DEPARTMENT FOR TRANSPORT

BUSINESS CONTINUITY MANAGEMENT POLICY

Introduction

1. This policy is a key part of the Department for Transport's internal control framework and specifically covers the Department's approach to Business[1] Continuity Management (BCM). This policy applies to all parts of the Department for Transport (DfT) and its Executive Agencies and all of the activities it undertakes. The Department's Non-Departmental Public Bodies (NDPBs) and those treated as NDPBs are to decide what BCM arrangements they need to have in place, using this policy as a guide.

2. DfT's BCM processes are intended to create and maintain a strategic and tactical capability, based on a common approach, to plan for and respond to incidents and disruptions in order to continue and recover DfT activities in an agreed timescale and to an acceptable pre-defined level. BCM is not about how DfT deals with external disruptive events but effective BCM will help ensure that the capability to do so is maintained.

3. In line with Cabinet Office guidance[2], DfT's approach is to align its BCM arrangements with business objectives; British Standard 25999 (BS 25999)[3], the British Standard for BCM and to comply with the four mandatory requirements (see Annex A) in HMG's Security Policy Framework[4] (SPF) that refer to business continuity.

4. BS 25999 defines BCM as a : "Holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." The standard identifies six elements of the BCM lifecycle that together make up an effective BCM system as shown at Annex B. It is not DfT policy to seek third-party accreditation to British Standard 25999 or to mandate that its suppliers are certified to the Standard.

[1] The word "business" is used here in its widest sense and refers to all DfT activities not simply those with a commercial dimension.
[2] Alignment with BS 259999 Guidance for Government Departments dated November 2009.
[3] 2 BS 25999 is in two parts - BS 25999-1:2006: Code of Practice and BS 25999-2:2007: Specification.
[4] HMG's Security Policy Framework Version 6.0 dated May 2011.

Statement of Intent by the DfT Board

5. The DfT is committed to maintaining the safety and security of all of its staff, visitors, information, buildings and other assets from serious disruption and to continued delivery of key services to the public and other stakeholders. Preparedness and resilience have a vital role to play in the overall success of the Department. An absence of appropriate business continuity arrangements would represent a significant corporate risk and would undermine stakeholders' confidence in the Department's ability to fulfil its obligations. The DfT Board is therefore committed to effective BCM and will ensure that DfT's BCM arrangements are appropriately resourced, supported, and reviewed on a regular basis. The Board expects all organisations across DfT to reach at least Tier 3 level of BCM maturity as described in Annex C by 1 July 2012. In order to achieve this the Board requires the cooperation of staff at all levels, and particularly those with particular responsibilities for BCM, to comply with this policy.

Departmental Vision and Priorities

6. DfT's vision, high level priorities and key responsibilities are contained in the Department's Business Plan 2011-2015 available on the Number 10 website here.

7. The DfT's time-critical priority[5] activities, listed in priority order, are at Annex D. Business units must take account of their contribution to delivering them when they scope their BC arrangements.

DfT Business Continuity Management Structure and Responsibilities

8. The Table at Annex E summarises BCM roles and responsibilities across DfT.

DfT(c) and Agency BCM Policies

9. Because of the diverse nature of DfT, each executive Agency Chief Executive must set out how their area is to undertake BCM in a top level policy/strategy document taking account of this policy. Such policies should be reviewed, updated and re-issued regularly. A top level policy for DfT(c), including the Shared Service Centre[6], (SSC) will be prepared on behalf of and with the involvement of the DfT Executive Committee (ExCo) by the Departmental Security Continuity and Vetting Team (DSCVT). Top level polices should take account of internal (DfT) interdependencies e.g. dependencies on the SSC and the SSC on its customers, priorities and appetite for risk.

[5] These priorities will always be subject to review against wider priorities for Government in the event of major cross-departmental disruption.
[6] The policy will take account of the possibility that the SSC's might be sold to the private sector with the new owner taking over in late 2012.

Incident Management, Emergency Management and Counter-Terrorist Plans

10. BCM encompasses the early phases of disruptive incidents. Such events need to be catered for by up to date incident management plans, or emergency management plans and procedures and Counter-Terrorist plans. A key part of such plans is clarity over when and how, if necessary, business continuity plans (see below) are invoked. Full guidance on all aspects of BCM is available on Transnet.

Business Continuity Plans

11. Business Continuity Plans (BCPs) provide a structured framework for recovery and continuity. A suggested format for a BCP is on Transnet. BCPs must be prepared:

a. by all Directorates/business units.

b. at site level, taking account of the requirements of all activities undertaken at the site[7].

12. All DfT staff, contractors and consultants must be briefed on their role should BCPs affecting them be invoked.

13. All DfT(c) BCPs, sanitised by deleting sensitive and protectively marked information if necessary, are to be published on Transnet. Executive Agencies are similarly required to make their BCPs available to all their staff electronically.

14. If a BCP is invoked, DSCVT's BC, Personnel and Physical Security Manager (telephone: 0207 944 3374) must be informed as soon as possible. Once the situation has returned to normal, a Post Invocation Report (PIR) is to be forwarded to DSCVT's BC, Personnel and Physical Security Manager. The format for a PIR is on Transnet.

15. All BCPs are to be reviewed and re-published at least once a year.

16. All BCPs are to be tested and exercised at least once a year on an incremental basis, each test/exercise becoming increasingly realistic. Guidance on how to test and exercise BC plans is available on Transnet. Copies of post test/exercise reports (PTXR) are to be sent to DSCVT. The format for PTXRs is on Transnet.

[7] A "site" is either a physical building, a number of buildings which may or may not be in close proximity or a part of a building which is occupied, owned or leased by the Department.

Suppliers and Delivery Partners

17. It is not DfT policy to mandate that suppliers and delivery partners must have sound business continuity plans in place or be certified to BS 25999, but business units must take all reasonable steps (which they are responsible for deciding the extent of) to encourage key suppliers and delivery partners to ensure they can cope with disruptions without detriment to their performance for DfT.

Funding

18. Other than staff costs, and a small budget managed by DSCVT, no specific funding has been allocated for BCM. If specific funding is required, a business case will need to be submitted to the relevant budget manager.

Re-Organisation and Change

19. From the outset, consideration must be given to the BC implications stemming from any proposed re-organisation or major change.

Guidance, Training and Awareness

20. This policy is supplemented by the BCM guidance available on Transnet. The guidance is maintained by DSCVT and is updated as necessary. DSCVT will also produce instructions, updates and guidance from time to time.

21. All staff are required to undertake appropriate BCM awareness training at least once. This will take the form of a series of PowerPoint slides accessible via Transnet and on disc. Staff with specific responsibility for BCM should receive appropriate, needs-based, training.

Strategic Direction, Reviews, Monitoring, Audit and Reporting

22. The DfT Executive Committee (ExCo) and the DfT Board will discuss BCM on an annual basis as part of its “In-Depth” review process of risks across the Department and provide strategic direction as necessary.

23. DfT’s performance on BCM will be reported by the Permanent Secretary in the Statement of Internal Control and in the annual Security Risk Management Overview report to the Cabinet Office.

24. DGs and Agency CEs are required to confirm that they have in place an up-to-date Business Continuity Plan which follows the Department’s guidance and where appropriate, emergency plans, in their six-monthly assurance returns (which is one of a small number of Key Performance Indicators DSCVT use to track BCM maturity).

25. DfT(c) and Executive Agency internal auditors will assess the state of BCM in DfT on a risk based basis.

Equality Impact Assessment

26. This policy was reviewed taking account of the Department's guidance on Equality Impact Assessments. It was concluded it has no bearing on equality groups.

Approval and Review

27. This policy was approved by the DfT Board on 14 October 2011. It will be reviewed and approved at least annually by ExCo.

Implementation Date

28. This policy takes effect on 1 November 2011.

Questions and Comments

29. Any questions or comments about this policy should be addressed to DSCVT's BC, Physical and Personnel Security Manager.

14 October 2011

Annex:

A. Business Continuity Management – Extracts From HMG's Security Policy Framework.
B. The Business Continuity Management Lifecycle.
C. Department for Transport - BCM Maturity Model.
D. Department for Transport - Time-Critical Priority Activities.
E. Business Continuity Management Responsibilities.

Annex A

BUSINESS CONTINUITY MANAGEMENT – EXTRACTS FROM HMG's SECURITY POLICY FRAMEWORK[8] (SPF)

SPF Mandatory Requirement (MR)	Mandatory Requirement
MR 49	Departments and Agencies must ensure that all locations where information and system assets (including cryptographic items) are kept must have appropriate Business Continuity and Disaster Recovery[9] Plans.
MR 67	All Government establishments that are assessed to be a HIGH or MEDIUM risk from terrorist attack must have a Counter-Terrorist contingency plan in place. This must seek to deter or minimise impact of an attack or hostile interest and must include: a) Details of all protective security measures (including physical, personnel, information) to be implemented following an increase, or decrease, in the Government Response Level. b) Instructions on how to respond to a specific threat, event or item (e.g. telephone bomb threat, a suspicious package or delivery, Vehicle Borne Improvised Explosive Device (VBIED), hostile reconnaissance or hostile individuals). c) A search plan. d) Evacuations plans, including details on securing premises in the event of full evacuation. e) Business continuity plans. f) A communications and media strategy, including handling enquiries from concerned family and friends. g) Liaison with emergency services and any multi-agency contingency plans. Government establishments that are assessed to be at LOW threat from terrorist attack must ensure that these requirements are incorporated into general business continuity plans (see MR 70)

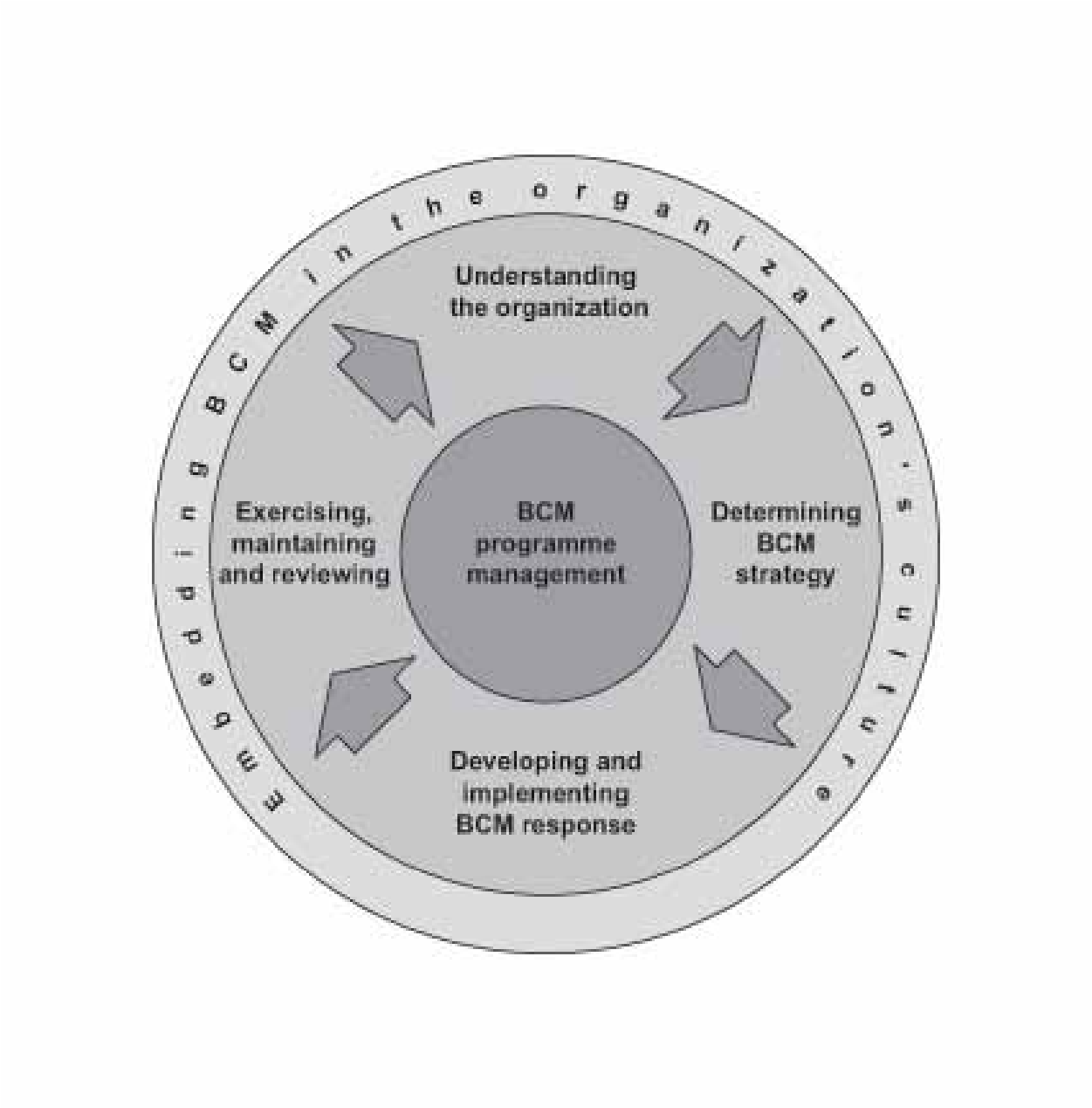
[8] Version 6.0 dated May 2011.

[9] "Disaster Recovery" (DR) is a term sometimes used in the context of planning the recovery of IT systems. A DR Plan is effectively a specialist BC plan.

SPF Mandatory Requirement (MR)	Mandatory Requirement
MR68	As part of Business Continuity and emergency response plans, Departments and Agencies must test their Counter-Terrorist contingency plans regularly to ensure that plans are effective and that any potential problems are identifies and remedied. Minimum requirements are: a) HIGH risk - at least annually b) MODERATE risk – at least once every two years c) LOW risk – at the least every 3-5 years or part of broader business continuity and emergency evacuation tests.
MR70	Departments and Agencies must have robust, up to date, fit for purpose and flexible business continuity management arrangements that are supported by competent staff that allow them to maintain, or as soon as possible resume provision of, key products and services in the event of disruption. These arrangements must follow industry best practice (BS25999 or equivalent standard) and Departments and Agencies must be able to clearly evidence alignment to this level. BCM arrangements must be tested and reviewed at least annually or following significant organisational change.

Annex B

THE BUSINESS CONTINUITY MANAGEMENT LIFECYCLE



Extract from BS 25999-1:2006[10].

[10] Permission to reproduce extracts from BS25999 is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001, Email: cservices@bsigroup.com.

Annex C

DEPARTMENT FOR TRANSPORT – BUSINESS CONTINUITY MANAGEMENT MATURITY MODEL

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Governance	Ownership of business continuity not clearly defined Basic BCM policy exists	Ownership of BCM is defined at business unit level only Limited Executive involvement Policy defines role & responsibilities	Governance programme and operating model established Executive involvement Agreed budget	Model meets external standards and regulations BCM steering committee represented across the business	Validated by external experts Transparent reporting with clear metrics BCM is part of internal audit programme
Business Alignment	Some BCM arrangements established but in isolation from core business	Basic scenario-based risk assessment BIAs have been performed in some parts of business	Formal BIA process in place across business Gap/remediation programme implemented Critical suppliers identified	Critical suppliers engaged in BCM programme Alternate suppliers identified Pro-active business integration	BCM is used by Executive and is integral to business strategy Change management process ensures continued alignment
Strategy and Plans	Basic IT Recovery/Continuity plans established	BCM plans exist and are aligned with IT Recovery/Continuity plans Plans form part of a broader over-arching strategy	Key scenarios integrated into planning Business-focused IT Recovery/Continuity plans Clear escalation process and responsibilities	End-to-end Crisis Management established including incident Mgmt, BCM, and communications plans and strategies	Sophisticated 'Live' planning, maintenance and monitoring software implemented and supported across the business The strategy is designed to enhance enterprise resilience
Capabilities and Testing	No proven capability Limited testing performed Business not engaged	Uncoordinated testing and exercising in some areas of the business IT / Work Area Recovery testing completed in isolation	BCM tests/exercises across multiple business areas at least annually in each area IT testing linked to business objectives	Recovery solution with confirmed availability and implementation timescales Live testing performed and reviewed post-test	IT Recovery/Continuity solution meets business requirements Fully tested & exercised capability Captures lessons learned from tests/incidents
People and Skills	Awareness of BCM limited to those involved Core BCM team not established Only basic training delivered	Little external expertise involved Basic awareness of BCM across some parts of business Limited team development	Core BCM team undertake some exercising Broad awareness of BCM Crisis training given to central functions	BCM roll-out programme completed and included in induction process Deputies and succession planning identified	Regular communication with mature BCM community led by Executive Advanced team-building

Annex D

DEPARTMENT FOR TRANSPORT – TIME-CRITICAL PRIORITY ACTIVITIES

1. The Department for Transport's time-critical priority[11] activities, listed in priority order, are shown in the Table below. Business units must take account of their contribution to delivering them when they scope their BC arrangements.

Serial Number	Time-Critical Activity	Business Unit/(s)Agency Responsible
1	Handling issues relating to the Department's responsibilities where failure to respond in a timely fashion would put public or staff security, health or safety at risk.	All
2	Responding to transport emergencies which includes undertaking the Lead Government Department role[12] following disruption that affects transport.	Transport Security Strategy, DG IS&E
3	Delivering services to the public and other customers.	All
4	Maintaining strategic communications with DfT staff and the media.	Press Office, DG Corporate External Communications, DG Corporate
5	Maintaining strategic communications with DfT customers.	All
6	Provision of IT and telephony services to DfT customers and staff.	IT Services, DG Corporate
7	Meeting Statutory and Regulatory obligations, depending on their nature (e.g. a case falling within Section 1 of the Civil Contingencies Act may take priority).	All

[11] These priorities will always be subject to review against wider priorities for Government in the event of major cross-departmental disruption.
[12] See http://www.cabinetoffice.gov.uk/resource-library/list-lead-government-departments-responsibilities

Serial Number	Time-Critical Activity	Business Unit/(s)Agency Responsible
8	Supporting Ministers and the Permanent Secretary in their decision-making capacity.	All
9	Management of security in all transport modes.	Transport Security Compliance, DG IS&E Transport Security Strategy, DG IS&E Aviation, DG IS&E Maritime & Land, DG IS&E
10	Safeguarding physical and information assets.	All
11	Dealing with Parliamentary business, particularly where there are time-critical issues, such as Bills nearing Royal Assent.	All
12	Financial management, particularly the payment of outstanding grants or invoices where delay would cause difficulties to the recipients or reputational risk; payments to suppliers and staff.	Group Finance, DG Corporate Shared Service Centre, DG Corporate DG Domestic
13	Transport ownership and sponsorship responsibilities.	DG Corporate
14	Management of accident and investigation in all transport modes.	Air Accident Investigation Branch, DG IS&E Marine Accident Investigation Branch, DG IS&E Rail Accident Investigation Branch, DG IS&E
15	Submitting time-limited responses to the European Parliament or Commission.	General Counsel, Non-Group
16	Award of compliant, deliverable, affordable, value for money contracts ensuring that the Accounting Officer does not have any successful procurement related legal challenges	Corporate Procurement, DG Corporate
17	Facilites Management	Property, DG Corporate

Annex E

BUSINESS CONTINUITY MANAGEMENT RESPONSIBILITIES

Group/Post	BCM Roles and Responsibilities
All staff	a. To be familiar with the incident management plan(s), emergency plan(s) and BC plan(s) that cover their business unit and site and to respond as required when plans are invoked. b. To complete DfT BCM training at least once.
Department for Transport Board	a. Own and be responsible for DfT BCM policy and strategy b. Undertake regular "in-depth" BCM reviews.
DfT Executive Committee	a. Provide DfT-wide strategic direction on BCM.
Permanent Secretary	As Principal Accounting Officer, responsible for maintaining a sound system of internal control that supports the achievement of the Department's objectives which includes ensuring risks are identified, evaluated and managed in a cost-effective way.
General Counsel	a. DfT Business Continuity Champion. b. Provide advice to the DfT Board and Permanent Secretary on BCM. c. BCM policy owner. d. Senior Information Risk Officer. e. Management of the Departmental Security Continuity Vetting Team (DSCVT)
DfT Directors' General, Non-Group Heads and Chief Executives	a. Set out their area's key activities and approach to BCM in their own BCM policy/strategy documents. b. Ensure effective BCM arrangements are in place for their area. c. Report the position on BCM in their area as part of DfT's 6-monthly management assurance process and for Agencies and in their annual Statement of Internal Control.
Departmental Security Officer, DSCVT	a. Responsible for ensuring all BCM related Mandatory Requirements in HMG's Security Policy Framework are met and day to day responsibility for all aspects of protective security including physical, personnel and information security
Deputy Departmental Security Officer, DSCVT	a. Chair the Agency Security Forum (which includes Business Continuity Management business). b. Representing DfT at inter-Departmental BCM meetings.
Business Continuity, Physical and Personnel Security Manager, DSCVT.	a. Responsible for maintaining and exercising the DfT Headquarters London Business Continuity Plan. b. BCM advice and best guidance.
All DfT Managers	a. Responsible for ensuring that they and their staff understand DfT's BCM policy and their area's approach to BCM.

Group/Post	BCM Roles and Responsibilities
	b. Maintaining and developing BCM arrangements throughout their business unit. c. Managers with staff who have a particular responsibility for BCM must ensure that those staffs' Terms of Reference/Job Descriptions include those responsibilities. Managers must also ensure appropriate BCM-related objectives and targets are agreed as part of the annual staff appraisal process.
BCM Focal Points/ Business Unit BC Planners	a. Representing their area on BCM. b. Acting as local source of BCM advice. c. Producing, updating and exercising business unit level BC plans.
Site Level BC Planners	Producing, updating and exercising a site level BC plans.
Group Audit Committee	Supporting the Principal Accounting Officer on issues of risk control and governance and associated assurance, including BCM.
DfT Audit and Risk Assurance Group	Internal audit of BCM across DfT in support of the Group Audit Committee.
DfT Resource Accounting & Corporate Governance	Gathering and reporting BCM data as part of DfT's 6-monthly management assurance process.
DfT Risk Policy Manager	Ensuring DfT's BCM arrangements are formally reviewed at least annually by the DfT Board.
Executive Agency Management Boards	Provide Agency-wide strategic direction on BCM.
Executive Agency Audit Committees	Supporting the Chief Executive on issues of risk control and governance and associated assurance, including BCM.
DfT Risk Managers	To work with BCM Managers, ensuring that BCM is an integral part of their organisation's risk management framework.