level of noise. Requires civil authorities to have a similar capability if communication with them is required. Radio itself requires periodic testing to ensure batteries are charged or fresh.</p>
Satellite	<p>Communications is not affected by terrestrial infrastructure damages. Commercially available portable and handheld equipment of small size for a variety of services</p>	<p>Line of sight is required and indoor operation is not possible. Battery life is an issue.</p>
TETRA	<p>Noise-free operation. Commercial equipment is typically quite robust. “Party-line” where everyone on the channel can hear what’s going on (extremely important). Other emergency organizations might be using them as well.</p>	<p>Possible congestion during disaster. Battery life.</p>

ACTION – PROPOSAL 13:	EETT working together with the Carriers to identify the best combination of equipment and services for continuous communication among the involved members The cost of the communications requirement will be covered by each participating organization.
------------------------------	---

7.1.2.3 *WEB Site*

As part of the properly organizing the ICMCC, and providing proper public awareness, a website is required that will contain a publicly accessible section and a password protected secure section.

- The public sections will incorporate as a minimum:
 - Information for public behaviour.
 - Emergency response numbers and procedures.
- Basic description of disaster scenarios and associated action plan.
- Information regarding availability of Emergency Services (provided by Telecom Carriers).
- Information regarding the health of the telecommunications infrastructure of all Carriers (provided by the Telecom Carriers and possibly viewable only by the Carriers and EETT).
 - Information regarding the health of telecommunications services (provided by the Telecom Carriers).
- The secure section will incorporate as a minimum:
 - Crisis Team contact information.
 - Escalation procedures.
 - A depository of all information associated with the national action plan.
 - Any other information mutually agreed between EETT and the Telecommunications Carriers.
 - Access during crisis, to the Emergency Management System described below.
 - During crisis, information for the public as described above.

ACTION – PROPOSAL 14:	EETT in cooperation with the Telecommunications Carriers will consider the development of a website and an update mechanisms EETT working together with the Carriers to identify the best combination of equipment and services for continuous communication among the involved members
------------------------------	--

7.2 MEDIA AND CARRIER COMMUNICATIONS

7.2.1 Carriers

7.2.1.1 Public Warning and Information Dissemination Systems

During and after a disaster in the public telecom infrastructure it is imperative to keep the users informed and sometimes advise them on how to use the telecom public network. Based on current and leading edge telecommunications technologies, public warning and event information broadcasting systems should be considered. In order to reach as many users as possible, the core components of these systems should utilize broadcast via radio and television and possibly SMS broadcasts. Since the public must, in certain cases, be alerted rapidly and continuously be informed about the restoration progress, a medium capable of transmitting emergency messages and information as quickly as possible should be considered. Examples of this type of systems exist in Canada, USA, Germany and other countries.

One example is to use a satellite communication based solution. Satellite communications due to their nature could be used to relay emergency information, avoiding the terrestrial bottlenecks in the event of a disaster. In combination with terrestrial broadcasting facilities they could disseminate information to the public instantly. In addition this type of public warning system offers the possibility not only to announce events, but also to inform and advise the public what to do during and immediately following a disaster.

A typical and robust infrastructure for relaying this type of information to radio, TV and other media organizations with the use of a satellite network consists of a dedicated uplink at the crisis management centre or another central location accessible by the information originating organizations, and receive terminals at all radio, television and other media facilities. The system should be capable of broadcasting, audio, video and graphics.

The primary information originator for Public Warning and Information Dissemination Systems should be the Government agency that has the primary responsibility for overall national security. The crisis management team of the NTC Plan should have access also, in order to relay to the public information associated with the health of the national telecommunications infrastructure and to instruct them as to how to use the telecommunications services to avoid congestion and bottlenecks for the Critical telecommunications Services especially those pertaining to the Emergency Services (e.g. police, fire brigade etc.). Procedures for periodic testing, activating, and using this network needs to be developed in close cooperation with the participating radio, TV and media organizations as well as other participating Government organizations. The system should be capable of National as well as regional broadcasts and announcement. News wire agencies and the Internet should also be connected to this system.

ACTION – PROPOSAL 15:	EETT will play a role in developing a National Warning and Information Dissemination System. EETT could be the owner and keeper of the network or to support the national emergency responsible authority for its implementation and certainly be one of the users of the system during a disaster event.
------------------------------	---

7.2.1.2 Emergency Management System

As part of Public Warning and Information Dissemination System described in this Section a software system will be implemented to provide a full range of emergency management decision support, resource management, and incident documentation functions.

Although specific capabilities will need to be reviewed and determined more accurately, the software system as a minimum will allow the crisis management members to:

- Manage resource databases; and maintain an event record.
- To catalogue the information as described throughout in section 7.
- Originate and track tasks, record entries and plot telecommunications infrastructure disaster effects and complete checklists of required actions.
- Publish information to the WEB site.
- Store reference plans and supporting documents, and communicate both internally and externally among all team members EETT and Telecommunications Carriers.

ACTION – EETT will lead the implementation of the Emergency Management PROPOSAL System as part of the Crisis Management Centre.
16:

7.2.2 EETT

7.2.2.1 Public Awareness

Within the context of preparedness of the NTC Action Plan it is important for the public to be:

- Aware of the existence of a national telecommunications action plan.
- Informed about what they can and cannot do with their telecommunications services in case of an incident (generally) so that they react in an appropriate way.
- Aware of the content and be in a position to understand the information delivered to them during an incident.
- Aware of the kind of information (identity, incident, location, damages etc.) they need to provide to emergency centres when required, in order to avoid long conversations, confusing messages and to reduce the risk of congestions.

Other means that can be used to raise the awareness of the users could be possible placement of announcements in media (newspapers, radio, and television), as well as distribution of booklets and brochures in public places like hospitals, police stations, schools and in other public spots like sport arenas and in the specially established Telecommunications Emergency Action website.

Telecommunications Carriers can contribute to this activity by providing additional information about available Emergency Telecommunication Services and network capabilities that are crucial to users of a service. Special attention should be given to roaming/visiting mobile users or new users who might be familiar with a different way of contacting Emergency Services (i.e. different number in different countries). For instance for roaming mobile users this can be done by sending an SMS with the country

specific emergency numbers upon first handset connection and for new users by providing leaflets/stickers when purchasing a new mobile or fixed-line telephone.

ACTION – In general a public education program will be devised which could be
PROPOSAL instigated by EETT and supported by the Telecommunications Carriers
17:

7.2.2.2 *Web Site*

See Section 7.1.2.3 WEB Site.

7.3 RECOVERY ENVIRONMENTS

7.3.1 Carriers

7.3.1.1 *Systems Enhancements*

As part of an ongoing effort certain enhancements with infrastructure related systems could help optimize the performance of the Critical Telecommunication Services during a disaster condition. The Carriers should consider implementing these enhancements to improve the resiliency of the infrastructure and introduce expediency in the resolution of Crisis Events.

7.3.1.1.1 SMS in Emergency Situations

The use of SMS in emergency situations should be investigated as a tool for the following communication scenarios:

- Communication from authorities to users.
- Communication from users to authorities.
- Communications from Carriers to users.

The first type of communication would typically be a SMS broadcast to a certain area to warn or inform citizens about an incident. This could be used by the Crisis Management Team during an emergency situation to advise users in a stricken geographical area. The second type may be useful when no emergency call is possible. And the third to advise the users as to network related issues during emergency situations.

Some difficulties related to SMS are:

- Store-and forward mechanism; therefore no real-time and bi-directional connection.
- No guaranteed delivery.
- The location information is not always trusted.

Nevertheless:

- SMS may be used when calls are not possible.
- SMS can be used in both ways.
- SMS can be in point-to-point (single user) or broadcast mode.

- SMS can be used in combination with base station support to transmit targeted information.
- SMS requires smaller bandwidth than an equivalent vocal call. This makes SMS suitable when a wider number of subscribers need to be contacted.
- To facilitate the writing of SMSs and for a more efficient handling in emergency situations, standard texts messages may be predefined.

Special routing profiles might be required for emergency SMSs.

In some mobile systems this facility is used to alert subscribers within the coverage of a certain geographical area (a pre-selected number of base stations can be activated to “broadcast an emergency message”). A similar situation can now be foreseen with the extension of the SMS Services to the fixed network (ETSI ES 201 912).

For complex messages, a coordinated information system could well make use of the SMS Service and invite the user for further information in a certain identified broadcasting channel (TV, radio, or web page).

SMS messaging to fixed subscribers should be considered and the additional functionality required and level of complexity should be considered.

SMS emergency texting cannot be considered a priority service. The time to deliver latency of text messages is unreliable and not guaranteed. Nevertheless users can use this type of feature to be informed of the extent of the disaster and what steps to take in addition to other information disseminating mechanisms (radio, TV etc.).

ACTION PROPOSAL 18: – EETT will consider in cooperation with the Telecommunications Operators whether additional functionality is required in their network, establish procedures and communication content for using SMS during emergency situation for fixed and mobile users.

7.3.1.1.2 E112 Service

During emergencies citizens, authorities and emergency response teams have a need for dedicated, high quality communication systems operating at all times.

In the past this area of communications has been developed, provided and organized by the national telecommunications operators and the national safety and security agencies/organizations. In today's deregulated and liberalized telecommunications market, operators of public telephone networks have the obligation to provide this type of communication under their licenses on a European and national basis. Recently the European emergency call number (112) was created. The E112 Service does include the provision of caller location information and it should be a harmonized service incorporating response by the police, fire-fighting, medical response and disaster response agencies.

ACTION PROPOSAL 19: – EETT in cooperation with the Telecommunications Carriers to take the lead in the effort of establishing a ubiquitous E112 Service which brings together all national emergency agencies and includes forwarding caller location information to the emergency responding agencies.

7.3.1.1.3 Location Information to Emergency Organizations

When a user calls an Emergency Service (112, 100, 199, 166, 108,109) **it is important that the caller location information be made available to the responding Emergency Service.** This location information in the form of subscriber name, address, and number could be vital to the welfare of the caller. Primarily this information can be used to direct emergency teams to the user location.

Besides providing important information to guide emergency relief teams as fast as possible to the place of emergency, the location information may also allow for the detection of fraudulent calls.

Geographic numbers and location databases can allow a cross checking with the location given by the calling party. This mechanism may also be helpful in cases where the calling party is not able to name its location, e.g. children, the handicapped and the elderly.

A further property of the emergency system in connection with the location information is the routing of incoming emergency calls to a response unit located nearest to the user of the Emergency Service.

All this functionality is a network matter, it is under study by the ETSI TC TISPAN project EMTEL and it is described in detail in many ETSI documents (see Appendix 1 - Bibliography recommendations for E112 deployment).

ACTION – PROPOSAL 20:	EETT in cooperation with the Telecommunications Carriers and Emergency Response Organizations to evaluate the possible deployment of this functionality for existing emergency numbers (100, 199, 166, 108,109) while awaiting full deployment of the E112 Service.
------------------------------	---

7.3.1.1.4 Satcoms in the Event of Disaster

Satellites have played a key role in disaster relief, Emergency Services and temporary restoration of Critical Services, providing vital links during both natural and man-made disasters especially in cases where terrestrial networks have been disabled as a result of the disaster.

Satellite technologies can play an important role in disaster preparedness by carrying broadcast messages to local radio and television, alerting the population before a disaster strikes and giving clear advice about what action should be taken during and after.

Satellite technologies are used for imaging and sensing as well as communications where terrestrial systems are either not available or become interrupted after volcanic eruptions, earthquakes, landslides, windstorms, floods and forest fires. The European Space Agencies (ESA) REMSAT project (Real Time Emergency Management via Satellite) integrates satellite observations with the use of telecommunications and navigation satellites in a generic system that could be used anywhere in the world to manage the response to any large natural (or manmade) disaster.

In the immediate aftermath of a catastrophic disaster it should not be assumed that any terrestrial telecommunications infrastructure would be available and still in working order. For instance, an earthquake can cause major fiber links to be severed, exchanges collapse, microwave towers can be toppled or the links put out of alignment. Cellular networks would in such a situation suffer similarly. Prudence therefore dictates that it would be very unwise from a planning perspective to rely upon being able to use the normal means of communication in the aftermath of a major disaster.

Satellites have the capability of simultaneously handling multiple telephone calls, transporting data and providing connection to the Internet. They are therefore ideally suited to large-scale operations such as disaster relief. In practice they can form the basis of a communications centre through which many different agencies and other workers can make telephone calls and connect to the Internet to obtain maps and other pertinent information. Internet bandwidth can be provided to a site at any data rate required. Telephone traffic can be routed in and out of the international Public Switched telephone Network (PSTN). Alternatively a private direct data or voice link can be established between the site and the central coordination centre or headquarters or any other entity. Where a direct link is established with the HQ the telephones at the remote site can even be programmed as extensions off the main PABX.

The inherent characteristics of satellite systems make them key in crisis communication networks. They constitute a reliable and “always-on” communications link. In addition, they have the flexibility to adapt to the location and scope of the emergency and crisis situations either by providing a wide global coverage or by concentrating their capacity on localized spots.

A combination of outdoor satellite backbone link to the public telecom network interconnected if necessary back to back locally, to a mobile GSM or Tetra base station could extend the use of existing mobile handsets in indoor and outdoor operations. This could also address one of the major drawback of satellites communications i.e. their inability to operate indoors.

In summary the role of a satellite-based infrastructure is essentially four-fold:

- To allow mobile communications in the emergency area through standard mobile handsets, small transportable or even handheld terminal.
- To provide a means to temporarily restoration of interconnection with the public network(s).
- To integrate seamlessly with terrestrial emergency networks and complement them in terms of coverage, bandwidth, connectivity, redundancy and broadcasting capability.
- To provide a means for real time data collection, transfer and broadcasting through real time data relay services.

ACTION – PROPOSAL 21:	EETT in cooperation with the Telecom Carriers and the responsible Government agencies to consider the possible use of satellite communications as a means of temporarily restoration of: public telecom Critical Services (fixed and mobile), to support dissemination of warning messages and advices to the general public and contributor to improved Emergencies Telecom Services as described in section 7.2 “Media and Carrier Communications”.
-----------------------------	--

7.3.1.1.5 Interim Restoration for National Telecom Infrastructure

The diversified nature of the elements of the telecommunications infrastructure (telephone, data lines, cellular systems, pagers, satellite, cable, wireless broadband, radio and television) means that total failure is virtually inconceivable. What is more likely is that one or two elements (e.g. voice and data lines) could fail but the other elements would be unaffected.

The most critical elements of the traditional telephone network are the switches, catastrophic failure of a switch e.g. due to earthquake or fire, could disable tens of thousands telephone lines and thousands of data lines.

Depending on size and capacity full restoration of a switch could take about one to two weeks or more. In the interim, a transportable switch could be used. Depending on the severity of the incident, a coordinated response would likely invoke Telecom Carrier's mutual aid provisions.

Aside from natural and man-made disasters, the telecommunications facilities are also vulnerable to power failure, though all switches have battery backup. Beyond that, major central offices have generators with fuel to last several days. Even if the telecom infrastructure is in operation, a power failure could affect the today's modern user telecom equipment (modems, telephone cordless etc.).

Businesses and individuals especially in rural and remote areas should be provided with guidelines on the vulnerability of their telecommunication equipment due to power failures.

ACTION – PROPOSAL 22: EETT will work with Telecom Carriers and the Government to consider the use of transportable mobile switching units and other telecom facilities (base stations, satellite equipment, generators, etc.), their storage facilities and to develop procedures for their transportation and operation for interim restoration.

In addition EETT will consider the development of guidelines for the user communities, especially those living and operating in rural and remote areas, on the vulnerability of their telecommunication equipment due to power failures and what measures that they should take to mitigate disruption.

7.3.1.1.6 Internet Services

Internet Services constitute an area of growing significance with respect to critical dependencies. All Critical Industry Sectors, Government on-line service delivery, education, business and personal e-mail services, healthcare delivery systems and an increasing number of business-related on-line services (such as on-line reservation systems) are dependent on the Internet. A serious failure of the Internet at the national or regional level would be highly disruptive to Government and business alike. Even local failure of individual Internet Service Provider (ISP) services would cause wide public inconvenience and business disruption.

Another very important aspect of the Internet is its potential to be used as a conduit for the launch of cyber attacks against any individual or organization that relies on the Internet. This potential extends to attacks on infrastructure elements, particularly large public utilities that use network-based facilities to control of elements of the infrastructure remotely. Care should be taken by Telecommunications Carriers to

prevent malicious access to infrastructure management systems against hacker attacks with proper use of firewall and secure access systems.

In general, because of the robust design and built-in redundancy of routing, the Internet backbones are not vulnerable to major failures of equipment or communications links on individual legs of the network. A major failure in one leg would simply result in re-routing of messages to alternative routes. The greatest risk of hardware and/or communications failure is between the subscriber and his/her ISP (or in the case of large users who interface directly to the Internet, a failure at the user's premises). If an ISP suffers a hardware failure, restoration capability generally depends on the individual ISP, with some being more robust than others (for example in being able to switch quickly to a backup server). If the ISP itself suffers a major failure such as an electricity blackout, fire or other major disaster, restoration could take hours, days or even weeks. In cases of very serious ISP failure, subscribers would be forced to seek alternative ISP services (few subscribers actually have active accounts with more than one ISP.) For users with dial-up Internet access, the communications links between the subscriber and the ISP are as robust as the telephone service and local communications redundancy is built into the service. For users of DSL services, communications failure could result in a prolonged outage and in the event of a failure of the ISP, establishing service with an alternate ISP would be less easy than for a dial-up service user. Given the increased number of users, and the number and variety of distinct ISP services, it is impossible to estimate the likely impact of any particular type of failure. The more Internet users, the more the impact will be noticeable.

However, the most serious Internet vulnerabilities are not those inherent in the equipment or communications facilities: they are the vulnerabilities arising from the Internet Service itself and its users. The issue of viruses, malicious code and denial of service attacks have received wide publicity. Most ISPs and organizations, in addition to many individual users, spend a great deal of money, time and resources implementing layers of protection to try to evade the most serious threats. Unfortunately, the reality is that serious service disruptions caused by malicious code and denial of service attacks continues to be almost daily routine for many Internet users. Meanwhile, the software companies, firewall suppliers and suppliers of filters and scanners struggle to respond to the growing inventiveness of the hackers and cyber criminals. A further point is that the damage resulting from a malicious code or virus attack is not isolated to a discrete part of the infrastructure: it is generally widely spread among many users and can cause serious damage to files and software, sometimes to the point of destruction. Recovery must be established on an individual basis and can take much longer than even fairly serious disruptions caused by network or ISP failure.

Firewalls, virus scanners and filtering devices can detect and often block known malware, provided the filters and virus definitions are up-to-date, but they are seldom able to protect against new forms of attack. Strict computer hygiene measures and enforcement of appropriate use policies can also help reduce vulnerabilities. Ensuring that installed software is properly maintained (including ensuring that current, approved patches are installed and operational) can also reduce the risk of an attack (including a denial of service attack) succeeding. Taking regular backups of important files can assist in the recovery process, should an attack succeed. However, none of these measures can eliminate or even reduce the threat or guarantee that an attack will not succeed. Given the ubiquitous nature of the Internet, the virtually uncontrolled trans-national data flows, the inability of national laws to fully protecting against cyber attacks, it is likely that the

Internet will remain seriously vulnerable and will be a major conduit for attacks on the infrastructure for some years to come.

ACTION – PROPOSAL 23:	As a longer term objective EETT to encourage ISPs to improve the robustness of their services and in consultation with them to consider the development of guidelines to Internet users on ways to protect themselves in case of emergency situations or attacks EETT to encourage and reward Carriers who adhere to good practice of secure and fire walled intranet and operations system remote access.
------------------------------	---

7.3.1.1.7 Priority in emergency situations

The most important attributes of a telecommunications infrastructure, to be in a position to accommodate the tough user demands during a crisis, are availability and reliability. Building a robust infrastructure will not always guarantee that all possibilities for faults are addressed. During disaster conditions it is vital for the general population and the business sectors to ensure access to Critical Emergency Organizations (such as ambulance, hospitals, fire departments, responsible Government authorities and police). This can be achieved with a call priority mechanism incorporated in the telecommunications infrastructure.

Priority of Emergency Services as described in ETSI SR 002 180, is central and according to it all network operators should accord emergency calls priority over all other calls.

Examples on how to implement priority access are the following:

- Use separate communication infrastructure supporting only Emergency Services (prioritised routing).
- “A priori” reservation of channels or bandwidth where connectivity is set up ahead of time and will always be available for Emergency Services.
- "On-the-fly" prioritisation performed by the network utilizing QoS mechanisms to ensure that Emergency Services are supported.

In order to support emergency traffic, in addition to priority treatment, it is important to establish an inter-working and interoperable Emergency Services priority mechanism across all elements of the national telecommunications infrastructure (fixed and mobile), and across the networks of all service providers. This priority mechanism should be available to all national public emergencies numbers such as 112, 100, 199, 166, 108,109, etc.

A fully comprehensive priority system needs to have a richness of capabilities to support a variety of operational requirements for emergency recovery forces. The following is a list (by no means exhaustive) of specific features that could potentially facilitate communications for Disaster Recovery activities:

- Rapid authentication of authorized emergency users.
- Security protection of emergency traffic.
- Preferential access to telecommunications facilities.
- Preferential establishment of emergency communications.
- Preferential routing of emergency traffic.

- Preferential use of remaining operational resources (after a disaster) for emergency traffic.
- Preferential completion of emergency traffic to destination.
- Optional pre-emption of non-emergency traffic (if consistent and compliant with regulatory provisions, this is an area where EETT could assist).
- Allowable degradation of service quality for emergency traffic.

Not all of these features may be possible, practical, or available universally. These features may only be implemented if appropriate laws or policy allow. The above list focuses on the basic capabilities that need to be addressed and developed. These capabilities could greatly facilitate effective and timely recovery operations during emergency events.

ACTION – PROPOSAL 24:	Telecom Carriers to consider steps to gradually fully implement the priority treatment by the wire line and wireless public networks of the emergency telecommunication services.
------------------------------	---

7.3.1.1.8 Priority treatment of other Critical Industries and Sectors

The public telecom networks have evolved to become a common infrastructure to support a wide range of applications, including voice, data, video, and multimedia. This converged infrastructure must, as far as possible, maintain the reliability, quality of service, and security required by modern business especially the Critical Industries, Sectors and Government bodies.

These Sectors utilizing telecommunications services will need to continue to function in the event of a disaster. Priority treatment for telecom services provided to Critical Industries/Sectors and Government bodies over the PSTN (fixed and mobile) could be developed in parallel to the emergency priority services described above and should take advantage of the same infrastructure.

Because natural or man-made disasters could happen anywhere, these Critical Sector entities need to have wide communication coverage in order to fulfil their missions. Their traffic needs to access, traverse, and egress different networks where different technologies are deployed.

High reliability, availability, survivability, and endurance of Critical traffic needs to be implemented in order for Telecommunications Carriers to be able to provide the priority services to the chosen Critical Sectors during an emergency event.

ACTION – PROPOSAL 25:	EETT will take the lead and work with, members of the Critical Sectors and the Carriers, to agree on the levels of these parameters. The long-term objective of this effort could be to overlay to the public telecom networks fixed and mobile a network with special offering to provide the enhanced attributes that Critical Industries/Sectors is requiring. The Carriers at an additional charge for the defined Critical Industries and Sectors should offer this type of premium service. Initiatives to this direction are already in advanced consideration in Canada and the USA for Critical Sector industries including Government bodies. (ANSI Committee T1, T1A1 Working Group) and UK is considering changing the existing arrangements.
------------------------------	---

7.3.1.1.9 Call Duration Control

During disaster events, which impact the national telecommunications infrastructure and during peak demand activity, traffic on the backbone will increase dramatically due to both failures caused by the event and the anticipated significant increase of the demand from different sources including the general public. Possible existing design limitations of the telecommunication networks to carry calls and traffic stretched to their limits due to the event, call for some controlled measures. Such measures could be to limit the duration of calls in order to help the surviving infrastructure satisfy call requests of a larger number of users. These limit triggers could be geographic, link specific, destination/origination specific or any other that could help ease traffic flow and better sharing of resources of a Carrier or between Carriers. Care should be taken that the priority services described in previous sections do not suffer from the control mechanism.

ACTION – PROPOSAL 26:	EETT will take the lead to consider together with the Telecommunications Carriers deployment of call duration control during emergency conditions and agree on the trigger points and chosen control mechanisms. Examples could be to interrupt non priority calls after a predetermined period, totally switch off known abusers for the duration of the incident etc.
------------------------------	---

7.3.1.2 Inter-network operations

Public telecommunications networks consist of multiple non-homogeneous interconnected networks that are based on different technologies (e.g., circuit-switched, wireless, IP, and ATM) and architectures supporting a variety of services. Besides the protection standards for the networks of individual telecom operators described previously, in a competitive multi-Carrier environment it is important to set guidelines to encompass actions (that may be) required by interconnected network operators during emergency conditions associated with disasters that threaten life or property and cause congestion in the public telecommunications networks.

The purpose of guidelines of this nature would be to delineate network traffic management actions that should be performed prior to and during disaster conditions and once agreed should be applicable to all telecommunications network operators that are interconnected and are part of the public telecommunications networks. A coordinated network traffic management response taking into consideration a consistent call prioritization and call duration control mechanism by all affected network operators could enhance the integrity of the public telecommunications networks.

When disaster conditions seriously impact traffic flow through interconnected network elements of interconnected network operators, the need for cooperative network management actions exists. The coordinated network management actions consist of planning, real-time surveillance for detection of disaster conditions, data and situation analysis, control of traffic flow, system restoration and recovery strategies and evaluation of the actions and responses normally undertaken by the Crisis Management function. The objective is to ensure the maximum utilization of the public telecommunications networks under stressful conditions due to traffic overload or network failure. In some cases, the specific types of network management actions needed may be dependent upon the underlying technology, architecture, or service being provided.

It is expected that network interconnections between the various different network types will be based on standardized interconnection interfaces. For example, it is expected that the different network types will interconnect to each other using PSTN interconnection standards; such as SS7 protocols for call control signalling and TDM trunks for bearer interconnection. In the longer term, the different types of networks may interconnect directly using interconnection standards other than the traditional PSTN interconnection. Therefore, inter-working of network management control mechanisms used in the different network types will need to be agreed upon and included within interconnection standards as they are defined.

In practice and depending on the network conditions detected, one or more strategies could be employed during disaster conditions that could help to optimize the integrity of the network while obtaining the maximum use of network capability. Such strategies could aim to inhibit the switching congestion, optimize facilities in terms of enabling maximum number of call attempts, redirect overload traffic to trunk groups with available capacity and to give priority to calls originating from a disaster area.

ACTION – PROPOSAL 27:	Network operators are required to work together to develop emergency guidelines for their interconnected networks. This will be an ongoing effort under the leadership of EETT
------------------------------	--

7.4 REPORTING

7.4.1 Carriers

For the CMT Problem Management see Section 6.2 “CMT Problem Management Report”. For the Service Management Report, see Section 6.1 “Carrier Bi-annual Service Management Reports”.

7.4.2 EETT

Will issue a statement of the lessons learned made publicly available to all Carriers – usually via the biannual Service Management Report’s feedback detailed within 6.1.5 “Communication and Feedback”.

1 APPENDIX 1 - BIBLIOGRAPHY

Relevant reference

International Telecommunications Union (ITU)

ITU-T Recommendation E.106: "Description of an International Emergency Preference Scheme".

ITU-T Recommendation E.115: "Computerized directory assistance".

Draft ITU-T Recommendation F.706: "Service Description for an International Emergency Multimedia Service (IEMS)".

ITU-T Recommendation Y.1541: "Network Performance Objectives for IP-Based Services", 2002.

ITU-T Recommendation E 410: "International network management - General information"

ITU-T Recommendation E 411: "International network management - Operational guidance"

ITU-T Recommendation E 412: "Network management controls"

ITU-T Recommendation E 413: "International network management – Planning"

ITU-T Recommendation E 414: "International network management – Organisation"

ITU-T Recommendation E 415: "International network management guidance for common channel signalling system No. 7"

European Telecommunications Standards Institute (ETSI)

ETSI SR 002 180: "Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling)"

ETSI SR 002 181: "Requirements for communication between authorities/organizations during emergencies"

ETSI SR 002 182: "Requirements for communications from authorities/organizations to the citizens during emergencies".

ETSI SR 002 299: "Emergency communications; Collection European Regulatory Principles".

ETSI SR 002 410: "Requirements for communication between affected citizens during emergencies"

ETSI TS 101 109 (V7.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (3GPP TS 03.32 version 7.2.0 Release 1998)".

ETSI TR 101 300, V2.1.1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues", October 1999.

ETSI TS 102 302: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 5; Emergency Priority Telecommunications Service (EPTS)"

ETSI TS 102 164: "Services and Protocols for Advanced Networks (SPAN); Emergency Location Protocols".

ETSI TS 101 909: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services"

ETSI TR 102 133: "Human Factors (HF); Access to ICT by young people: issues and guidelines".

ETSI EG 202 116: "Human Factors (HF); Guidelines for ICT products and services; Design for All".

ETSI TS 123 271: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Services (LCS); Functional description; Stage 2 (3GPP TS 23.271 version 5.7.0 Release 5)".

ETSI ETR 333: "Human Factors (HF); Text Telephony; Basic user requirements and recommendations".

ETSI ETS 300 488: "Terminal Equipment (TE); Telephony for hearing impaired people; Characteristics of telephone sets that provide additional receiving amplification for the benefit of the hearing impaired".

European Commission

Commission Recommendation of 25th July 2003 C(2003)2657: "Recommendation on the processing of caller location information in electronic communications networks for the purpose of location-enhanced emergency call services", published on O.J.E.U. L 189/49 the 29.7.2003.

European Commission Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive).

European Commission Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

European Commission Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector (Directive on privacy and electronic communications).

European Commission Recommendation 2003/558/EC of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services (notified under document number C(2003) 2657).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector (Directive on privacy and electronic communications).

European Computer Manufacturers Association (ECMA)

ECMA 263: "Private Integrated Services Network (PISN) - Specification, Functional Model and Information Flows - Call Priority Interruption and Call Priority Interruption Protection Supplementary Services"

ECMA 264: “Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Call Priority Interruption and Call Priority Interruption Protection Supplementary Services”

American National Standards Institute (ANSI)

ANSI T1.202-2004: “Guidelines for Network Management of the Public Switched Networks Under Disaster Conditions”

ANSI T1.211-2001: “Representation of National Security Emergency Preparedness - Telecommunications Service Priority”

2 APPENDIX 2 - ACROMYMS

NTC	National Telecommunications Contingency
NTCP	National Telecommunications Contingency Program
CMT	Crisis Management Team
NMS	Network Management Systems
KPI	Key Performance Indicators
EM	Electromagnetic Blast
ITIL	Information Technology Infrastructure Library