



The Lead Government Department and its role – Guidance and Best Practice



Introduction

1. This guidance has been set out to enable Departments to carry out effectively the responsibilities and functions associated with their role as Lead Government Departments. It describes the key processes and disciplines necessary in planning for and responding to crises for which they are either the nominated lead or have key responsibilities to act during the progress of the crisis. It also describes how these processes will be monitored and audited in order to achieve a uniformly high standard of planning and preparation.
2. The guidance consists of 11 chapters. They are:
 - the Core Guidance document itself (Chapters 1–10); and
 - Guidance for Departmental Internal Auditors and Other Reviewers (Chapter 11).

Contents

Item	Page
Summary – Overview and scope	4
LGD response – the three levels	4
The Centre and Assurance	4
Assessment, Planning, Preparation and Validation	5
Conceptual bounds and planning assumptions	6
Chapter 1 – Core responsibilities	7
Chapter 2 – The Centre and Assurance	9
Chapter 3 – The CCS and Assessment	12
Chapter 4 – The CCS Key Capabilities Programme	14
Chapter 5 – The planning process	19
Chapter 6 – Plan content	23
Chapter 7 – Checklist of questions	26
Chapter 8 – Emergency Operations/Co-ordination Centres	29
Chapter 9 – Training and exercising	32
Chapter 10 – Public information and Media	36
Chapter 11 – Guidance for Internal Auditors and Other Reviewers	40

Summary – Overview and scope

1. Most emergencies in the United Kingdom are handled at a local level by the emergency services and by the appropriate local authority or authorities, with no direct involvement by Central Government. However, where the scale or complexity of an incident is such that some degree of Central Government co-ordination or support becomes necessary, a designated Lead Government Department (LGD), or where appropriate, a Devolved Administration department, will be made responsible for the overall management of the Central Government response to the incident.
2. The Home Secretary announced the designated LGDs for different categories of emergency, in answer to a Parliamentary Question on 23 July 2002. Generally, the LGD for a specific set of contingencies is that which has day-to-day policy oversight of the sector(s) of the national infrastructure that may be affected in an emergency. A list of LGDs, together with their responsibilities, is maintained, and updated where appropriate, by the Civil Contingencies Secretariat (CCS) in the Cabinet Office. Where an emergency occurs that does not permit straightforward LGD categorisation, then it will be the responsibility of the Head of the Civil Contingencies Secretariat to make a judgement, and appoint the most appropriate LGD. The LGD lists and responsibilities are also reproduced and updated as necessary on the ukresilience.info website.

LGD response – the three levels

3. There are three broad levels for engagement at Departmental level. They are as follows:
 - **Level 1** – The Lead Department Minister runs the crisis response from their premises using their own emergency facilities as appropriate. CCS advises as and where necessary.
 - **Level 2** – Issue co-ordinated from the Cabinet Office Briefing Rooms (COBR) by the LGD.
 - **Terrorism** always starts at this level with Home Office in the lead, whilst Defence and Overseas Secretariat in the Cabinet Office (ODSec) are responsible for the activation of COBR and, if required, the crisis facilities in 10 Great George Street.
 - **Other emergencies** where the LGD determines that the crisis response may require the deployment of wider government resources. CCS provides support on impact management and recovery issues.
 - **Level 3** – COBR/Civil Contingencies Committee (CCC). PM or nominated Secretary of State leads in the event of a catastrophic incident requiring the involvement of Central Government from the outset to deliver an effective response, or where Emergency Powers are invoked.
4. Guidance on LGD responsibilities, together with arrangements for transition to different levels, is outlined in **Chapter 1**.

The Centre and Assurance

5. LGDs will be required to incorporate assurance on contingency planning within the annual assurance and risk control mechanisms presently being developed within the Central Government corporate governance regime. Senior officials will need assurance that the processes used to develop contingency plans and to determine both the planning process and plan content are adequate and that some level of validation

(testing) has been carried out. Assurances will necessarily be obtained from a variety of sources within the LGD, its stakeholders and other appropriate reviewers. This should be reflected in the Department's **Statement on Internal Control** (SIC) where this is a sufficiently material aspect of the Department's risk and control profile. The Department will therefore need to ensure that it has appropriate review and assurance mechanisms in place. Examples of these are set out in **Chapter 2**, whilst the *Guidance for Internal Auditors and Other Reviewers* is set out in **Chapter 11**.

6. **Engagement** – It is recognised that Departments have a wide range of varying responsibilities, partnerships and levels of engagement with their stakeholders and that this will affect the degree and detail of their planning activity. For example, some Departments' planning activities (such as DTI, DfT and DEFRA) are largely dependent upon the environment, relationships and management structures existing mainly within the private sector. Others (such as ODPM, Home Office and DOH) will have large public sector planning constituencies. This guidance, therefore, **does not set out to be over-prescriptive**, but offers a menu for activity. Departments should use those elements best suited to their particular responsibilities and planning environment.

Assessment, Planning, Preparation and Validation

7. **Assessment** – The two main areas are:
 - **Risk Assessment** – Assessing those risks for which the LGD should be capable of responding. This should be carried out as an iterative process, in co-operation with Departmental stakeholders and the CCS assessments/horizon scanning contacts (see Chapter 3), and encompassing those risks identified in the Resilience Capability Framework (RCF, see Chapter 4) – a strategic management tool for the Capabilities Programme;¹ and
 - **Capability Assessments** – Assessing the current state of preparedness of the component capabilities required by an LGD to fulfil its remit. This process will involve LGDs requesting Readiness Levels (components of the RCF) from relevant Capability Workstream Managers.
8. **Planning** – The main areas for evaluation are:
 - **the planning process** – **Chapter 5**. How plans are conceived and produced; and
 - **plan content** – **Chapters 6 and 7**. The key elements common to all contingency plans, together with a checklist of planning themes and associated questions.
9. **Preparation** – Effective Planning and Crisis Management Teams will require:
 - well-resourced and resilient Emergency Operations/Co-ordination Centres – **Chapter 8**, backed by;
 - good, regular training and motivation – **Chapter 9** outlines the principles and lists where both general and specialist training can be accessed; and
 - a sound public information and media strategy (**Chapter 10**).
10. **Validation** – Effective plan validation is primarily achieved by:
 - **exercises** – **Chapter 9**. Regularly carried out in close co-operation with key stakeholders and other Departments, as appropriate. They must incorporate efficient mechanisms for follow-up, review and incorporation of lessons learned. Lessons may need to be reflected in the Readiness Levels assessed by Workstream Managers; and
 - **benchmarking** against experience (local, national and international) and specialist/scientific knowledge.

¹The RCF is under development at the time of writing; the risk assessment and planning assumptions should be available from May 2004.

Conceptual bounds and planning assumptions

11. The driving concept for this guidance is the integration of an assured standards-based regime for LGD contingency planning with the mechanisms for training and validation necessary to attain the required standard.
12. Departments should look upon this guidance as providing an environment within which they can tailor and validate their plans in association with their particular planning regimes and needs, whilst recognising, however, the importance of a co-ordinated Departmental and cross-Departmental approach to contingency planning.
13. The core strategy is to embed audit, review and validation processes to identify capability gaps and to stimulate cross-Departmental decision-making about the best ways to reduce these gaps. This process should be tightly integrated with the Strategic Capability Management Resilience Capability Framework.

Chapter 1

Core responsibilities

Preparation and planning

1. All Government Departments must maintain a state of readiness. This entails:
 - building up the Department's resilience to shocks and its capacity to lead the response to the emergencies for which it is the nominated Central Government lead. This means planning, training and exercising (alongside those likely to have a stake in potential crises) so that it is able to pick up the reins quickly and effectively. This preparatory work should ensure that the Department is clear about its local, regional and Devolved Administration contacts and the working relationships it wants to have with them in the event of an emergency. It should also identify the other Departments, Devolved Administrations and agencies whose interests will be affected and whose assistance will be needed. On the immediate, practical level, it must also maintain and equip a facility for use as an Emergency Co-ordination Centre, including press/public information facilities;
 - identifying the capabilities that the local responders and those at each level of crisis management can call upon (for example to evacuate large numbers, to treat large numbers of casualties, to access specialist supplies and technical and scientific expertise, to provide accurate and reassuring information) and then building them up so that the Department is in a position to deal with a number of potential scenarios;
 - maintaining press/public information contacts (including the Government Information and Communication Service (GICS)), so that the Department is in a position to effectively co-ordinate the press/public information effort during crisis. This should also include mechanisms for co-ordinating with other interested Government Departments and reporting to Parliament and the public in a timely fashion;
 - planning for and leading negotiations with the Treasury for any necessary additional funds; and
 - keeping aware of the changing set of risks, threats and vulnerabilities which bear upon its fields of responsibility, co-operating with the Civil Contingencies Secretariat (CCS) in the Cabinet Office.

Handling an event

2. **Departments must move into action immediately an emergency arises where Central Government co-ordination is required and where they are designated as having the lead. Normally this will be contained within the Department's own contingency management arrangements. But where the Department identifies a potential or actual civil emergency that poses a major disruptive challenge to the UK, then it will need to:**
 - act as the focal point for communication between Central Government and the multi-agency strategic co-ordinating group(s) on the ground;
 - produce a brief, accurate situation report on the nature and scale of the emergency and submit this promptly – along with the central briefing for media purposes – to their Minister, copied to the Head of CCS who will advise on wider distribution (*of course, the public will already be receiving briefings from the statutory response agencies through the media and other mechanisms, especially where issues of public safety need to be urgently addressed*);

- produce a handling plan as soon as possible. This should offer a clear assessment of whether the emergency is within the scope of the Lead Government Department (LGD), or whether support is needed and, if so, what degree of central co-ordination is required. The decision on this will be for the Head of CCS in close consultation with the LGD, the Head of Crisis Management in Defence and Overseas Secretariat (ODSec), the Security and Intelligence Co-ordinator and No 10;
- draw upon and apply the relevant capabilities applicable to the emergency in hand and, if required, co-ordinate the support needed from other Government Departments and agencies through COBR;
- use its authority decisively to take whatever executive decisions and actions are needed from the centre to handle the emergency or to help the local responders to deal with it;
- act as the focal point for information flows between Central Government and, in most cases, sponsored bodies;
- co-ordinate and disseminate information for the public and the media at the national level, collaborating with other Government Departments, including Cabinet Office/GICS, the News Co-ordination Centre when activated (see Chapter 6) and CCS;
- account to Parliament and lead in the submission of evidence to any subsequent Government-appointed inquiry; and
- learn and share the lessons from the emergency.

Chapter 2

The Centre and Assurance

The requirement

1. Ministers have endorsed the principle that, for the majority of emergencies requiring response at the national level, there will be a pre-nominated Lead Government Department (LGD), which will be responsible for both the planning for and activation of Central Government arrangements. These arrangements could be in support of local, regional or national response. The Home Secretary, together with the Permanent Secretary at the Cabinet Office, in his role as the Security and Intelligence Co-ordinator, wishes to see all Government Departments with lead responsibility for contingency planning working to common guidance and best practice in planning for and responding to emergencies. There is then a requirement for a means of reviewing conformity with guidance for contingency planning.
2. This section outlines the core guidance given in the document *Guidance for Internal Auditors and Other Reviewers* (see Chapter 11) on how those reviews could be undertaken and describes the evidence required to show that the Department is complying with the contingency planning guidance.

Responsibility for Assurance

3. LGDs will be required to incorporate assurance on contingency planning within the annual assurance and risk control mechanisms presently being developed within the Central Government corporate governance regime. A senior official should be designated with responsibility for providing assurance that the process used to develop contingency plans and to determine the plan content is adequate and that some level of validation (testing) has been carried out. Assurances will be obtained from a variety of sources within the LGD, its stakeholders and other appropriate reviewers. In addition, reference to contingency planning should be reflected in the Department's **Statement on Internal Control** where this is a sufficiently material aspect of the Department's risk and control profile. The Department will need to ensure that appropriate review and assurance mechanisms are in place. These could include the following:
 - stewardship reports on conformity with contingency planning guidance and best practice from designated managers within the LGD – each level of management reviews risks and controls for which it is responsible and provides a level of assurance to the senior official responsible for contingency planning within the LGD;
 - internal assurance derived from an assessment of the Department's performance and progress in improving their risk management capabilities, using the **Risk Management Assessment Framework** document which includes contingency planning;
 - specialist internal assurance derived from the results of tests and exercises carried out; post-incident analysis etc. on aspects of the contingency plan;
 - independent internal or external assurance arising from reviews undertaken by specialist groups, e.g. TIDO(R) Exercise Working Party, other review bodies and/or consultants on aspects of contingency planning;
 - independent internal assurance derived from Internal Audit reports where reviews of contingency planning have been undertaken, and from the annual Head of Internal Audit's independent opinion on the adequacy and effectiveness of the Department's system of internal control together with recommendations for improvement.

4. In all cases lessons learned from both successes and failures identified in the various reviews should be promulgated to those in positions able to take appropriate action and to feed appropriate improvements back into the planning process.

The Assurance and review process

5. In providing the assurance, LGDs will need to review conformity against accepted guidance and best practice.
6. The designated senior officer will require:
 - evidence of the adequacy of the risk assessment and of the strategic and contingency planning processes;
 - assurance that the processes and systems of control implemented and operated by line management contain risk to an acceptable level; and
 - assurance that the planning process complies with guidance for contingency planning.
7. The flow diagram (Figure 1 opposite) illustrates the strategic management framework and the planning and validation process. It identifies the component parts of the process and can be used to help reviewers plan the scope of their reviews and determine where to target resources. Reviews could be undertaken at either the strategic or planning level. For example, a review could take its starting point from the risk/capability assessment and work forward through the development and testing of contingency plans, or start with the plan elements and work backwards in order to validate conformity with guidance. Alternatively individual components, e.g. consultation, could be taken and subjected to separate reviews.

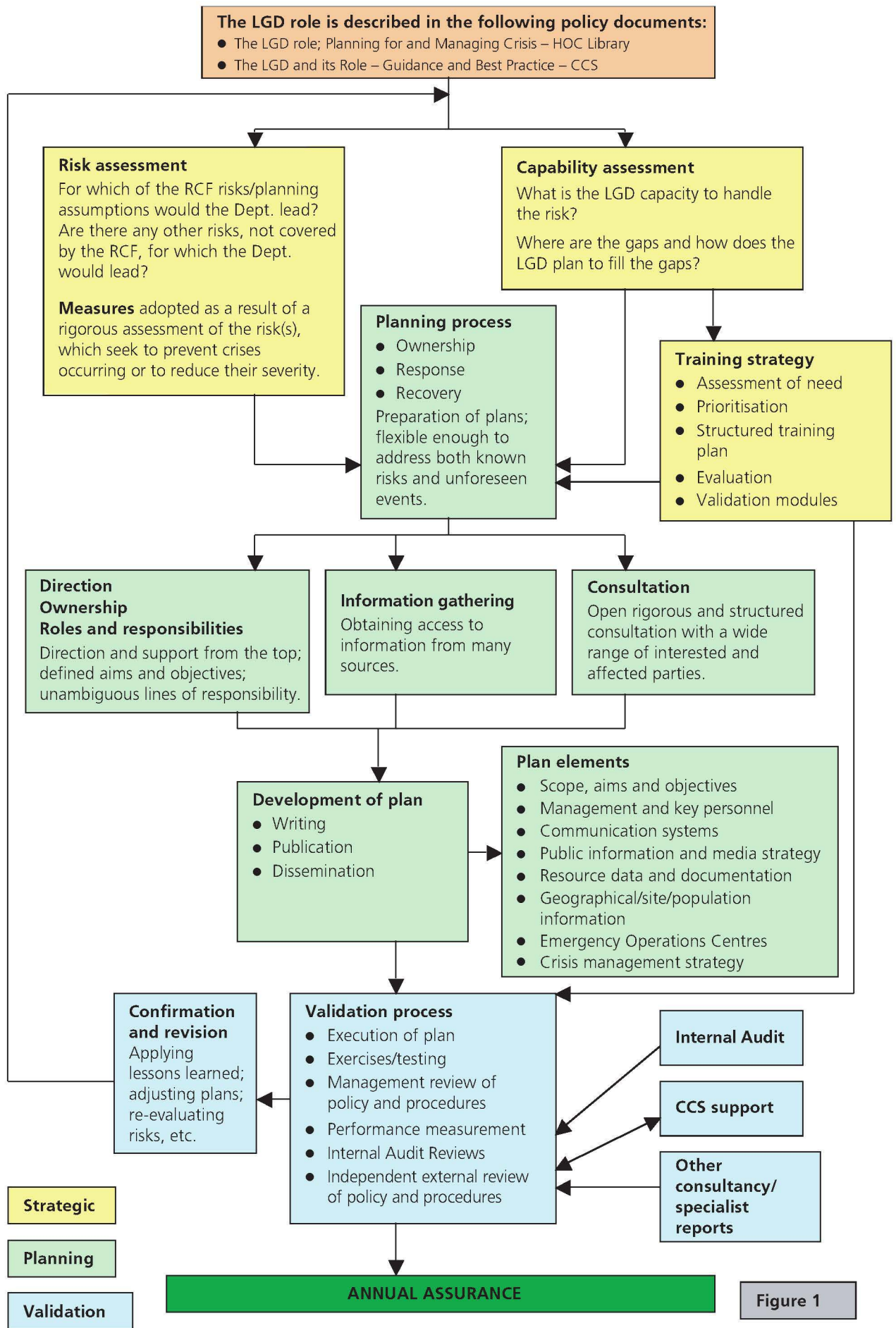


Figure 1

Chapter 3

The Civil Contingencies Secretariat – Assessment

1. The Civil Contingencies Secretariat aims to improve the UK's resilience through working with others on anticipation, assessment, preparation, prevention, response and recovery. We need therefore to be able to skilfully assess circumstances that may precipitate a disruptive challenge and communicate our assessment to decision makers and other key players, assisting in the development of an integrated response. Six specialist desks cover the full range of disruptive challenges, each with its own networks of contacts and up-to-the-minute sources of information. Departments should ensure that they are aware of, and develop close working relationships with, their key contacts on the desks as appropriate. If Departments experience any difficulty in either establishing or maintaining their contacts, then they should make this known to the Head of the CCS Assessment and Commitments Team.
2. The desks cover:
 - **Social stability and continuity of government**
 - **Communications and media**
 - **Economic and financial affairs**
 - **Transport, energy and distribution**
 - **Public and animal health and food safety**
 - **Environment and water.**
3. Departments and other organisations have an interest in spotting risks that could affect their own operations. When they spot something that could potentially develop into a disruptive challenge they should alert CCS. Conversely if CCS picks up signals either directly or from one of its other contacts, it will share and discuss the indications with relevant partners in Government Departments and elsewhere. Together we aim to reach a view of the potential challenge that takes into account all relevant perspectives to prepare an assessment of likelihood, impact and readiness.
4. This has the key benefits of:
 - increasing the chance of averting crisis through prompt action;
 - giving more time to make decisions which may otherwise become uncomfortably tight in a crisis;
 - improving the quality of decision making;
 - generating agreed information as a basis of decision making and minimising confusion and the time lost in a crisis through wrangling about facts; and
 - reducing unstructured and unco-ordinated requests for information in a crisis.
5. Horizon scans will be circulated as issues are identified to senior officials across Whitehall. Written assessments, and updates, will go forward to the cross-government Domestic Horizon Scanning Committee (DHSC) and once approved will be issued to senior government officials and Ministers as an agreed assessment on which to base decisions and planning.
6. The DHSC may commission assessments on specific subjects.

7. **For terrorist incidents, CCS focuses on wider impact management and recovery issues, complementing the predictive work of the Security Service, the police and the Home Office Terrorism and Protection Unit.**
8. During a crisis there is likely to be a need to produce more regular and immediate assessments of how the crisis is developing, again taking into account the information from all relevant partners. These would be produced by a Joint Analysis Cell, run by the Assessments and Commitments Team, in support of activities in COBR, which are designed to deliver an integrated government response.

Chapter 4

Civil Contingencies Secretariat – The Key Capabilities Programme

1. The Key Capabilities Programme is the core framework through which the Government is seeking to build resilience across all parts of the United Kingdom.
2. ‘Capability’ is originally a military term which includes personnel, equipment and training and such matters as plans, doctrine and the concept of operations. ‘Resilience’ is defined as the ability to detect, prevent and if necessary handle disruptive challenges. This includes but is not limited to disruptive challenges arising from the possibility of a terrorist attack. The scope of the programme accordingly extends to the full range of responses and contingencies likely to face the UK in the first decade of the 21st century.
3. The aim of the Key Capabilities Programme is to ensure that a robust infrastructure of response is in place to deal rapidly, effectively and flexibly with the consequences of civil devastation and widespread disaster inflicted as a result of conventional or non-conventional disruptive activity. In the terms of the programme, it is intended that this should be achieved by identifying the capabilities necessary to build UK resilience. The programme also ensures that each of these is developed in accordance with the delivery techniques developed by the Prime Minister’s Delivery Unit (PMDU) under Professor Michael Barber in connection with the Government’s Public Service Agreement (PSA) targets.
4. The programme consists of a total of 17 capability ‘workstreams’. These fall into three groups:
 - three workstreams which are essentially structural, dealing respectively with the central (national), regional and local response capabilities;
 - five which are concerned with the maintenance of essential services (food, water, fuel, transport, health, financial services, etc.);
 - nine functional workstreams, dealing respectively with the assessment of risks and consequences; chemical, biological, radiological and nuclear (CBRN) resilience; infectious diseases – human; infectious diseases – animal and plant; mass casualties; mass fatalities; mass evacuation; site clearance; and warning and informing the public.
5. Each of these workstreams is the responsibility of the appropriate Lead Government Department (LGD). Within each LGD, a workstream leader at Senior Civil Service (SCS) level is responsible for the management of a programme of work set out in a delivery plan agreed with Ministers and with the Civil Contingencies Secretariat (CCS). Within the Cabinet Office, an SCS-level programme director reporting to the Head of CCS is responsible for the management of the programme as a whole, on behalf of the Security and Intelligence Co-ordinator. The programme director holds a monthly meeting of workstream leaders (the programme management team) and provides a monthly report of progress to TIDO(R), the official committee on UK resilience chaired by the Security and Intelligence Co-ordinator. Ministerial oversight of the programme is exercised through the DOP(IT)(R) committee, the Ministerial committee on UK resilience chaired by the Home Secretary, with periodic reports to the Prime Minister.
6. The leaders of the nine functional workstreams have responsibility for developing capability at the national (UK) level. The newly-established Regional Resilience Teams in each of the Government Offices for the Regions are responsible for co-ordinating activity at the local (local authority or police force) level. They are also responsible for communications between workstream leaders at the national level on the one hand

and local authorities and first responders on the other. To this end each of the SCS-level Regional Resilience Directors has been given a lead responsibility on behalf of his or her colleagues for one of the functional workstreams. Responsibilities at the local level will be formalised through the provisions of the proposed Civil Contingencies Bill, and through regulations and guidance to be made or issued should the Bill become law.

7. An important part of the work is to identify the current level of resilience in each of the areas covered by the workstreams. This will enable Ministers to decide what increased level of resilience they wish to achieve in each area, and then to plan and if necessary to allocate additional resources to achieve that increased level of resilience. Testing and exercising will make an important contribution to this assessment. The delivery plan for each workstream explains how resilience is to be tested and exercised, and one component of the central response capability workstream is the development of a cross-Government programme of exercises and training, structured around the Key Capabilities Programme. To this end an Exercise Working Party has been set up, reporting regularly to TIDO(R).
8. The Key Capabilities Programme is intended to cover the whole of the United Kingdom, including Scotland, Wales and Northern Ireland (the Devolved Administrations). Where the content of a particular workstream is devolved, responsibility for that part of the workstream rests with the Devolved Administration.

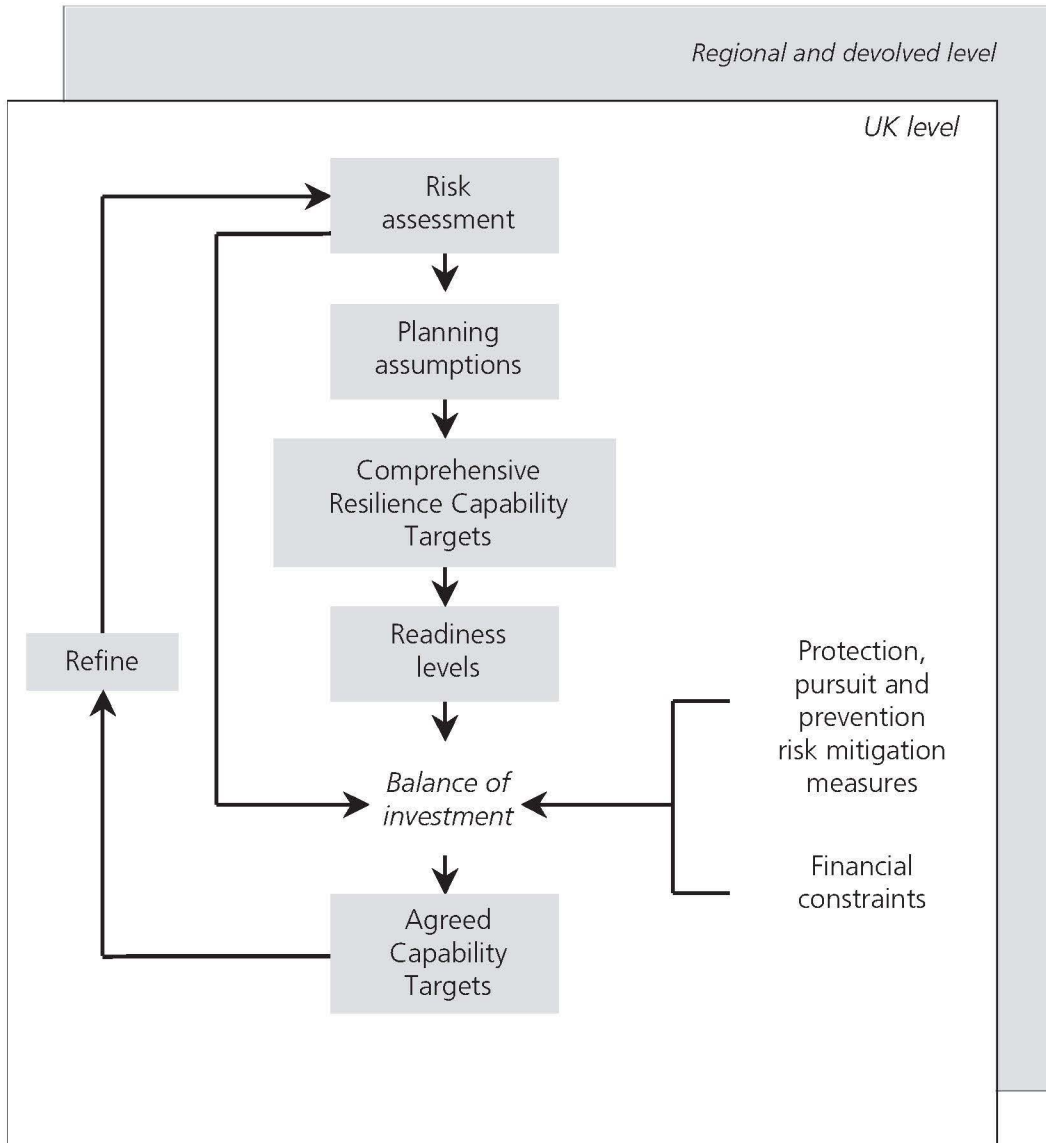
Risk assessment and the Resilience Capability Framework

9. The Key Capabilities Programme aims to promote the resilience of the UK to the full spectrum of risks that we face. However, resources are limited and so it is important that capability development is commensurate with the risks and that available resources are used in the most cost-effective way. To this end, the Key Capabilities Programme will be managed using a framework comprising systematic assessments of the risks, the extent of the capability challenges that they present, and our current ability to respond and recover. The framework will provide a rational basis for the programme's strategic objectives and its management. Consequently, it must:
 - be based on the best available evidence and judgement;
 - allow capability targets to be specified on the basis of assessed risks;
 - facilitate an assessment of existing capability levels and a projection of future capability levels;
 - support balance of investment decisions across the Key Capabilities Programme and also across the four security risk reduction agendas: 'Prevention', 'Protection', 'Pursuit' and 'Preparation' (i.e. resilience);² and
 - facilitate joined-up planning, based on consistent assumptions, across the Key Capabilities Programme.
10. The Resilience Capability Framework (RCF) comprises planning assumptions that capture the assessed risks, capability targets based on the planning assumptions, and assessments of capability readiness levels.³ The process for developing and using the RCF is shown in Figure 2 overleaf.

² This categorisation was recently described by the Intelligence and Security Co-ordinator.

³ More information is provided in *The Resilience Capability Framework: Overview and Approach* (CCS).

Figure 2: Developing and using the Resilience Capability Framework



Detail – The 17 capability workstreams

The three structural workstreams

1. Central Response

Lead Department: Cabinet Office

Aim: to enhance, improve the resilience of and, where necessary, further integrate Central Government’s crisis management arrangements.

2. Regional Response

Lead Department: Office of the Deputy Prime Minister

Aims: to ensure that the current state of resilience in each of the English regions is fully understood; to identify gaps in resilience; and to put work plans in place to ensure that such gaps are filled.

3. **Local Response**

Lead Department: Cabinet Office (but subject to ongoing Departmental negotiations)

Aim: to ensure sound structures are in place to support a local response to emergencies and disruptive challenges, through the Civil Contingencies Bill, together with associated guidance and regulations.

The nine functional workstreams

4. **Chemical, Biological, Radiological and Nuclear (CBRN) Resilience**

Lead Department: Home Office

Aim: to ensure that the country is capable of responding quickly and effectively to deal with and recover from the consequences of incidents involving chemical, biological, radiological or nuclear material, particularly those caused by terrorism.

5. **Site Clearance**

Lead Department: Office of the Deputy Prime Minister

Aim: clearance, removal and disposal of large volumes of rubble and other debris after a catastrophic disaster.

6. **Infectious Diseases – Human**

Lead Department: Department of Health

Aim: to build an effective capability to vaccinate and treat people as part of an emergency response to an infectious disease such as smallpox or a ‘flu epidemic.

7. **Infectious Diseases – Animal and Plant**

Lead Department: Department for Environment, Food and Rural Affairs

Scope to be confirmed.

8. **Mass Casualties**

Lead Department: Department of Health

Aim: to build on the current preparedness and response arrangements already in place for dealing with major incidents and mass casualty incidents through the establishment of appropriate UK doctrine and an associated operational framework for the NHS.

9. **Mass Evacuation**

Lead Department: Home Office

Aim: to ensure UK-wide mass evacuation arrangements are in place in the event of a major disruption following a CBRN or other catastrophic incident.

10. **Assessment of Risks and Consequences**

Lead Department: Cabinet Office

Aim: to enhance the current capability to collect, assess and share across Government information concerning the likelihood and impact of challenges with the potential to disrupt UK life or the operation of UK Government.

11. Warning and Informing the Public

Lead Department: Cabinet Office (Government Information and Communication Service)

Aims: to educate the public about current and new threats without causing panic; to develop mechanisms to alert members of the public to the need to take action, and to ensure that broadcasters can get timely, accurate and authoritative information to the public, in the event of an incident.

12. Dealing with Mass Fatalities

Lead Department: Home Office

Aim: to deal with fatalities resulting from a major or catastrophic incident; to identify the dead, to investigate causes of death and to dispose of the deceased in a safe and decent manner.

The five essential services workstreams**13. Health Services**

Lead Department: Department of Health

Aim: to ensure that plans exist to maintain continued health services in England in the event of a catastrophic incident.

14. Environment

Lead Department: Department for Environment, Food and Rural Affairs

Aim: to ensure that plans exist to maintain continued provision of water supplies, food supplies and flood and coastal defence in England in the event of a catastrophic incident.

15. Transport

Lead Department: Department for Transport

Aim: to ensure that plans exist to maintain continued provision of transport services, including public transport and supply chains and freight haulage capacity in England in the event of a catastrophic incident.

16. Utilities

Lead Department: Department of Trade and Industry

Aim: to ensure that plans exist to maintain continued provision of utilities (e.g. gas, electricity, telecommunications and postal services among others) in England in the event of a catastrophic incident.

17. Financial Services

Lead Department: HM Treasury

Aim: to ensure that plans exist to maintain continued provision of financial services (information clearing house; market information; telecommunications; physical infrastructure; back-up arrangements (private sector); authorities' contingency response) in England in the event of a catastrophic incident.

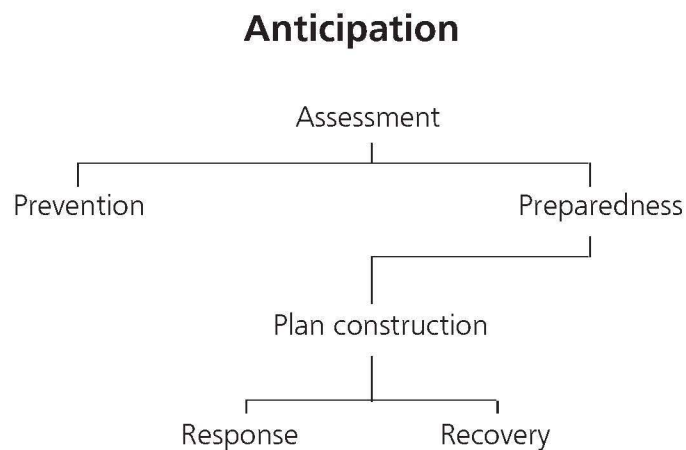
Chapter 5

The planning process

The planning context

1. The true measure of any structure's resilience is its ability to absorb and recover from shock or stress. The length, quality and sustainability of the recovery process are, amongst other inputs, a function of the quality and effectiveness of the contingency planning and management process. It is the skill and commitment that are applied to its response that will, in the end, characterise a Department's success in managing the crises for which it has lead responsibility. Key to this is the understanding of each of the elements, their relationships and interdependencies, as illustrated in Figure 3 below.

Figure 3: Integrated Resilience Management



2. **Anticipation and assessment:** professionally conducted risk assessments encompassing the five-year Resilience Capability Framework Risk Assessment and the shorter-term disruptive challenges assessed by the Civil Contingencies Secretariat horizon scanning team.
3. **Prevention:** measures adopted as a result of a rigorous assessment of the risk or risks, which seek to prevent crises occurring or to reduce their severity. These can include strategies for reduction and/or redistribution of risk.
4. **Preparedness:** preparation of plans that are flexible enough both to address known risks and to provide a starting point for handling unforeseen events. Preparedness includes, for example, the arrangements for identifying and calling out key personnel, together with arrangements for deploying and sustaining key assets, as well as predetermined arrangements for both intra and inter-Departmental augmentation. There needs to be clear ownership of the plans, whilst their effectiveness needs to be tested in regular exercises which feed the lessons learned back to those organisations and individuals to whom they would be of value.

5. **Response:** usually (but not always) the initial response to an incident is provided by the statutory emergency services and, as necessary, by the appropriate local authorities, Government Offices for the Regions, agencies, and possibly voluntary organisations. The Lead Government Department should be prepared to act immediately, for example to provide strategic direction, to assist Ministers in communicating with the public and to handle international aspects.
6. **Recovery:** this phase covers those activities that provide as rapid a recovery as possible, both for the community and for those involved with the response. The Lead Government Department should be fully prepared for this phase, which may well be a long and complex one, involving interface and negotiation with a wide range of other Departments, organisations and agencies. ***This phase can (and in many cases will) involve the handing over of Lead Government Department responsibility from one Department to another. Planning (especially inter-Departmental plans) should ensure that this transition will be as smooth and effective as possible.***
7. There is not one model response to crises. Nevertheless, any response has to be a combined and co-ordinated operation. Prevention strategies will impact on recovery strategies and so on. As illustrated in Figure 3 above, the development and activation of response and recovery strategies should be treated as parallel activities.

The planning process and validation

8. The planning process is best considered under the following headings (Figure 4):
 - Direction
 - Information gathering
 - Plan writing
 - Consultation
 - Publication
 - Training
 - Validation
 - Confirmation or revision.

There should be clear evidence that each of these elements has been properly addressed and that the planning process is a dynamic and continuous one, regularly feeding upon new lessons learned and new information as it emerges.

Figure 4: The planning process



9. **Direction:** the planning process should start with clear direction (and support, e.g. from Permanent Secretaries) to planners at the outset from the top. It is important for Departmental Heads, together with the major stakeholders, to define their aims and objectives clearly, together with straightforward and unambiguous lines of responsibility. They should ensure that those involved in plan preparation are fully aware of the scope of the plans and assets available for deployment on plan activation. Equally, Departments should ensure that strategic guidance is consistent with the resilience planning assumptions that are approved by the Planning Assumptions Group and Ministers.
10. **Information gathering:** the initial stages of investigation and analysis will require access to information from many sources. Key activities should include:
 - identification of risks from specialised, stakeholder or local knowledge;
 - identifying and reviewing overlapping plans and procedures;
 - identification of assets and resource requirements (human and material). These could include, for example, communications directorates, accommodation services, IT services and finance;
 - assessing available human and material resources;
 - identifying relevant legislation and regulations; and
 - identifying and learning from lessons from previous incidents or near misses (at home and overseas).

11. **Plan writing:** plan writers should use the most sophisticated level of document production available. If modern computer-based tools are used from the very beginning, revisions, updates, modifications and cross-referencing tasks can be carried out much more effectively. However, care should be taken with respect to dependence upon IT-based systems in the transmission of plan elements during the actual response to crises. The key elements of plans should be readily available to responders without the need for recourse to long and complicated access procedures that may crash on the day.
12. No plan can be produced in isolation. Contributions will come from many sources. Key stakeholders and other Government Departments should be actively involved in the writing phase as appropriate. Plans should be both internally consistent and compatible with overlapping or related plans and structures.
13. Whatever the level of detail of the plan document, the content of the document should be expressed in such a way as to ensure uniformity of interpretation. Terminology should be internally consistent and so far as possible consistent with commonly used terms in the manuals and plans of other agencies with which the Department must work. Reference to national guidance documents will also help identify core terminology and associated definitions.
14. **Consultation:** has everyone been consulted who needs to be involved? This might include other Government Departments, industry, the utilities, emergency services, local government, regulatory and legal bodies, voluntary agencies, etc. It is at this stage when it will become apparent where plans interlock and overlap across a wide range of contingencies and organisational structures. The consultation and feedback process should be accepted as an essential preliminary validation of how workable a plan is, from both intra- and inter-agency perspectives.
15. **Publication:** once tasks such as final indexing and cross-referencing have been completed, documents should be published and disseminated to all appropriate parties. Placing unnecessary limits on the number and dissemination of copies is in general a false economy. This stage of the planning process should include formal arrangements for channelling feedback and update information to the plan authors. Automatic review dates for both the whole plan and key elements should be built into the planning documents. Documents must, therefore, have strict version control.
16. **Training:** it is of no use having plans in place if people are not properly trained to work within them. Most tasks in an emergency are ones with which staff will already be familiar. However, crisis management does involve some specific skills. These, and how they may be applied, are outlined in Chapter 9, Training civil servants for crisis management.
17. **Validation, confirmation and revision:** the aim of validation is to ensure, as far as possible, that plans are transparent to all those involved in their activation, and that they are:
 - accurate
 - up to date
 - workable
 - user friendly
 - agreed with all partners.
18. **Exercising:** a properly structured, managed and monitored exercise programme is the most effective way of validating the effectiveness of plans. The number, type and complexity of exercises is for Departments, their partners and stakeholders to work through. However, exercises must be a co-operative venture (sometimes between Departments) with real confirmation and learning outcomes, leading to substantive revision and re-thinking where appropriate. It is also essential that lessons learned from critical appraisal of plans in respect of 'near misses', or in debriefs arising from live-incident plan implementation, are incorporated into the validation process.
19. The Exercise Working Party (EWP) has been set up to address the requirements for cross-Departmental co-ordination of planning and exercising. It keeps a careful record of Departmental major exercises and works to ensure close inter-Departmental co-operation and co-ordination. EWP also co-ordinates national exercises up to and including Ministerial participation. The working party reports regularly to DOP(IT)(R) through TIDO(R).

Chapter 6

Plan content

Essential plan elements

1. There is a wide variety of contingency plans and plan types. These include generic, site specific, event specific, single and multi-agency, responding agency and victim agency plans. Each type of plan has its own characteristics and requirements. In the case, however, of the Lead Government Department plan, its emphasis should be on how the Department's input will add value to a crisis response process already being addressed at a number of different levels, locally, regionally, nationally *and possibly internationally*.
2. The roles and responsibilities outlined for Lead Government Departments, and in particular those highlighted as requiring a considerable level of pre-planning, can be summarised in a set of essential elements that will be common to the activities of all Departments that have a defined Lead Government Department responsibility. They are:
 - clearly defined and understood scope, aims and objectives;
 - robust management and key personnel arrangements, including well tried call-out, cascade, triggering and augmentation arrangements;
 - robust, secure and flexible intra/inter-agency communication systems and arrangements;
 - a well defined and regularly practised public information and media strategy;
 - up-to-date and accessible resource data and documentation (both inter-Departmental and stakeholder);
 - accurate and easily accessible geographical, site and population information;
 - one or more designated and well resourced Emergency Operations Centres (EOCs); and
 - a fully integrated crisis management strategy, through from response to recovery.

Detail

3. **Scope:** the boundaries and limits of the plan must be clearly set out, together with key areas of overlap with other agencies, structures and planning environments.
4. **Aims and objectives:** the high-level aim of the plan should be agreed at top management level within the Department and each of its key stakeholders. The aim must then be transmitted fully and unambiguously to planners, together with agreed resourcing. Objectives should support the aim by being **specific, realisable and measurable**. Any auditing mechanism put in place will rely on the supporting objectives being specific enough to be able to measure performance against them. Therefore, the objectives will have to embody quantifiable elements leading to the achievement of the aim.
5. **Management and key personnel arrangements** (including call-out, cascade and augmentation systems): one of the crucial elements in any crisis response and handling system is the speed and effectiveness with which the decision-taking process can be brought to bear. In at least its initial phases, this is dependent upon:
 - a clear understanding by all concerned of roles and responsibilities within the relevant organisational and management framework;
 - clearly defined, well tried and robust structures for call-out, reception, management, augmentation, changeover and support for key personnel throughout the period of the crisis; and

- a clear understanding of the links and relationships between the Departmental crisis management teams and those of their stakeholders and partners.
6. The above elements should be well documented and regularly exercised by all personnel involved, including senior players. There should be firm evidence that the documentation for these links and structures is kept up to date and understood at every level.
7. **Intra- and inter-agency and inter-Departmental communications systems:** to be a viable tool for use in crisis management, communications systems and technologies must display the following characteristics:
- robustness, both in structure and in ability to handle high traffic volumes and peaks. This should include properly organised real-time support for the systems both on site and on call;
 - interoperability – internally; between the Department, its key stakeholders and agencies and between Departments;
 - security – at levels appropriate to the information being handled and the needs of the different partners in the system; and
 - knowledge management – effective filtering and prioritisation of information from data.

Departments should include crisis communications systems and protocols within their overall communications plans, upgrades and modernisation policies.

8. **Public information and media strategy:** ensuring that the public have up-to-date, concise, clear information, including, where necessary, advice on what to do, is crucial to maintaining their confidence. This means having communication strategies and operational plans that are robust, clearly thought through, and fully tested. Communication strategies should be flexible, and should be based on the following:
- identification of all those likely to be affected, both the most immediate and obvious stakeholders, and the less obvious such as minority ethnic communities and other groups, including disabled people, who may be particularly vulnerable;
 - regular issuing of key messages that are up to date, consistent and comprehensive. A single brief that brings together all the necessary information and linking up all those involved is probably the single most important element in crisis communication; and
 - use of the widest possible means of communicating with the public and its constituent parts. The media provide one means, but only one. Websites, call centres, advertising, public meetings and door-to-door calls all have their place and should be structured into plans.

In any major emergency requiring central co-ordination, the News Co-ordination Centre (NCC) of the Government Information and Communication Service (GICS) will support the Lead Government Department. Ensuring that the NCC is factored into a Department's crisis or emergency communications strategies should be integral to its overall crisis management strategy. The nature of the NCC support given will depend on circumstances, but could take the form of staff working in the Department, or in a central operations centre, helping in compiling and distributing briefing material, and designing and establishing websites. It can also include collation of requests for Ministerial interviews and preparing media and public mood assessments. Additionally, the NCC could provide a central press office to co-ordinate the overall Government message. The NCC target is to be operational within 90 minutes of call-out. The NCC manager also alerts the Government News Network (GNN) and other Departmental press offices. GICS can also set up a news co-ordination centre regionally using GNN. **Further detail is contained in Chapter 10.**

9. **Resource data and documentation:** the ability to apply appropriate levels of required resources in a timely manner as and where needed is a key contributor to successful crisis resolution. Departments and key stakeholders should therefore keep well managed and up-to-date resource inventories. These should provide details of:
 - quantities and location(s) of vital material stockholdings;
 - strategies for managing access to those resources and for transporting them to where they are needed;
 - the timescales involved;
 - relevant contracts and agreements;
 - alternative providers and supply chains; and
 - strategies for augmenting and sustaining supplies.

10. **Information management:** efficient systems and protocols for storing, accessing and retrieving required information are vital. While these will vary according to the roles and needs of individual Departments and stakeholders, certain requirements should apply to all:
 - Geographical Information Systems (GIS) and crisis planning – ensure that appropriate use of GIS is part of the planning process within the Department;
 - data sharing and communications networks – maintain good data sharing networks routinely between offices, stakeholders and Departments;
 - information – content and currency – ensure use of the most current data at the appropriate level of detail;
 - data co-ordination – ensure interoperability and compatibility between GIS platforms, especially when high levels of inter-Departmental co-operation are needed in an emergency; and
 - expert advice – Departments should have in place systems to provide expert advice ahead of and during a crisis. These systems should draw on a range of expertise, and be suitably open and transparent.

Chapter 7

Checklist of questions

(Drawn from Guidance for Internal Auditors and Other Reviewers)

The checklist and associated questions below should not be treated either by Departmental managers or auditors as a list to be applied or gone through slavishly for each and every plan or planning environment. For example, some questions are best suited to those plans relating to a Department's relationship with private sector organisations, whilst others apply more readily to central/regional/local government planning environments. They should, therefore, be treated as a *menu*, with judgement applied to the degree or applicability of each question and sub-set.

Additional validation checklists

1. In addition to the essential plan elements, in the process of developing contingency plans Departments should:
 - develop their understanding and expertise of those sectors for which they are responsible, and produce maps for those sectors for which they are responsible;
 - identify and highlight vulnerabilities and interdependencies for their sectors;
 - establish an alert, triggering and warning system, which will identify when and at what levels disruption is likely to cause critical damage;
 - establish agreed response plans with their sectors and partners, which will include the maintenance of business continuity;
 - have an understanding of the legal powers available and of their use in an emergency;
 - understand the limitations and dependencies of any response plan;
 - know the mechanisms for encouraging the sectors to respond to Government requirements; and
 - have a public/media handling strategy relevant to the emergency, together with the resources to implement it.
2. The following sets of questions provide more detail on the above criteria. Internal auditors and others involved in the validation process may find them useful to use as a checklist during reviews of Departmental contingency planning arrangements.

Detail

3. **Developing understanding and expertise of sectors for which Departments are responsible**
 - Is the Department up to date with the market and/or regulatory structures of its sectors, and their impact on emergency management arrangements?
 - Does the Department have mechanisms for taking into account planned or unplanned changes in the regulatory or competitive structures of its sectors which have an impact on management of emergencies?
 - Is the Department up to date with the processes, supply chains, dependencies and resilience of its sector companies and/or organisations?
 - How familiar is the Department with the commercial and/or strategic priorities of its sector organisations?

- Is the Department familiar with the links and interdependencies between its sector organisations and other national/international/commercial structures and administrations?
 - Does the Department have an up-to-date map of its day-to-day links and communication channels with sector and partner (e.g. regulator) organisations?
4. **Identification and highlighting of vulnerabilities for sectors**
- Has a vulnerability analysis for each of the Department's key areas or sectors been completed, how is it maintained and how up to date is it?
 - Does the Department have agreements and systematic liaison on risk assessment and risk management mechanisms between itself and the other players in its plan(s)?
 - Does the Department have active systems in place to identify and track existing, potential or emerging vulnerabilities in other sectors which may impact upon its own sectors?
 - Does the Department have active systems in place to identify and track existing, potential or emerging vulnerabilities in its sectors, which may impact on other Departments' sectors?
5. **Establish an alert and warning system which will identify when and at what levels disruption is likely to cause critical damage**
- Does the Department have an agreed hierarchy, for each of its sectors, of crisis trigger points and mechanisms? Is it regularly tested and updated?
 - Are there agreed actions between the Department and its sectors following notification of a crisis management trigger event, and are they regularly reviewed?
 - Does the Department have inter-Departmental and cross-sector crisis communication mechanisms, such as call-out cascades, etc. in place, and how regularly are they tested?
 - Is the Department fully aware of the mechanisms for and triggering of additional Central Government crisis management procedures, and how often does it practise them?
6. **Establish agreed response plans with sectors which will include the maintenance of business continuity**
- Does the Department have arrangements for systematic liaison with its sectors on emergency planning and response issues and protocols; including appropriate other Government Departments, the Devolved Administrations, local authority bodies, police (e.g. ACPO), industry groups and regulating bodies?
 - Are the arrangements active and have appropriate plans been produced?
 - What systems are in place for regular consultation, exercising and review of emergency response plans?
7. **Have an understanding of the legal powers available and of their use in an emergency**
- Is the Department familiar with national emergency planning and crisis management legislation?
 - Is the Department familiar with specific emergency legislation covering sectors for which it has responsibility and powers that can be invoked under this legislation?
 - Is the Department familiar with police powers covering the deliberate disruption of supplies, delivery routes or systems essential to the effective operation of the Department's sector(s) of the Critical National Infrastructure?
 - Is the Department familiar with the provisions contained in Human Rights, Health and Safety and related legislation in respect of its effect on the powers mentioned above?
 - Is the Department familiar with obligations/limitations applicable under international protocols and legislation to sectors for which the Department has responsibility?
8. **Understand the limitations and dependencies of any response plan**
- What arrangements does the Department have for formal validation procedures to test its plans?
 - What is the level of engagement by senior management in the formulation and tracking of these procedures?
 - Are validating and testing procedures agreed with all stakeholders and sectors with which the Department has a responsibility to plan and liaise? How are these documented and reviewed?

- How frequently are contingency plans and emergency procedures exercised both internally and jointly with key sectors and stakeholders?
- Is the Department capable of sustaining its crisis management structures over a prolonged period of time? What arrangements does the Department have in place to support these structures?
- What arrangements does the Department have in place for an efficient, robust and sustainable crisis operations centre? How is it activated, staffed and resourced?
- Does the Department have formal mechanisms in place for learning and applying lessons from exercises, incidents or near misses, both national and international, affecting the Department, its sectors or related sectors?

9. **Know the mechanisms for encouraging sectors to respond to Government demands**

- Has the Department organised a working strategic group for its sectors?
- Is the dialogue within the strategic group open and frank?
- Is the Department familiar with the obligations/regulatory/commercial imperatives affecting key sector players' ability to respond to Government requests or demands?
- Is the Department familiar with issues such as those of 'commercial-in-confidence' within its sectors?
- Has the Department considered the treatment under competition law of any joint arrangements, if appropriate?

10. **Public/media handling strategy relevant to the emergency**

- Does the Department have a well-developed public information and media strategy for the management of a major emergency or catastrophe, and is it well resourced?
- Are there arrangements in place for activating joint media strategies with other key Departmental, stakeholder and emergency services players?
- Are there arrangements in place to train key managers and staff in the public information and media handling processes peculiar to crises or emergencies?

Chapter 8

Emergency Operations/ Co-ordination Centres

1. A well designed, implemented and managed Emergency Operations Centre (EOC) is vital for the co-ordination of response and recovery processes. Clear operating procedures, staff roles and responsibilities are required, as is an effective workspace supported by appropriate technologies and a safe location. The EOC is not an incident command post; rather, it is the operations centre where co-ordination and management decisions are facilitated.
2. The EOC should provide the following functionality:
 - a dedicated location for the response organisation (including alternative EOC sites and structures);
 - dedicated associated media response facilities;
 - integration of varied forms and channels of information;
 - visualisation and other techniques/technologies to support decision takers;
 - pre-planning for crises;
 - regular training;
 - mobilisation of the organisation;
 - procedures and materials for dealing with crises;
 - robust communications (including a high-specification audio-visual link with COBR where appropriate);
 - regular testing of equipment, and a faults log;
 - recording facilities; and
 - post-incident analysis.
3. **EOC management:** a properly designed EOC should serve as an effective and efficient facility for co-ordinating emergency response efforts. The EOC design must optimise communication and co-ordination by effective information management and presentation.
4. Strong management will be needed during EOC operations. A dedicated EOC manager should be appointed and trained. EOCs should be activated as soon as possible to ensure that rapid decision taking can occur. During the crisis response phase, the real-time tracking of incidents and response resources is critical. Resources will be in short supply, while multiple requests for help and information pile up.

Detail

5. Definition

An EOC is the physical location where key decision makers in an organisation come together during an emergency or crisis to *co-ordinate* response and recovery actions and resources. The EOC is *not* an incident command post; rather, it is the operations centre where co-ordination and management decisions are *facilitated*.

6. EOC functionality

The EOC should provide the following functionality:

- a dedicated location for the response organisation;
- the integration of varied forms and channels of information (multi-mode capability);

- visualisation and other techniques and technologies to support decision takers;
- pre-planning for crises;
- regular training;
- rapid mobilisation of the organisation;
- procedures and materials for dealing with crises;
- robust communications;
- recording facilities, for audit and learning; and
- post-incident analysis.

7. EOC design

A properly designed EOC should serve as a safe, secure, effective and efficient facility for co-ordinating decision making for emergency response. An EOC may serve a number of associated uses including operations, training and meetings. It should be set out so as to fully support this range of uses. The EOC design must optimise communication and co-ordination by effective information *management* and *presentation*.

8. EOC management system (EOCMS)

The EOCMS should provide a *straightforward* structure for conducting crisis operations. It should ideally be applicable to small-scale daily operational activities as well as having the capability to scale up for major operational activities. It should provide operational staff with a standardised operational structure and common terminology. Crucially, it should provide the *flexibility* to rapidly activate and establish an organisational format around the *functions* that need to be performed (i.e. the taking of the best possible decisions to ensure recovery).

9. Event information tracking

Co-ordination of response and recovery processes involves the collation and use of a tremendous amount of information. The EOC must be capable of *collecting* and *managing* this information on a dynamic and sustained basis. Typically, the information flow will look something like this:

- **Incident/crisis occurs/develops**
- **Notification sent to staff**
- **Status evaluated by EOC management**
- **EOC activated, log opened**
- **Standard Operating Procedures (SOPs) implemented using checklists**
- **Tasks assigned according to plan**
- **Resource allocation (tracked in log)**
- **Task performance (tracked in log)**
- **Status briefings and updates to stakeholders.**

10. Information management

All the information will need to be managed and documented, so a strong information management system is a must. The system will have to:

- **above all else – be easy and efficient to use;**
- **collect failure information to allow rapid and early contingency response;**
- **track multiple incidents and resources – to provide a strategic picture;**
- **communicate activities efficiently across the core stakeholder group (and beyond when necessary);**
- **provide good documentation capability – for audit and post-incident review; and**
- **support learning and thus improvement processes.**

Good information management tools can help contingency managers create and organise their plans and processes as well as in exercising and executing them. While contingency plans often end up in binders

and files, a good information management system can make plans and supportive materials easily available to those who need them when they need them.

11. EOC software

This is often a difficult area to address, as the software must be fit for purpose, and not just the nearest ‘fix’. Well engineered, it can make life much easier and decisions better. Ill thought out software solutions can be a problem. The key to getting the right blend is securing an appropriate user specification in the first place, followed by a real partnership between users and development engineers – precisely what the best EOC implementations have achieved. Overall, the software should be able to perform all of the following generic functions:

- **Operate an alert network**
- **Event alert evaluation and triage**
- **Incident logging**
- **Team tasking**
- **Status boards**
- **Executive, press and other briefings**
- **Documentation.**

12. Summary – The ideal information system

Finally then, the ideal EOC is a reliable environment which will be readily signed up to by all of its stakeholders. It will have an easy-to-use and robust information and decision management system that brings together diverse interdisciplinary teams in an efficient and coherent manner, and provides:

- **Central co-ordination and control**
- **Well integrated media/public information facility**
- **Early alert communications**
- **Integrated information presentation and visualisation (e.g. ‘smart’ multimedia whiteboards)**
- **Functionality as a ‘Remote EOC’ (to every desktop in the organisation)**
- **Secure data sharing over the Internet and other networks**
- **Event tracking and logging**
- **Standard Operating Procedures and contingency plan check-off lists**
- **Resource management (including HR)**
- **Documentation of activities.**

Strong management will be needed during EOC operations. However, this should be balanced by an environment and culture that respects, promotes and facilitates creativity and innovation in problem solving. EOCs should be activated as soon as possible to ensure that rapid decision making can occur. During the crisis response phase, the real-time tracking of incidents and response resources is critical. Resources will be in short supply, while multiple requests for help and information pile up. A robust operations log capability is essential to fulfil the requirements of documenting, tracking and managing the response where Departments may be faced with a large number of concurrent incidents.

Chapter 9

Training and exercising

Joint training and exercising

1. Training and exercising must underpin planning and embrace the activities of all staff. The Departmental contingency planning team, or its equivalent, in close co-operation with the TIDO(R) Exercise Working Party, should oversee the multidisciplinary aspects of activities which, although interrelated, are considered in turn in the following paragraphs.

Training and exercising – are they the same?

2. **Training** is about equipping people with relevant knowledge and skills. It should raise general awareness as well as addressing specific skills. It should also recognise the importance of building relationships between people who may need to work together under difficult circumstances. Properly structured joint training is critical for realising the full potential of all the agencies involved. Whether dealing with emergency situations is part of day-to-day work or not, **major emergencies** demand levels of joint working that are exceptional and extend roles beyond the norm.
3. **Exercising** is primarily about testing plans and procedures. It will also help to evaluate the need for further training requirements. While exercises obviously provide valuable experiential learning, they should not be confused with basic training. *Throwing untrained people into an exercise predisposes a plan to failure* and may make it difficult to establish whether the plans and procedures themselves are valid.

Subject areas for joint training

4. **General awareness**
All those who may be involved in responding to a major emergency or crisis, however remotely, should be aware of the management framework within which the response is made. For nominated managers, training will include the more detailed aspects of joint operations.

Training civil servants for crisis management

5. Crisis management is essentially the ability to solve problems by adapting very quickly to a fast changing situation.

Planning the training

6. Exercises are **not** the ideal training environment. Prior training for particular skills or roles must take place in a non-threatening and non-pressurised learning environment. There is then a requirement for the following activities:
 - assessment of training needs, based on a ‘gap’ analysis of what is required to match staff knowledge and skills to the needs of the Department’s crisis management structure;
 - prioritisation of elements of the training agenda. Crises do not wait until governments are ready for them, so certain cross-cutting and inter-Departmental requirements should be identified and prioritised;

- a structured plan for both timing and content of training. This must be flexible so as to dovetail with the other priorities and calls upon officials' time; and
- a careful programme of evaluation and benchmarking of each training segment, and effective assessment of the learning that has taken place.

Skills and attributes

7. Effective crisis management is about effective planning and informed decision taking, followed up by equally effective communication and activation of decisions taken. This requires a number of personal and collective qualities, some of which may be regarded as core management skills, whilst others may be regarded as unique to crisis management. They would include:
 - leadership, including team-working, decision making and assertiveness;
 - issue identification (including prioritisation);
 - systematic information management and dissemination;
 - critical thinking, evaluation and problem-solving;
 - effective deployment and use of available resources;
 - effective communication (including networking and negotiation); and
 - flexibility (including ability to refocus and modify plans).

Sources and types of training

8. In-house training is likely to cater for many of the aspects of the combined response. Other sources are available to complement this and to cover aspects which cannot be dealt with as effectively in house. Some are listed below.
9. **Colleges**

The Cabinet Office Emergency Planning College at Easingwold (EPC), The Hawkhill, Easingwold, York YO61 3EG, website: www.epcollege.gov.uk

Tel: 01347 821406

Fax: 01347 822575

– provides a range of multidisciplinary training in the form of seminars, workshops and courses. It aims to raise awareness of civil protection issues and disseminate good practice and lessons learned. College staff are also available to participate in or conduct off-site events that are tailored to local needs. The college library is also a national centre for the deposit of, and access to, a wide range of literature and other materials on civil protection issues.

The College has tailored a number of courses and events specifically aimed at the needs of Central Government managers and contingency planners. These include events run in situ at the Departments' own facilities, as well as more generic College events. Details can be obtained from the College *Programme Manager*.

EPC has a formal relationship with the *Department of Criminology*, University of Leicester, The Friars, 154 Upper New Walk, Leicester LE1 7QA

Tel: 0116 252 3946

Fax: 0116 252 5788

Email: criminology@le.ac.uk

– contributing to and validating key modules in its MSc Course in Emergency Planning Management.

The Government Centre for Management and Policy Studies (CMPS) at Sunningdale, Larch Avenue, Ascot, Berkshire SL5 0QE

Tel: 01344 634000 or GTN 3803 4000

Fax: 01344 634233 or GTN 3803 4233

Email: customer.services@college-cmps.gsi.gov.uk

– runs a number of courses, including some that equip managers with the range of leadership attributes applicable to effective crisis management.

Centrex (the police staff training college), Bramshill, Hook, Hampshire RG27 0JW, website: www.centrex.police.uk

Tel: 01256 602100

Fax: 01256 602223

– provides a major incident management course primarily for senior police officers, but can advise and facilitate on a range of contingency planning issues that require interface with the police.

Government News Network (GNN) Courses

The Government News Network is willing to assist in mounting training seminars. Experienced staff from GNN offices are available to advise on or participate in events which cover the confrontational issues that can inflame media/official relations. The GNN also run courses in specialist media liaison techniques.

Higher and further education, commercial training organisations

Certain other institutions run specialised courses on crisis management, disaster management and risk management. Other organisations run training activities on topics such as business continuity, risk assessment, media training, etc. Use of a search engine on the Internet will identify relevant organisations' websites. Information on some of these may also be obtained from the Emergency Planning College, Easingwold.

Exercises and exercising

10. Exercising – validating arrangements

The most effective way to validate the effectiveness of plans (other than real events) is to test and review them regularly. Exercises are a key mechanism for achieving this: to assess the arrangements properly and then to update the plans as appropriate in the light of the experience.

Exercises are an important management tool for informing and motivating personnel and giving confidence to those who may be required to respond in a crisis. They bring together those who may be involved with responding to an incident and they allow scrutiny of their responses under controlled conditions. Exercises should therefore reflect reality as far as is practicable. They can establish and reinforce relationships between those taking part, often under stressful conditions. They bring people from different areas together to work as a team, to realise clear goals and to get to know and understand each other's strengths and weaknesses.

Exercises must not be seen in isolation but rather as part of a programme of validating plans and consolidating learning. They should meet their aims and objectives in the most appropriate manner. They need not necessarily be major undertakings in size, duration or involvement, but good exercises, whatever their format, can take a considerable amount of preparation and follow-up assessment.

11. Types of exercise

There are basically three types of exercise, although there are variations on the theme of each of them. The choice of an appropriate exercise is important; it should provide the most cost-effective way of achieving its aim and objectives and take into account the possible disruption of normal work activities. The three main types are discussion-based, table-top and live exercises. Any component part of the resolution of an emergency can be exercised under each heading.

- **Discussion-based exercises**

Discussion-based exercises are generally low-cost activities, which are often a component of a seminar or other training activity. They are designed to inform participants about the organisation and the procedures, which would be used to respond to an incident. Those involved can be either new to the job or established personnel. This type of event will bring staff together in order to raise their awareness of current developments and thinking.

Discussion normally centres on a given scenario or set of circumstances. Participants will explore the scenario, its developing circumstances and its consequences. The emphasis of such an exercise is on identifying problems and finding solutions rather than on decision making. They are usually designed to focus on particular aspects of the response. Problems and findings from the exercise are often shared with a wider audience through panel discussions.

- **Table-top exercises**

Table-top exercises are a form of role-play exercise. They are a very cost-effective and efficient method of testing plans, procedures and people. They provide the few players involved with an excellent opportunity to interact with and understand the roles and responsibilities of the agencies taking part. They can engage players imaginatively and generate high levels of realism.

Participants will get to know the people with whom they have to work in responding to an emergency. Those who have worked together and know each other will provide a much more effective response than those who come together for the first time when an emergency occurs.

- **Live exercises**

Live exercises range from a small-scale single agency test of one component of the response through to a full-scale multi-Departmental/agency test of the whole response to a crisis. Live exercises provide the best means of confirming the satisfactory operation of crisis management strategies. *Exercises also provide the only means for fully testing the crucial arrangements for handling the media.*

12. Exercise control and follow-up

Whatever type of exercise is chosen it is important to record and evaluate the event. Provision of a succinct report of successes and failures to which management can refer is a vital part of the overall learning process. In the event of a crisis or disaster, previous exercise reports can demonstrate the commitment of the organisation to the proper handling of risk and management contingency arrangements.

13. Recovery

Testing recovery plans is especially problematic. Proper account of the timing and complexity of the recovery process is often difficult to achieve within the confines of a typical exercise. One way of overcoming this is to incorporate an in-depth discussion element of this issue into the exercise at the level of the Senior Management Group.

Further information on the use of exercises is available in a Home Office leaflet *Why Exercise your Disaster Response?* and in the publication **Exercise Planners Guide**, both to be found on the ukresilience.info website under the 'publications' link.

14. Other aspects of validation

While exercising is of immense value in helping to validate plans, there are other dimensions to validation. Lessons need to be learned from actual emergencies. A review of arrangements may be appropriate as a result of debriefs, reports, investigations or other feedback mechanisms.

Chapter 10

Central Government public information and Media operating procedures and protocols

Major or significant incidents – standard operating procedures

1. If there is a major incident anywhere in the country – for example, the recent power cuts in London or a rail crash – the Lead Government Department (LGD) has certain responsibilities in leading and co-ordinating the Government’s response. This note seeks to clarify who needs to do what, and when, particularly for local or regional incidents.
2. Some incidents will have such an extensive national impact that the News Co-ordination Centre is set up straight away. There are well known and practised arrangements in place to do this.
3. However, there will be some problems which, even though they have a major impact only locally or regionally, will attract media interest and political pressures on a scale that requires some centralised co-ordination. Our arrangements need to be more robust to handle this scale of event.
4. If the incident happens in London, GICS Ops will immediately set up a small ‘top level’ group of London bodies (emergency services, Association of London Government, ODPM, Regional Co-ordination Unit, the Mayor’s Office and the London Resilience Team). Each of the members will ensure that they co-ordinate their own area of communications with other activities. As soon as it is clear who the LGD is, they will also be involved.
5. Figure 5 on page 39 shows the actions that LGD press offices should take **as soon as they hear of a major incident**. The tip-off may come from anywhere, of course – including the media. If the Duty Press Officer has any doubt about the *bona fides* of the story, they should check as best they can to validate it before starting the cascade procedure.
6. Circumstances will, of course, differ widely from incident to incident and Departments will have to prepare arrangements that ensure that contacts with their partner agencies and organisations and other Government Departments are in place.

Media protocol on public warnings during a catastrophe or major national emergency

Introduction

This protocol has been agreed between the UK Government and principal media organisations. In the event of a catastrophe or major national emergency, the protocol is intended to facilitate effective communication of vital information to the public.

The circumstances in which it is invoked would be truly exceptional and of such magnitude that the national response was being led by Cabinet Ministers, with information being channelled through a special News Co-ordination Centre. The term ‘catastrophe or major national emergency’ may cover:

- events causing, or with the potential to cause, mass casualties;
- terrorist release of chemical, biological, radiological and nuclear (CBRN) material;
- toxic or radiological contamination of a wide area; and
- multiple terrorist attacks.

During a catastrophe or major national emergency, the Government’s overriding aims will be to save life, minimise casualties, limit damage and restore normality. To achieve these aims it will probably be necessary to give the public safety information and advice, tailored to the specific incident, without delay.

People in the immediate vicinity of the incident will receive instructions from the emergency services onsite. Many more, however, are likely to be out of the emergency services’ reach, yet still at risk. Depending on the hazard, it may be necessary to advise people in the affected area either to stay indoors and watch TV or listen to the radio for updated information, or to prepare for evacuation. In most scenarios the Government will be able to provide practical instructions and advice which will help people keep themselves and their families safe.

Other members of the public may need simply to be told that they are not in danger. To avoid obstructing the work of the emergency services, the Government may need to tell these people not to enter the affected area or not to overload the telephone and mobile networks with calls.

The co-operation offered in advance by media signatories to this protocol (who retain complete editorial control) is that during an officially designated catastrophe or major national emergency, they will broadcast and publish without delay the Government’s announcements, instructions and advice to the public.

The Government will use the provisions of this protocol only to disseminate information to the public about the specific hazard faced, safety advice, and instructions or requests which are intended to assist the emergency services in their work.

Signatories

Jon Williams, BBC News

Derval Fitzsimons, ITV News

Simon Bucks, Sky News

Malcolm Douglas, GMTV

John Perkins, IRN

Jonathan Grun, Press Association

Mike Granatt, Government Information & Communication Service (GICS)

Preparation

Each signatory media organisation will nominate an editor and two deputies, who will be familiar with the protocol, and whose full contact details will be kept by Government solely for this purpose.

Every three months the Government Information and Communication Service (GICS) will circulate to these nominated individuals a code word, which would be used to authenticate official communications in the event of a catastrophe or major national emergency. The code word should only ever be relayed verbally – never in print or by email. Each time GICS staff circulate a new code word to a signatory organisation, they will also check that the contact details held for its three nominees are up to date. In the event that a code word becomes known outside this very small group of nominees, the organisation concerned should notify GICS, and a new one will be issued. GICS should also be informed without delay if there are changes to an organisation's list of nominees, or to their contact details.

Activation

The decision that an incident required a government announcement on public safety, and that this protocol should therefore be invoked, would be taken by the Director General of GICS (or post-Phillis review equivalent), in consultation with Ministers.

Activation of the protocol would be notified by telephone to the nominated editor at each media organisation. This call would alert the organisation that a public safety announcement was imminent. It would specify the proposed means (email, fax, etc.) by which the text is to be delivered, and agree with the organisation's nominated contact – who at this point might well not be at work – which email address, fax or phone number would be the most appropriate.

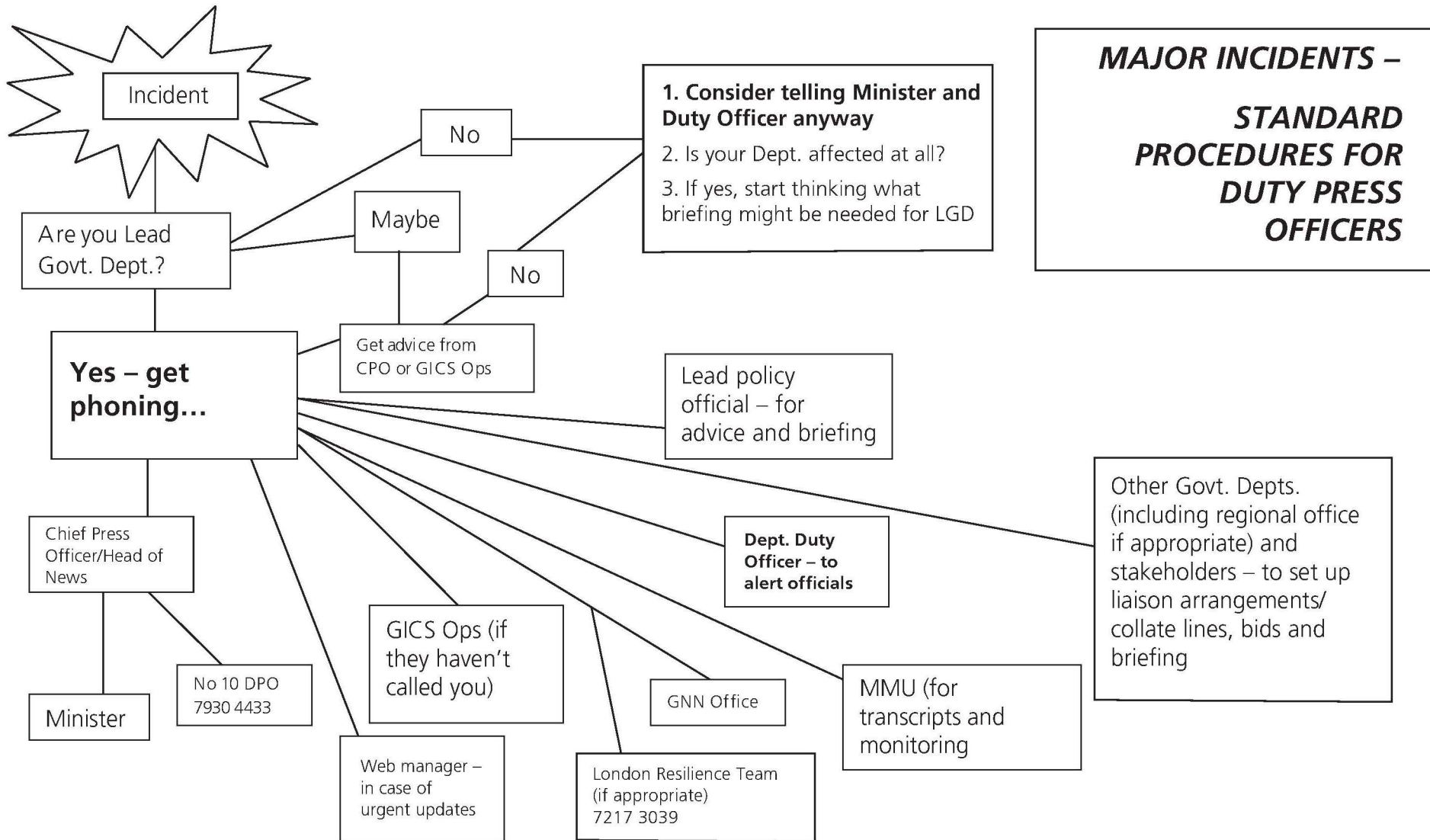
This activation call would also allow an organisation to alert relevant staff to begin preparations immediately – for instance warning the relevant output departments, calling up graphics for TV, alerting newscasters (if not already on air), etc.

Format of announcements

An announcement for public dissemination under this protocol would be sent to media organisations under the heading '**Major Emergency Warning Protocol**', with a sub-heading referring to the actual incident. It will state the date, time, name of the originator and contact details, and will request the organisation to call back for verification. To authenticate the announcement, recipient organisations should call GICS, refer to the communication they have received, and demand the code word. Having satisfied themselves that it is a genuine government message, organisations would then broadcast and/or publish the safety information as rapidly as possible across all available formats (TV, radio, web, teletext), targeting particular regions as appropriate.

Failsafe

To help ensure that this arrangement will function even amid severely disrupted communications, the lead editor at each organisation should inform his/her newsdesk staff of the existence of the protocol. In the unlikely event that GICS is unable to contact any of the organisation's three nominees, it will approach each organisation's newsdesk direct, referring to the protocol. Were such a direct approach necessary, the prevailing circumstances would tend to reinforce the authenticity of the Government's request. In the event of disruption to email and telephone networks, GICS might need to deliver the Government message on paper, by courier.



**MAJOR INCIDENTS –
STANDARD
PROCEDURES FOR
DUTY PRESS
OFFICERS**

Chapter 11

Guidance for Internal Auditors and Other Reviewers

Contents

	Paragraph number
The requirement	1
Responsibility for Assurance	3
The Assurance and review process	5
Sources of Assurance	9
Internal Audit	10
Risk Improvement Managers (RIMs)	14
Management review/specialist groups and consultancy reports	16
Civil Contingencies Secretariat (CCS)	17
The validation process	19
Direction	23
Information gathering	24
Consultation	25
Writing plan documents	27
Publication/dissemination	31
Training	32
Validation	35
Confirmation and revision	38
Annex 1	
Essential plan elements	1
Other validation checklists	2

Reviewing conformity with guidance and best practice for contingency planning by Lead Government Departments

The requirement

1. The Home Secretary has endorsed the principle that, for the majority of emergencies requiring response at the national level, there will be a pre-nominated Lead Government Department (LGD), which will be responsible for both the planning for and activation of Central Government arrangements. These arrangements could be in support of local, regional or national response. The Permanent Secretary at the Cabinet Office, in his role as the Security and Intelligence Co-ordinator, wishes to see all Government Departments with lead responsibility for contingency planning working to common guidance and best practice in planning for and responding to emergencies. There is then a requirement for a means of reviewing conformity with guidance for contingency planning.
2. This chapter gives guidance on how those reviews could be undertaken and describes the evidence required to show that the Department is complying with the contingency planning guidance.

Responsibility for Assurance

3. LGDs will be required to incorporate assurance on contingency planning within the annual assurance and risk control mechanisms presently being developed within the Central Government corporate governance regime. A senior official should be designated with responsibility for providing assurance that the process used to develop contingency plans and to determine the plan content is adequate and that some level of validation (testing) has been carried out. Assurances will be obtained from a variety of sources within the LGD, its stakeholders and other appropriate reviewers. In addition, contingency planning assurance should be reflected in the Department's **Statement on Internal Control** (SIC) where this is a sufficiently material aspect of the Department's risk and control profile. The Department will need to ensure that they have appropriate review and assurance mechanisms in place. These could include the following:
 - stewardship reports on conformity with contingency planning guidance and best practice from designated managers within the LGD – each level of management reviews risks and controls for which it is responsible and provides a level of assurance to the senior official responsible for contingency planning within the LGD;
 - internal assurance derived from an assessment of the Department's performance and progress in improving their risk management capabilities (using the **Risk Management Assessment Framework** document which includes contingency planning);
 - specialist internal assurance derived from the results of tests and exercises carried out; post-incident analysis, etc. on aspects of the contingency plan;
 - independent internal or external assurance arising from reviews undertaken by specialist groups, e.g. CCS/Emergency Planning College Exercise Programme, other review bodies and/or consultants on aspects of contingency planning; and
 - independent internal assurance derived from Internal Audit reports where reviews of contingency planning have been undertaken, and from the annual Head of Internal Audit's independent opinion on the adequacy and effectiveness of the Department's system of internal control together with recommendations for improvement.
4. In all cases lessons learned from both successes and failures identified in the various reviews should be promulgated to those in positions able to take appropriate action and to feed appropriate improvements back into the planning process.

The Assurance and review process

5. In providing the assurance, LGDs will need to review conformity against accepted guidance and best practice.
6. The designated senior officer will require:
 - evidence of the adequacy of the risk assessment and of the strategic and contingency planning processes;
 - assurance that the processes and systems of control implemented and operated by line management contain risk to an acceptable level; and
 - assurance that the planning process complies with guidance for contingency planning.
7. The flow diagram in **Chapter 2, Figure 1** illustrates the strategic management framework and the planning and validation process. It identifies the component parts of the process and can be used to help reviewers plan the scope of their reviews and determine where to target resources. Reviews could be undertaken at either the strategic or planning level; for example a review could take its starting point from the risk/capability assessment and work forward through the development and testing of contingency plans, or start with the plan elements and work backwards in order to validate conformity with guidance. Alternatively individual components, e.g. consultation, could be taken and subjected to separate reviews.
8. The following paragraphs describe how that assurance can be delivered and where resources could be targeted. Internal Audit will form part of that assurance, evaluation and validation process.

Sources of Assurance

9. Assurances can be obtained from a number of different sources both within the Department and from outside. The designated senior officer will need to determine the mix and level of assurances required to reach a decision that the Department conforms to guidance and best practice on contingency planning. That person will also need to determine the extent of the evidence required to support the assurance and the reliance they can place on that evidence in reaching their decision.

INTERNAL ASSURANCES

Internal Audit

10. The Internal Audit strategy (or plan) is based on management's risk priorities. In developing their audit strategy, Heads of Internal Audit (HIAs) evaluate the adequacy of business risk identification and the adequacy of the response to identified risks. HIAs should consider the elements of the organisation's risk analysis, which are regarded as essential for annual review, in order to provide a positive, reasonable assurance to underpin the Statement on Internal Control (SIC). HIAs recognise that contingency planning will be high priority for those Departments concerned (LGDs).
11. Senior management will wish to consult with HIAs about the level of assurance required in order to reach a decision that the Department conforms to contingency planning guidance and best practice. This will determine the level of Internal Audit coverage considered necessary each year and from where else within the organisation, or externally, assurance might be obtained.
12. For their part, Internal Audit could review high-risk elements of contingency plans each year and other elements less frequently. Alternatively, Internal Audit might only look at key plans (i.e. those for continuing the essentials of life) and evaluate them on an annual basis.
13. In addition Internal Audit, as part of their ongoing responsibilities for assurance on the risk management, control and governance arrangements within a Department may also review the adequacy of arrangements used by the designated senior officer to gain their assurance on contingency planning.

Risk Improvement Managers (RIMs)

14. A framework for assessing the standard of risk management in a Department has been developed by the Risk Support Team in HM Treasury. This is offered to Departments as an optional tool to help them collect and assess evidence of their performance and progress in improving their risk management capability. The framework will support the production of the Statement on Internal Control. Part of the framework consists of a number of questions relating to **contingency planning arrangements**. The questions are fairly generic but are intended to be indicative of the range of issues and the extent of the evidence needed to come to a decision in respect of those key questions.
15. RIMs in Departments using this tool, or a similar evaluation tool, will therefore be collecting and assessing evidence in this area, with effect from the 2003/4 Statement on Internal Control (SIC), which could feed into the overall assurance.

Management review/specialist groups and consultancy reports

16. Other elements of assurance could be drawn by senior management from line management reviews of the planning process; the results of tests undertaken on the plan itself; specialist reports; and special exercises undertaken to test out plan activation, response and recovery routines.

EXTERNAL ASSURANCE**Civil Contingencies Secretariat (CCS)**

17. Where an Internal Audit review has been undertaken, a post Internal Audit report should be provided to CCS by Departments, outlining key areas of concern together with proposed action plans whereby CCS could:
 - provide assistance or advice where necessary;
 - monitor progress through some form of exception reporting procedure;
 - follow up any cross-cutting issues identified;
 - take issues of sufficient urgency to appropriate committees/mechanisms; and
 - use the audit reports to provide Departments with systems advice and to take up any general issues such as resource problems with Ministers.
18. Where required, and in agreement with Departments, CCS should also have discretionary access to Internal Audit reports on the contingency planning arrangements.

The validation process

19. Guidance and best practice have been established for contingency planning, providing a framework to benchmark procedures established by managers.
20. A review and evaluation of the adequacy of controls recommended in the guidance can be used to provide the evidence that Departments are conforming to the guidance for contingency planning. Reviews should be conducted using the checklist given in paragraph 21. A further checklist covering the essential elements of a contingency plan and a set of questions designed to evaluate the effectiveness of contingency plans are given in Annex 1. Internal Auditors and others involved in the validation process will find these checklists useful to refer to during the reviews of Departmental contingency planning arrangements.

21. It is recommended that any monitoring and auditing regime should cover the eight areas of the contingency planning process in **Chapter 5** and Figure 4:
- Direction
 - Information gathering
 - Consultation
 - Writing
 - Publication
 - Training
 - Validation
 - Confirmation and revision.
22. There should be clear evidence that each of these elements has been properly addressed and that the planning process is a dynamic and continuous one, regularly feeding upon new lessons learned and new information as it emerges.
- Direction**
23. There should be evidence that clear direction (and support) is being given to planners at the outset from the top. Departmental Heads, together with the major stakeholders, should:
- define their aims and objectives clearly, together with straightforward and unambiguous lines of responsibility; and
 - ensure that those involved in plan preparation are fully aware of the scope of the plans and assets available for deployment on plan activation.



Information gathering

24. The initial stages of investigation and analysis will require access to information from many sources. Key activities should include:
- establishment and maintenance of information management mechanisms between the Department, its partners and stakeholders;
 - identification of risks from specialised, stakeholder or local knowledge;
 - identification and use of expert scientific and other advice;
 - identification and review of overlapping plans and procedures;
 - identification of resource requirements (human and material);
 - assessment of accessibility and quality of available human and material resources;
 - identification of relevant legislation and regulations; and
 - identification and learning of lessons from previous incidents or near misses (home and overseas).

Consultation

25. The consultation element of the process should go through as many cycles as necessary. It will feed back information from all interested parties into the direction and information gathering phases until a plan is sufficiently mature to gain senior management-level approval.
26. It is at this point that it must be ensured that open, rigorous and structured consultation with what may be a wide range of interested and affected parties takes place. Has everyone been consulted who needs to be involved, including other Government Departments, industry, the utilities, emergency services, local government, regulatory and legal bodies, voluntary agencies, etc? There should be clear evidence that this stage in the planning process has been rigorously carried out. The consultation and feedback process should be seen as an essential preliminary validation of how workable a plan is, from both intra- and inter-agency perspectives.

Writing plan documents**Writing and tools**

27. It should be recognised from the outset that future updates and modifications will be necessary. The design of the plan document(s) should be such that these processes will be as easy as possible.
28. From a practical point of view, plan writers should use the most sophisticated level of document production available. If modern computer-based tools are used from the very beginning, revisions, updates, modifications and cross-referencing tasks can be carried out much more effectively.

Stakeholder involvement

29. No plan can be produced in isolation. Contributions will come from many sources, and stakeholders should so far as possible be actively involved in the writing phase. Plans should be both internally consistent and compatible with overlapping or related plans and structures.

Quality, clarity and consistency

30. Whatever the level of detail of the plan document, the content of the document should be expressed in such a way as to ensure uniformity of interpretation. The document should then avoid inconsistency of terminology, excessive use of jargon and abbreviations or ambiguous sentence structure. Whenever it is practicable, terminology should not only be internally consistent, but also in harmony with commonly used terms in the manuals and plans of other agencies with whom the Department must work. Reference should be made to national guidance documents, such as *Dealing With Disaster*, the Government's core guidance to emergency planners, to help identify core terminology and associated definitions.

Publication/dissemination

31. If the plan-writing stage has made use of appropriate tools, the publication and/or dissemination phase should be fairly straightforward. Once tasks such as final indexing and cross-referencing have been completed, documentation should be published and disseminated to all appropriate parties. False economies of limiting the number and dissemination of copies must be avoided. This phase must also include formal arrangements for channelling feedback and update information to the plan authors.

Training

32. It is of no use having plans in place if people are not properly trained to perform in accordance with required procedures. Wherever possible, staff should be called upon to perform in an emergency those tasks with which they are already familiar. Nonetheless, the special circumstances experienced within an emergency incident will require some specific training, which may be anything from filling in a specialised form to handling much greater pressure than normal from the media.
33. One of the constraints of training within a Department is restructuring and remodelling of its administrative structures. In these situations, training must adapt to changing Ministerial and Departmental priorities; as otherwise the learning curve may be compromised by the energy siphoned off in the internal remodelling. Methods must be in evidence that ensure that key knowledge does not leave with the individuals or changing structures. The development of methods to assure retention of memory of knowledge in strategic matters is pivotal to the success of crisis management.
34. Benchmarking can facilitate effective strategic training and crisis preparation by raising awareness of any performance gap. Departmental and central trainers should take advantage of available resources and routes for benchmarking. The crisis management training strategy must also work towards interdisciplinary thinking, encouraging sharing and trans-Departmental thinking.

Validation (including confirmation and revision)

35. Validation is a critical element in the creation and maintenance of viable plans. It is especially important where Lead Government Departments are not only responsible for assuring their own response, but also that of those sectors, agencies and organisations with whom they must work to achieve a satisfactory outcome to crises. There should be clear evidence that a carefully co-ordinated overall validation strategy has been adopted by the Department. The aim of validation is simply to ensure, as far as possible, that plans are:
 - accurate
 - up to date
 - workable
 - user-friendly.

Exercising to validate the plan's effectiveness

36. Although consultation and feedback are essential elements for preliminary validation, once a plan is approved, a properly structured, managed and monitored exercise programme should be instituted in order to ensure the plan's effectiveness is fully validated. The number, type and complexity of exercises will vary. Departments and their stakeholders need to work through this process together.

Near misses and plan activation

37. There should be clear evidence that lessons from critical appraisal of plans in respect of 'near misses', or in debriefs arising from live-incident plan implementation are fully incorporated into the planning and validation processes.

Confirmation and revision

38. In all aspects of exercising and plan activation departments and stakeholders will need to work together in ensuring that these are co-operative ventures with real confirmation and learning outcomes, leading to substantive revision and rethinking where appropriate.

Annex 1

Contingency planning checklists

Essential plan elements

1. The roles and responsibilities outlined for Lead Government Departments (LGDs) can be summarised in a set of essential elements that will be common to the activities of all Departments which have a defined LGD responsibility. Any contingency plan should therefore contain the following elements:
 - scope, aims and objectives (clearly defined and understood);
 - robust management and key personnel arrangements (including well tried call-out/cascade, triggering and augmentation arrangements);
 - robust, secure and flexible intra/inter-agency communication systems and arrangements;
 - a well defined and practised public information and media strategy;
 - up-to-date and accessible resource data and documentation (both inter-Departmental and stakeholder);
 - geographical/site/population information (accurate and easily accessible);
 - designated and well resourced Emergency Operations Centre(s); and
 - a fully integrated crisis management strategy, through from response to recovery.

Other validation checklists

2. In addition to the essential plan elements, in the process of developing contingency plans Departments should:
 - develop their understanding and expertise of those sectors for which they are responsible, and produce maps for those sectors for which they are responsible;
 - identify and highlight vulnerabilities and interdependencies for their sectors;
 - establish an alert, triggering and warning system, which will identify when and at what levels disruption is likely to cause critical damage;
 - establish agreed response plans with their sectors and partners, which will include the maintenance of business continuity;
 - have an understanding of the legal powers available and of their use in an emergency;
 - understand the limitations and dependencies of any response plan;
 - know the mechanisms for encouraging the sectors to respond to Government requirements; and
 - have a public/media handling strategy relevant to the emergency.
3. The following sets of questions provide more detail on the above criteria. Internal auditors and others involved in the validation process may find them useful to use as a checklist during reviews of Departmental contingency planning arrangements.
4. **Developing understanding and expertise of sectors for which Departments are responsible**
 - Is the Department up to date with the market and/or regulatory structures of its sectors, and their impact on emergency management arrangements?
 - Does the Department have mechanisms for taking into account planned or unplanned changes in the regulatory or competitive structures of its sectors which have an impact on management of emergencies?

- Is the Department up to date with the processes, supply chains, dependencies and resilience of its sector companies and/or organisations?
- How familiar is the Department with the commercial and/or strategic priorities of its sector organisations?
- Is the Department familiar with the links and interdependencies between its sector organisations and other national/international/commercial structures and administrations?
- Does the Department have an up-to-date map of its day-to-day links and communication channels with sector and partner (e.g. regulator) organisations?

5. Identification and highlighting of vulnerabilities for sectors

- Has a vulnerability analysis for each of the Department's key areas or sectors been completed, how is it maintained and how up to date is it?
- Does the Department have agreements and systematic liaison on risk assessment and risk management mechanisms between itself and the other players in its plan(s)?
- Does the Department have active systems in place to identify and track existing, potential or emerging vulnerabilities in other sectors which may impact upon its own sectors?
- Does the Department have active systems in place to identify and track existing, potential or emerging vulnerabilities in its sectors, which may impact on other Departments' sectors?

6. Establish an alert and warning system which will identify when and at what levels disruption is likely to cause critical damage

- Does the Department have an agreed hierarchy, for each of its sectors, of crisis trigger points and mechanisms? Is it regularly tested and updated?
- Are there agreed actions between the Department and its sectors following notification of a crisis management trigger event, and are they regularly reviewed?
- Does the Department have inter-Departmental and cross-sector crisis communication mechanisms, such as call-out cascades, etc. in place, and how regularly are they tested?
- Is the Department fully aware of the mechanisms for and triggering of additional Central Government crisis management procedures, and how often does it practise them?

7. Establish agreed response plans with sectors which will include the maintenance of business continuity

- Does the Department have arrangements for systematic liaison with its sectors on emergency planning and response issues and protocols; including appropriate other Government Departments, the Devolved Administrations, local authority bodies, police (e.g. ACPO), industry groups and regulating bodies?
- Are the arrangements active and have appropriate plans been produced?
- What systems are in place for regular consultation, exercising and review of emergency response plans?

8. Have an understanding of the legal powers available and of their use in an emergency

- Is the Department familiar with national emergency planning and crisis management legislation?
- Is the Department familiar with specific emergency legislation covering sectors for which it has responsibility and powers that can be invoked under this legislation?
- Is the Department familiar with police powers covering the deliberate disruption of supplies, delivery routes or systems essential to the effective operation of the Department's sector(s) of the Critical National Infrastructure?
- Is the Department familiar with the provisions contained in Human Rights, Health and Safety and related legislation in respect of its effect on the powers mentioned above?
- Is the Department familiar with obligations/limitations applicable under international protocols and legislation to sectors for which the Department has responsibility?

9. **Understand the limitations and dependencies of any response plan**

- What arrangements does the Department have for formal validation procedures to test its plans?
- What is the level of engagement by senior management in the formulation and tracking of these procedures?
- Are validating and testing procedures agreed with all stakeholders and sectors with which the Department has a responsibility to plan and liaise? How are these documented and reviewed?
- How frequently are contingency plans and emergency procedures exercised both internally and jointly with key sectors and stakeholders?
- Is the Department capable of sustaining its crisis management structures over a prolonged period of time? What arrangements does the Department have in place to support these structures?
- What arrangements does the Department have in place for an efficient, robust and sustainable crisis operations centre? How is it activated, staffed and resourced?
- Does the Department have formal mechanisms in place for learning and applying lessons from exercises, incidents or near misses, both national and international, affecting the Department, its sectors or related sectors?

10. **Know the mechanisms for encouraging the sectors to respond to Government demands**

- Has the Department organised a working strategic group for its sectors?
- Is the dialogue within the strategic group open and frank?
- Is the Department familiar with the obligations/regulatory/commercial imperatives affecting key sector players' ability to respond to Government requests or demands?
- Is the Department familiar with issues such as those of 'commercial-in-confidence' within its sectors?
- Has the Department considered the treatment under competition law of any joint arrangements, if appropriate?

11. **Have a public/media handling strategy relevant to the emergency**

- Does the Department have a well-developed public information and media strategy for management of a Critical National Infrastructure emergency?
- Are there arrangements in place for activating joint media strategies with other key Departmental, stakeholder and emergency services players?
- Are there arrangements in place to train key managers and staff in the public information and media handling processes peculiar to crises or emergencies?

Cabinet Office
Civil Contingencies Secretariat
10 Great George Street
London SW1P 3AE
Tel: 020 7276 0356
Fax: 020 7276 5113

E-mail: ukrwebmaster@cabinet-office.x.gsi.gov.uk

Web address: www.ukresilience.info

Published: March 2004

© Crown copyright 2004

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.

The material used in this publication is constituted from 75% post consumer waste and 25% virgin fibre.

Ref: 261094/0304/D4