JOINT SERVICES PUBLICATION 503 (JSP 503) - MOD BUSINESS CONTINUITY MANAGEMENT

MINISTRY OF DEFENCE

© Crown Copyright 2011

First Edition published 2000

JSP 503 5th Edition (November 2011)

CONDITIONS OF RELEASE

Unless otherwise indicated, this information is Crown Copyright and the intellectual property rights for this publication belong exclusively to the Ministry of Defence (MoD). No material or information contained in this publication should be reproduced, stored in a retrieval system or transmitted in any form outside MoD establishments except as authorized by both the sponsor and the MoD where appropriate.

This information is released by the United Kingdom Government to a recipient Government for Defence purposes only. It may be disclosed only within the Defence Department of a recipient Government, except as otherwise authorized by the MoD.

This Joint Service Publication is sponsored by:

Director Business Resilience
Ministry of Defence
Main Building
1st Floor, Zone K
Whitehall
London SW1A 2HB

Intranet:
http://defenceintranet.diiweb.r.mil.uk/DefenceIntranet/Library/CivilianAndJointService/BrowseDocumentCategories/ManComm/CorporateGovernance/BusinessContinuityPlanning/BusinessContinuityDepartmentalGuidance.htm

EQUALITY & DIVERSITY IMPACT ASSESSING STATEMENT

This Policy has been Equality and Diversity Impact Assessed in accordance with the Department’s Equality and Diversity Impact Assessment Tool against:

Part 1 Assessment Only (no diversity impact found/policy is a reflection of legal requirements and has been cleared by a Legal Adviser)

INDEX

Chapter 5 – Developing and Implementing a BCM Response

Chapter 6 – Exercising, Maintaining, Reviewing and Assurance

Chapter 7 – Embedding BCM Culture

Chapter 8 – Sources of Information and Guidance

Glossary

CHAPTER 1 – INTRODUCTION TO BUSINESS CONTINUITY MANAGEMENT

Introduction

1.1 Mandatory requirement 4 of the Cabinet Office's Security Policy Framework[1] requires Government Departments to have:

> "robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business."

The British Standard for Business Continuity Management BS25999 (Part 1: Code of Practice, and Part 2: Specification) provides a structured approach to developing and implementing business continuity management, and enables organisations to measure their BCM in a consistent and recognised manner. To meet the requirements of the Security Policy Statement, Government Departments are therefore required to align their business continuity arrangements with the British Standard.

1.2 This Joint Services Publication, which is aligned with BS 25999 (Part 1: Code of Practice, and Part 2: Specification), provides detailed guidance on the implementation of MOD Business Continuity Management. Every effort must therefore to be made to adhere to its approach.

1.3 This Chapter explains:

- what Business Continuity Management (BCM) is and why it is important to MOD;
- how BCM is managed in MOD;
- how the different components of a successful Business Continuity Management framework fit together.

Business Continuity Management (BCM)

1.4 The term "Business Continuity" may be relatively new, but its principles are well understood through a variety of different business management processes (i.e. risk management, emergency management, disaster recovery).

1.5 JSP 525[2] details the requirement for all Departments, including MOD, to adopt Turnbull principles concerning Corporate Governance. Corporate Governance covers the way the Department is directed and controlled as a whole, with the *dual* aims of enhancing the prospect of achieving departmental objectives and providing a clear accountability framework. MOD's approach to Risk Management, which was

[1] http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework

[2] JSP 525 – Corporate Governance – September 2009 Edition 3

previously covered in JSP 525, is now set out in JSP 892. Business Continuity Management may be viewed as the effective management of business risks and, as such, falls squarely within the realms of good Corporate Governance and Risk Management.

1.6 The British Standards Institute (BSI) definition of Business Continuity Management is:

> **"A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."**

1.7 In simple terms, BCM identifies what needs to be done before an incident occurs to protect people, premises, technology, information, supply chains, stakeholders and reputation. This enables the development of strategies and contingency plans to manage the consequences of disruption, mitigate the impact on critical activities or outputs, and recover business back to normal levels of operation as soon as possible afterwards.

Why BCM is important to MOD

1.8 MOD plays a key role in defending the UK and its interests and in strengthening international peace and stability. The Department also has a unique set of responsibilities within Government that must continue to be met regardless of what may occur. Not only is MOD a key Department of State, it also provides political direction and key support to the nation's Armed Forces. For the Trading Funds (TFs), as with the Private Sector, the requirement to meet financial targets will be an important driver for ensuring that business can continue. BCM supports the achievement of the Defence Aim and the delivery of the Strategy for Defence by ensuring that MOD can continue to deliver or recover critical outputs (particularly operations) in the event of disruption.

1.9 MOD BCM therefore aims to:

- improve the resilience of MOD to disruption, protecting the ability to deliver key Defence outputs and objectives;

- provide a tried and tested method for restoring the MOD's ability to deliver key Defence outputs/activities, to a satisfactory level and within a specified time after disruption; and,

- deliver a proven capability to manage any disruption to MOD, and protect the reputation of both the Department and the UK Armed Forces.

1.10. There are three areas that are vital to MOD's ability to continue to deliver critical outputs following a disruptive event:

- **People.** Without our workforce, civilian and military, we will be unable to deliver Departmental objectives.

- **Processes.** MOD's key processes (including communication), maintained and implemented by our personnel, enable Departmental objectives to be met.

- **Resources**. This includes MOD infrastructure, supplies, services, information, budget and the time required to meet objectives.

Responsibilities for BCM in MOD

BCM Process Owner

1.11 Business Continuity Management has been identified by the Defence Board (DB) as a key, cross-cutting enabling business activity. To ensure that it is carried out in a coherent and consistent basis across the Department, PUS has delegated authority to the Director Business Resilience (DBR) as the Process Owner for Business Continuity.

1.12 DBR is formally accountable to the Defence Board (and PUS in particular), and is responsible for:

- the development and maintenance of a consistent system of Business Continuity policies, standards and practices;

- working across MOD to make it easier for TLBs and TFs to implement Business Continuity in support of the delivery of their outputs;

- driving continuous improvement in Business Continuity; and,

- providing assurance that all parts of the Department comply with this JSP and external requirements (e.g. the Security Policy Framework).

1.13 DBR has issued a combined Business Continuity Management Strategy and Plan[3], which is a subsidiary strategy (sub-Strategy) to the Strategy for Defence, and which builds on the business continuity framework established under the Departmental BCM Policy Statement and Strategy 2007-2008. This JSP supports the BCM Strategy and Plan by providing detailed BCM policy advice and implementation guidance.

[3] http://defenceintranet.diiweb.r.mil.uk/DefenceIntranet/Library/CivilianAndJointService/BrowseDocumentCategories/ManComm/CorporateGovernance/BusinessContinuityPlanning/MinistryOfDefenceBusinessContinuityManagementStrategyAndPlanCalendarYears20102015.htm

TLB Holders and Trading Fund Chief Executives

1.14 Responsibility and accountability for the implementation and maintenance of BCM arrangements within Top Level Budgets (TLBs) and Trading Funds is delegated to TLB Holders and Trading Fund Chief Executives. They are required to:

- Nominate an appropriate senior person (preferably at Board level) to be responsible for the development and implementation of BCM in their organisation, and to represent the TLB / TF on the Process Owner's Board;

- Nominate an individual or individuals (Business Continuity Focal Points) responsible for day-to-day BCM implementation in the organisation, and to encourage the establishment of a network of BC Planners within subordinate units;

- Publish a Business Continuity Strategy that gives subordinate units clear direction on what business functions are critical and how BC principles should be applied to protect them;

- Ensure that Business Continuity Plans are in place throughout their organisations and that the risks to continuity are managed effectively; and,

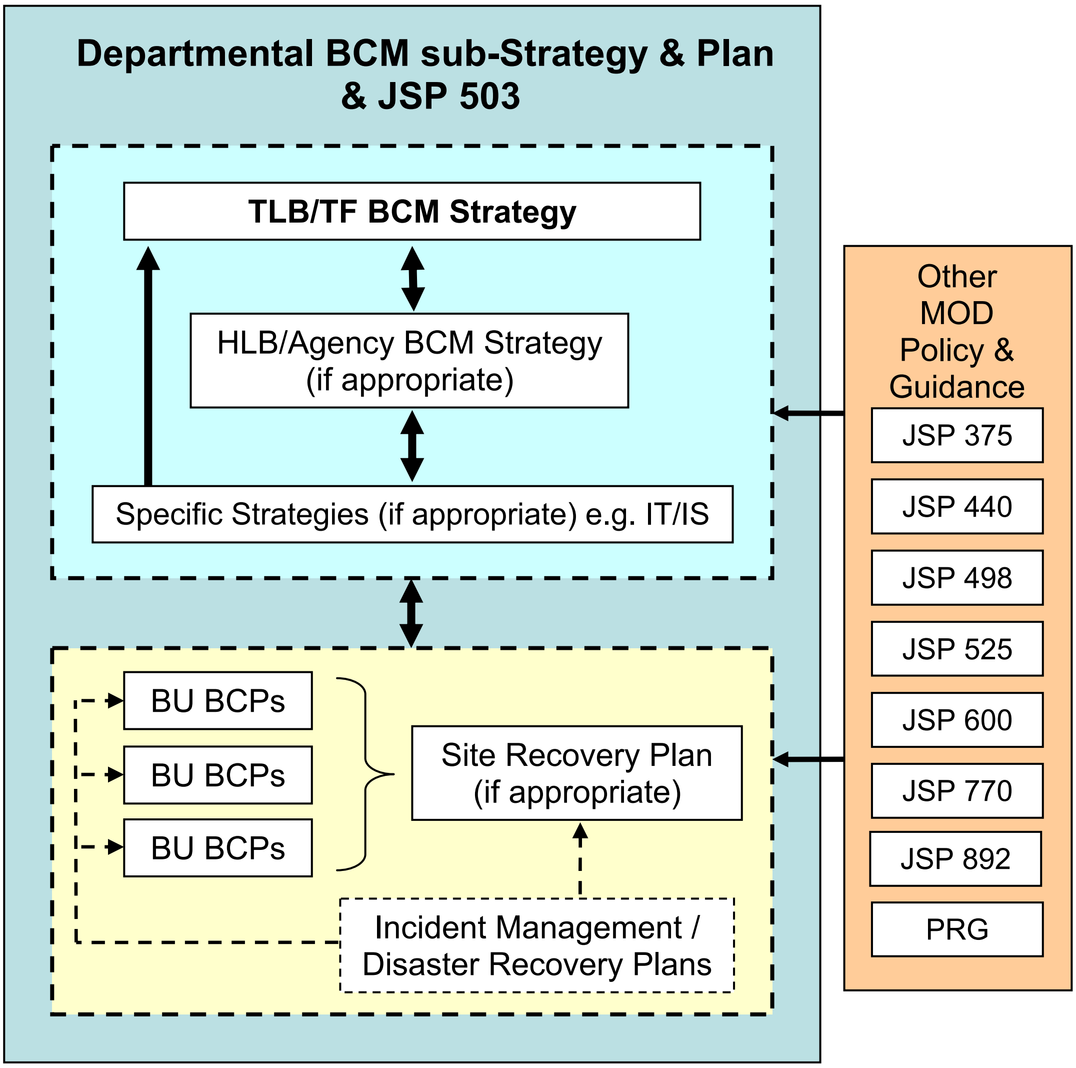
- Report annually on BCM as part of their corporate governance Statements of Internal Control (SIC) / Annual Accounts & Reports (AAR), and to contribute to the Process Owner's annual report on pan-Defence BCM to the Defence Audit Committee[4].

1.15 All Defence personnel should have, at the very least, a basic understanding of Business Continuity Management. However, certain individuals and groups of individuals in MOD have specific roles and responsibilities in respect of BCM. These are detailed in Annex 1A.

1.16 Figure 1 below shows the relationship between the MOD BCM sub-Strategy & Plan, policy guidance and lower level strategies and plans.

[4] Trading Funds provide an input to the Process Owner's annual report on BCM in recognition of their essential contributions to the delivery of critical Defence outputs, and to enable a pan-Defence picture to be presented.

Figure 1


Departmental BCM sub-Strategy & Plan & JSP 503
TLB/TF BCM Strategy
HLB/Agency BCM Strategy (if appropriate)
Specific Strategies (if appropriate) e.g. IT/IS
BU BCPs
BU BCPs
BU BCPs
Site Recovery Plan (if appropriate)
Incident Management / Disaster Recovery Plans
Other MOD Policy & Guidance
JSP 375
JSP 440
JSP 498
JSP 525
JSP 600
JSP 770
JSP 892
PRG

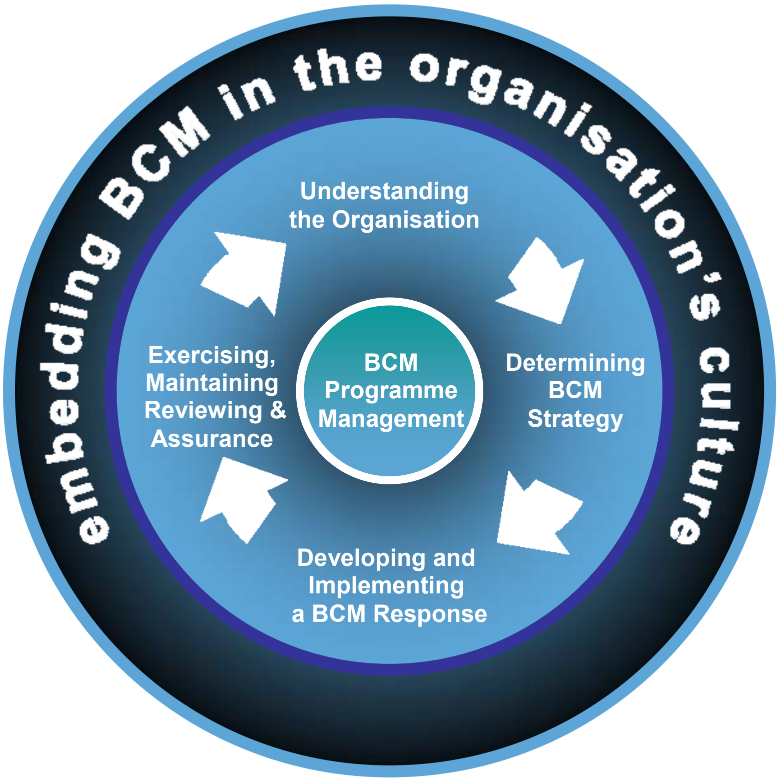
*Incident Management / Disaster Recovery Plan (or Emergency Plan) is shown here as a separate plan, although it may also form part of the Site Recovery or BU BC Plan. JSP 375 contains the detailed guidance on Incident Management and Emergency Plans.

Departmental BCM Model

1.17 The MOD's BCM model, which is based on the British Standard's BCM lifecycle, has six elements. Figure 2 below illustrates the approach, and each of the subsequent Chapters in this JSP covers in detail one of the six elements identified in the model.

1.18 The scope and structure of a BCM "programme" may vary both across the TLBs/TFs, and down through the various management levels (HLB, Business Unit etc), and the effort expended should therefore be tailored to meet the needs of individual organisations. <u>However, the six elements of the model should still be considered at each level of the organisation</u>.

Figure 2 – The MOD Business Continuity Model


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

1.19. The following paragraphs summarise the six essential elements of the Model:

1.19.1 **BCM Programme Management (Chapter 2)**. This is at the heart of the BCM process, setting both the organisational approach to BCM and how it is to be maintained, taking into account the size and complexity of the organisation.

1.19.2 **Understanding the Organisation (Chapter 3)**. The aim of this element is to identify the organisation's key outputs, and the critical activities and resources (including personnel) that support them. This involves undertaking a Business Impact Analysis and Risk Assessment, and identifying key stakeholders and dependencies.

1.19.3 **Determining Business Continuity Management Strategy (Chapter 4)**. This element takes the results of the analyses undertaken in "Understanding the Organisation" to develop appropriate BCM Strategies to ensure the continued delivery of key Defence outputs during and following an incident.

1.19.4 **Developing and Implementing a BCM response (Chapter 5)**. This involves the development and implementation of Business Continuity Plans, Site BC/Recovery Plans and Incident Management Plans that detail the steps to be taken during and after an incident to maintain or recover the delivery of Defence critical activities.

1.19.5 **Exercising, Maintaining, Reviewing and Assurance (Chapter 6)**. Plans must be updated regularly (at least annually) to cope with organisational changes, and exercised regularly to ensure that they are fit for purpose. Properly planned and conducted exercises will reveal weaknesses in BC arrangements which can be addressed subsequently. To meet Corporate Governance requirements it is necessary to undertake formal assurance review procedures. Issues of concern that arise during the assurance process should be recognised and addressed, thereby leading to improvements in BCM arrangements.

1.19.6 **Embedding BCM Culture (Chapter 7)**. All the work in the previous stages will count for nothing if there is insufficient understanding or awareness of Business Continuity and no commitment to establishing a “continuity culture”. Raising and maintaining awareness of BCM in Defence ensures that all personnel recognise why BCM is important, and the importance of their role in maintaining the delivery of Defence critical outputs. If personnel do not understand the general principles of Business Continuity, opportunities to improve Defence resilience will be missed when they arise during normal day-to-day management and operations.

ANNEX 1A

BCM IN MOD – ROLES AND RESPONSIBILITIES

The Defence Board (DB)

1.A.1 The Defence Board is the senior decision-taking body of the MOD. Its principal function is to make the high level decisions necessary to ensure that Defence delivers its outputs. The Process Owner for BCM, Director Business Resilience, is formally accountable to the Defence Board and is held to account by the Board. Once a year, TLB Holders will be held to account by the Defence Board for their delivery of their outputs and targets as set out in the Defence Plan, including on their implementation of effective BCM arrangements in accordance with this JSP[5].

The Defence Audit Committee (DAC)

1.A.2 The Defence Audit Committee (DAC) is a sub-committee of the Defence Board, and is chaired by a Non-Executive Director. It has a remit to review and challenge constructively the adequacy of internal controls and risk management assurance processes within Defence. It uses its independent perspective to provide assurance and advice on the application of Departmental BCM to the Defence Board.

TLB/TF Audit Committees

1.A.3 TLB/TF Audit Committees are to review BCM arrangements annually and this requirement must be included in their ToR. TLB Holders and TF Chief Executives are required to report to their Audit Committees via their annual Statement of Internal Control (SIC) and Annual Assurance Report (AAR) specifically on the progress and development of BCM throughout their TLB/TF.

The Audit Committee Non Executive Directors (NEDs)

1.A.4 NEDs can provide a valuable non-MOD perspective of TLBs' BCM. They may wish to challenge risk and Board-level governance, probe understanding of the Departmental BCM policy or seek evidence of BC Plan resilience e.g. testing, supply chains.

BC Focal Points

1.A.5 Each TLB/TF is to appoint a lead BC Focal Point (FP). TLB/TF BC FPs are responsible for the development of the TLB's/TF's BCM Strategy. They must set up a network within their TLB or TF to ensure that they can provide the necessary support to other BC Focal Points (e.g. at HLB / sub-ordinate levels) and Business Unit and Site BC Planners. TLB/TF BC FPs are to represent the needs of their local BC community and provide a conduit for communication with the DBR BC Policy

[5] Trading Fund Chief Executives are accountable to Ministers (and through Ministers to Parliament) for the discharge of the Trading Fund's functions.

Team. Suggested Terms of Reference for BC Focal Points can be found at Chapter 2, Annex 2A.

BC Planners

1.A.6 Individual Business Units are responsible for BCM at a local level. Business Unit BC Planners must develop, review, exercise and update their BC Plans as defined in their TLB/TF BCM Strategy (or HLB Strategy, where appropriate). BC Planners must also ensure that their BC Plans are regularly communicated to personnel to ensure that they are aware of their roles and responsibility in the event of a disruptive incident. Individuals needed to deliver critical activities / functions following a disruptive incident must also be aware of their roles and responsibilities. Suggested Terms of Reference for BU BC Planners can be found at Chapter 2, Annex 2B.

Heads of Establishment

1.A.7 Heads of Establishment (HoE) must ensure that every MOD building or establishment for which they are responsible has an up-to-date BC Site Recovery Plan. They are responsible for ensuring robust BC Site arrangements are in place, and for fostering a Site-level Business Continuity culture. If there is no nominated HoE for the site, the TLB/TF with the largest representation on it is to take the lead.

1.A.8 In the event of local or wide-spread civil emergencies (e.g. flooding), HoEs are to provide situation reports to the DBR BC Policy Team (or Operations Directorate UK CT&R) on any impact to their site or its outputs.

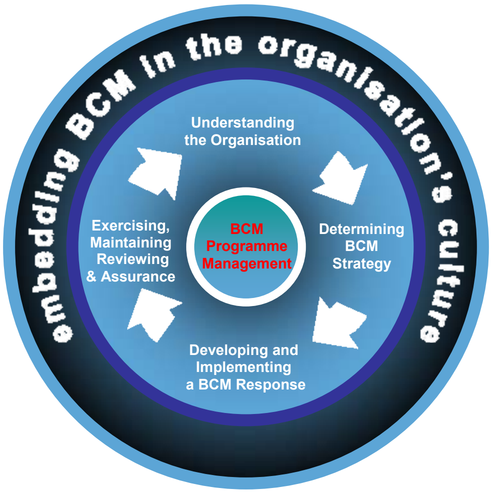
DBR Business Continuity Policy Team

1.A.9 The BC Policy Team has, under the direction of DBR (as Process Owner), responsibility for the MOD-wide governance of BCM; the development of MOD-wide BCM Strategy, policy guidance, and BCM training; the monitoring and managing of BC risk; raising BCM awareness across the Department; providing BCM advice to TLB/TFs (including on best practice); and generally promoting a more joined-up approach to MOD Business Continuity Management. The team has responsibility for maintaining this JSP.

1.A.10 The BC Policy Team is also the MOD lead on pandemic influenza planning and preparedness policy[6], and on engagement with the Cabinet Office and Other Government Departments, the private sector and academia on matters relating to Business Continuity Management.

[6] http://defenceintranet.diiweb.r.mil.uk/DefenceIntranet/Library/CivilianAndJointService/BrowseDocumentCategories/ManComm/CorporateGovernance/BusinessContinuityPlanning/ModPandemicInfluenzaPlanning.htm

CHAPTER 2 – BUSINESS CONTINUITY MANAGEMENT PROGRAMME MANAGEMENT


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

Introduction

2.1 Effective programme management is at the heart of the BCM process, providing the framework for MOD's approach to Business Continuity (as defined in the MOD BCM Strategy and this JSP).

2.2 Senior Managers (and TLB Holders / TF Chief Executives in particular) play a key role in ensuring the implementation of the BCM process throughout MOD, that it is adequately supported and resourced and is embedded in MOD's culture.

2.3 BCM programme management has three steps: Assigning responsibilities (governance of the process); implementing BCM in the organisation; and, the ongoing management of BC.

Assigning Responsibilities

2.4 TLB Holders / TF Chief Executives are to nominate an appropriately senior person (preferably at Board level) to be responsible for the development and implementation (and "championing") of BCM in their organisations. Their work is supported by a nominated TLB/TF lead BC Focal Point.

2.5 As the MOD is a large, diverse and complex organisation, TLBs/TFs should establish a network of BC Focal Points and BC Planners (including Site Planners) to assist in the delivery of BCM. TLBs/TFs are also encouraged to establish BC Focal Point Forums to assist in the development and delivery of BCM. The roles and responsibilities of all of these individuals should be contained in their job descriptions and skills profiles (see Annexes 2A – 2D for suggested Terms of Reference).

2.6 It is important that clear direction is given at the TLB/TF level so that managers and staff understand BCM priorities and risk appetite, and know that senior managers are committed to the principles of BCM and support the efforts of BC Focal Points and Planners.

Implementing BCM

2.7 TLBs/TFs must ensure that:

- BCM arrangements are communicated throughout their organisation and to all stakeholders;

- Staff with specific BC responsibilities receive adequate training to undertake their duties (see Chapter 7); and
- BCM arrangements are exercised at least on an annual basis, or when affected by significant change (e.g. organisational restructuring, installation of new IT system, move to a new location).

Ongoing Management

2.8 BCM should be an ongoing management activity embedded within TLBs/TFs. To ensure that it remains fit for purpose, BCM arrangements must be regularly exercised, reviewed and updated. In particular, plans must be reviewed and updated whenever there is a significant change in operating environment, personnel, processes or technology – or when an exercise or incident highlights areas for improvement.

2.9 To support the MOD BCM programme, the following documentation is to be created and maintained:

- MOD BCM Strategy and Policy (this is the responsibility of the BC Policy Team);
- TLBs'/TFs' Policy Statements and Strategies;
- Business Impact Analysis (BIA);
- BC Plans – including Site Recovery and Incident Management Plans, and Pandemic Influenza and other contingency plans (as appropriate);
- Risk and threat assessments;
- BC Training Plans and records (as appropriate);
- Communications/awareness plans;
- Exercise Programmes, scenarios and post-exercise reports;
- Service Level Agreements and contracts (with stakeholders, customers, suppliers and contractors);
- Audit Reports and Action Plans.

ANNEX 2A

SUGGESTED TERMS OF REFERENCE FOR TLB/TF/HLB BC FOCAL POINT (FP) / Planner

BC Management

- Maintain awareness and understanding of MOD BC Strategy and Policy, JSP 503 and other guidance documents (i.e. pandemic influenza).

- Development of TLB/TF BC Policy and Strategy, and awareness and understanding of key Site and BU BC Plans.

- Regularly review/update the TLB/TF BCM Strategy in line with TLB/TF BC reporting timescales.

- Set up and maintain a network of subordinate BC FPs and Site Planners that will enable coverage and communication with all BC BU Planners.

- Organise and chair regular BC FP Forums. The objective of the BC FP Forum is to provide an opportunity for all subordinate FPs and key BC planning staff to come together to drive forward TLB/TF BC and raise any BC related issues and concerns. BC FP Forum ToRs can be found at Annex 2D.

- Define ToRs detailing the roles and responsibilities of subordinate BC FPs (using a 'slimmed down' version of these ToRs as the basis).

- Provide support, advice and guidance to TLB BC planning staff on matters of BC Policy and good practice.

- Collate/co-ordinate and report information on TLB/TF business continuity activities and performance as required (see also under Corporate Governance).

- Maintain a database of the BC Plans (including Site Plans) in place within the TLB/TF.

- Ensure all BC Planning staff are aware of their responsibility to exercise and update plans (as defined in the TLB/TF BCM Strategy), and produce a post-exercise report which contains lessons identified, recommendations and an action plan.

- Ensure all staff are aware of their responsibility to have undergone BC training.

Corporate Governance

- Provide an input on the status of the TLB/TF BCM programme, when requested, for the annual assurance report for the TLB/TF Audit Committee.

- Collate/co-ordinate the required information for the TLB's/TF's input to the Annual Departmental BCM Report to the Defence Audit Committee, as directed by the BC Policy Team.

Communications

- Disseminate and capture information for the BC Policy Team using the subordinate BC FP and Site Planner Network.

- Actively seek to identify issues that would benefit from being addressed at TLB/TF level, such as knowledge/awareness issues and best practice. Inform the BC Policy Team of these issues where they may be benefit in addressing them departmentally.

- Maintain TLB/TF BC awareness, e.g. by running poster campaigns, workshops, briefings/seminars etc

ANNEX 2B

SUGGESTED TERMS OF REFERENCE FOR BU BC PLANNERS

Define the scope of BU Planners' responsibility i.e. the BU they are responsible for.

BC Management

- Maintain awareness and understanding of the MOD BC Policy, referring to JSP 503 and other guidance documents (i.e. pandemic influenza).
- Maintain awareness and understanding of relevant TLB/TF BC Policy and planning, referring to the TLB/TF BCM Strategy, local Site Plans, and related BU BC Plans.
- Know the local BC FP and Site Planners.
- Create BC Plans for new BUs or where the previous Plan is no longer valid (i.e. due to reorganisation).
- Undertake periodic reviews (at least annually) of the BU BC Plan to ensure it remains fit for purpose.
- Write, exercise and update the BU BC Plan in line with TLB/TF BCM Strategy guidance (and BC Site Plan where appropriate) and this JSP, produce post-exercise reports and implement any recommended changes to the BU BC Plan.
- Produce post-incident reports (copied to TLB/TF BC FP).
- Attend BC FP Forums, as required.
- Responsibility for maintaining BU BC awareness, particularly when Plans have been updated and before and after exercises. Awareness programmes/activities may include running poster campaigns, producing newsletters, websites etc.

Corporate Governance

- When required provide an update to the TLB/TF FP on BU BCM.

Communications

- Actively seek to identify issues that would benefit from being addressed at TLB/TF level, such as knowledge/awareness issues and best practice, and pass them onto the local BC FP.

ANNEX 2C

SUGGESTED TERMS OF REFERENCE FOR SITE BC PLANNERS

Define the scope of the Site Planner's responsibility i.e. the Site they are responsible for.

BC Management

- Maintain awareness and understanding of the MOD Site-level BC Policy, referring to JSP 503 and other guidance as appropriate.

- Maintain awareness and understanding of relevant TLB/TF BC Policy and planning, referring to the TLB/TF BCM Strategy, local BU BC Plans and related Site BC and Incident Management Plans.

- Know the local BC FP and the Site BU BC Planners.

- Work with BU BC Planners to create Site BC Plans for new Sites or where the previous Plan is no longer valid (i.e. due to reorganisation) – see Chapter 5.

- Exercise the Site BC Plan in line with TLB/TF BCM Strategy guidance (and Chapter 6), produce post-exercise reports and implement any recommended changes to the Plan.

- Produce post-incident reports (copied to the local BC FP and TLB/TF BC FP).

- Attend BCFP Forums, if required.

- Maintain responsibility for maintaining Site-level BC awareness, e.g. by running poster campaigns.

Corporate Governance

- When required provide an update to the TLB/TF FP on Site BCM.

Communications

- Actively seek to identify issues that would benefit from being addressed at TLB/TF level, such as knowledge/awareness issues and best practice, and pass them onto the local BC FP.

ANNEX 2D

SUGGESTED TERMS OF REFERENCE FOR BC FOCAL POINT FORUMS

Purpose

The purpose of the BC Focal Point Forum is to improve Business Continuity Management arrangements throughout the TLB/TF.

Objectives

The BC FPF will:

- Identify methods for increasing the profile of business continuity within TLB/TF areas and produce material which can be used for helping to increase staff awareness of BC within TLB/TF areas.

- Review the way in which Business Continuity risks are managed, as declared in the annual TLB/TF report to the TLB/TF Audit Committee.

- When appropriate review and promote TLB/TF Business Continuity training.

- When appropriate review TLB/TF Business Continuity Policy and Strategy.

- Identify areas for, and promote the sharing of, best practice between members (e.g. BC exercises, lessons identified/learnt, reciprocal support arrangements).

- Identify Business Continuity related issues that affect more than one area and which would benefit from being addressed by a joint approach.

Representation

Decide on management areas to be represented, by whom, at what level and how many representatives (including for example: Site Planners, functional experts (i.e. IT, Facilities Management), local TU representatives).

Meeting Frequency

Decide how often the Forum is to meet.

Location

Decide where the Forum is to meet.

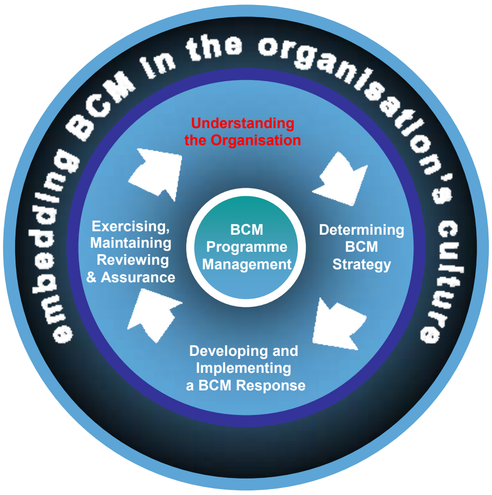
Secretariat

Decide who should provide secretariat support.

Accountability and Reporting

Decide to whom the Forum should be accountable.

CHAPTER 3 – UNDERSTANDING THE ORGANISATION


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
BCM Programme Management
Exercising, Maintaining Reviewing & Assurance
Developing and Implementing a BCM Response

Introduction

3.1 To develop and successfully implement a BCM Strategy, it is essential to have a clear understanding of the organisation (i.e. TLB/TF or subordinate level) it will cover.

3.2 In a BC context, building an understanding of the organisation involves the identification and prioritisation of the organisation's critical outputs, and of the time criticality of the key activities and resources (including personnel) that support them. These activities ensure that the resulting BCM Strategy best meets the needs of the organisation – specifically its objectives and obligations.

3.3 The following activities help to establish an understanding of the organisation:

- The identification of the organisation's objectives, stakeholder relationships and obligations and the environment in which it operates;

- The identification and prioritisation of all critical outputs and processes/activities, and the assets and resources (including those from outside of the organisation) that support their delivery;

- An assessment of the impact and consequences over time of a failure to maintain or deliver the key outputs, processes and activities;

- The identification and understanding of the interdependencies of the organisation's activities (e.g. intra-TLB, inter-TLB and external to MOD (commercial partners and contractors, OGDs and other Nations' Governments)), including any reliance placed on the organisation by others.

Identifying Critical Outputs

3.4 In the aftermath of a disruptive event there will not be the time or resources to do everything, and so **TLB/TF BC priorities must be set out in the BCM Strategy** document, to ensure that subordinate Business Units have the guidance necessary for effective and focused lower-level BC planning.

3.5 Each TLB/TF, in consultation with its subordinate formations, must review its organisational outputs/processes, with the aim of identifying all critical processes, outputs and/or other business activities undertaken within the TLB/TF which contribute to Defence critical outputs, and which are deemed worthy of BCM

Planning activity. The Strategy for Defence, Defence Strategic Direction and the Defence Plan set out the priority Defence tasks and operations, and provide a starting point for assessing what is Defence critical. Lower level strategies and plans (e.g. Sub-Strategies and local Management Plans) may also prove useful in providing information to support consideration of TLB/TF and subordinate level critical outputs and activities.

3.6 Some TLB/TFs may have priorities that regularly change - such as Urgent Operational Requirements (UORs) managed by Project Teams in Defence Equipment & Support (DE&S). In these cases, the identification and recording of critical activities may appear counter-productive. However, the need to identify critical activities is fundamental to BCM. Mechanisms to identify critical activities on a regular basis, or swiftly once an incident has occurred, must be robust and effective, and defined in the TLB/TF's BCM Strategy.

3.7 For BCM Strategies across the MOD to be coherent and joined-up there needs to be close dialogue between all TLB/TF planners. The MOD BC Steering Group (chaired by Assistant Head BC Policy and attended by TLB/TF BC FPs) is one mechanism for achieving this. In an ideal world, the needs of the 'customer' (the Front Line) will drive the overall BC priorities adopted across the Department, but in reality other factors come into play and so there will need to be a degree of negotiation before 'customer' and 'supplier' TLB/TF BC positions are finally agreed.

Business Impact Analysis (BIA)

3.8 Business Impact Analysis (BIA) is a process for analysing business functions and the effect that a disruption might have on them. It provides important information to support the development of BC Strategies to enable time critical business to continue following the effects of a disruptive incident.

3.9 To ensure coherence across the MOD, and to set the order in which business activities/outputs (and the personnel/posts[7] that support/deliver them) are recovered, TLBs/TFs are to adopt the following time criticality phases (Table 1). Each area is different, so options for phasing the recovery process should be discussed with local Site Recovery Planners and key BU BC Planners (see Chapter 5 paragraphs 5.24-5.25).

Table 1 – Time Criticality

Time Criticality Phases	Indicator	Description
In the first 24 hours	**RED***	What cannot be disrupted for more than a few hours (i.e. support to an important military capability)
Days 1-3	**RED**	What must be back in operation within the first few days
Days 4-7	**AMBER**	What cannot be delayed for more than a week

[7] Post Criticality is to be recorded on the Civilian Casualty Information Service (CCIS) on HRMS, in support of BU BC Plans and Site Recovery Planning. See Chapter 5, Annex 5B.

Days 8-21	GREEN	What can stand a few weeks delay, but no more
Day 22 and beyond	GREY	The rest: critical objectives not so sensitive to time delay, and the remaining non-critical objectives

3.10 Even within the time critical phases, there is likely to be a range of objectives, probably inter-related, with different resource needs and with different priorities. Some activities may need extensive effort to recover over a longer period of time whilst other more time critical activities may need less effort, and vice versa. To meet this challenge, **thought has to be given to the order in which critical objectives need to be recovered**, thus providing subordinate BC planners within the TLB enough information to plan and resource a successful and efficient recovery.

3.11 The scale of an incident will, however, dictate what resources are available and therefore what can or cannot be done. The TLB/TF Strategy must define the minimum level of activity that the organisation should prepare for against the worst credible scenario; defining the output priorities, and giving clear direction as to where BC effort should be focused (bearing in mind that all BC planning activities have, to some degree, a cost in terms of money or other resources).

3.12 In reality, an incident is unlikely to be so severe as to bring the organisation down to the planned worst case, and so the actual response locally should be focused on the most time critical outputs identified within the TLB BCM Strategy, plus whatever else can be achieved using the remaining resources. **It is therefore important to prioritise all TLB/TF objectives/outputs/activities so that subordinate formations know where to deploy additional resources once the most critical ones have been covered.**

3.13 For any less time critical activities that have particular sensitivities, for example political or PR, consideration will need to be given to what additional staffing or planning might be necessary to deal with the ramifications of not undertaking that work for a period of time (for example, the development of defensive press lines).

3.14 For BC planning to be meaningful, it must be based upon realistic assumptions. BC Planners must look carefully at the organisation and make choices (sometimes difficult) about **whom or what** is critical and non-critical. **Criticality has nothing to do with grade or rank.** Whilst an effective management structure is an important element in recovering from a disruptive event, BC Planners should avoid the temptation of recovering the organisation from the top down. It may prove necessary to tell a very senior person that they are not critical in the first few weeks; this does not detract from their importance during normal operations.

13.15 Resources are finite; during and in the aftermath of a disastrous event there will be an additional squeeze on their availability. The resources that each activity will require on resumption should be determined in consultation with the needs of stakeholders, including:

- Staff resources – numbers, skills and knowledge;

- Facilities required – buildings, sites;
- Supporting technology and equipment (e.g. IT terminals and software);
- Information requirements – to enable the activity to continue;
- External services and supplies (see also Dependencies below);
- Funding – to replace lost assets, for travel and other expenses.

3.16 Further information and a simple Business Impact Analysis template are provided at Annex 3A.

3.17 BC Planners (and Senior Managers) can then use the outcome of existing risk assessment processes (see paragraphs 3.22 to 3.31 below) to assess the likelihood of disruptive events occurring and therefore the level of resource to direct at their management.

Dependencies

3.18 All organisations, whether private or public sector, are in some way dependent on third-party providers, key suppliers or business partners for the delivery of their outputs. Simply put, dependencies can be:

- inputs – i.e. services or products - to the organisation that support or enable it to produce its outputs; and,
- outputs from the organisation that support or enable another organisation to produce their outputs.

3.19 For MOD, these dependencies occur both within the Department, i.e. an output from one TLB that is critical to the delivery of another TLB's outputs – known as "intra-dependencies", and between external organisations and the Department (and *vice versa*) – known as "interdependencies". (See Figure 2 below.)

3.20 It is important for the development of a BIA and Risk Analysis, and in the subsequent development of BC Strategies and Plans, that dependencies are properly identified, understood and managed. In particular, TLBs/TFs (HLBs and BUs) must ensure that they:

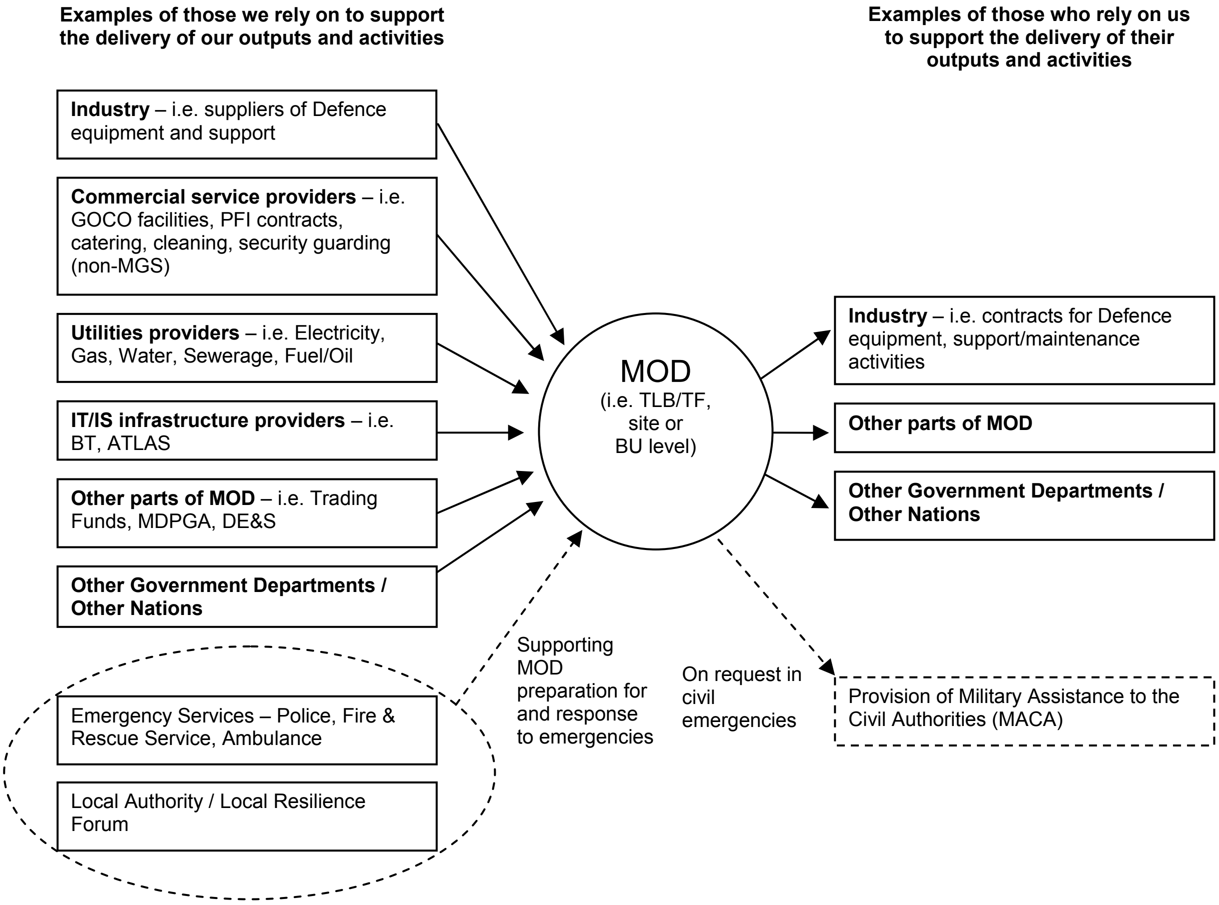
- identify and understand the interdependencies with contractors/suppliers, their approach to BCM and how resilient they are to disruption (including the resilience of their supply network);
- understand the impact of (and mitigate) the loss of services/support/equipment from contractors/suppliers due to disruption – particularly those that support or enable critical Defence outputs and activities;

- understand the recovery arrangements of contractors/suppliers and, where possible, ensure that these are coherent with MOD BC arrangements (and *vice versa*) – e.g. an understanding of what we can expect from them following an incident, and in turn what they can expect of us;

- understand how changes to a TLB's objectives, or disruption of their outputs, might impact on customers in other TLBs/TFs.

3.21 TLBs/TFs (HLBs and BUs) should ensure that contractual arrangements provide for adequate support to continue for the equipment/capability/service, in the event that a contractor is no longer able (or required) to provide the support expected of them. This can become more complicated where there is a jointly held responsibility (e.g. contracts with consortia) and individual parties may not be clear about their respective responsibilities for consequence management following disruption. Where possible, these risks are to be mitigated by ensuring Business Continuity requirements are stipulated in contracts, and interdependencies and supply chain vulnerabilities are identified and appropriately managed. Further information can be found in the Commercial Policy Statement on Business Continuity Management, published in The Commercial Toolkit on the Acquisition Operating Framework[8].

Figure 2 - Dependencies


Examples of those we rely on to support the delivery of our outputs and activities
Examples of those who rely on us to support the delivery of their outputs and activities
Industry – i.e. suppliers of Defence equipment and support
Commercial service providers – i.e. GOCO facilities, PFI contracts, catering, cleaning, security guarding (non-MGS)
Utilities providers – i.e. Electricity, Gas, Water, Sewerage, Fuel/Oil
IT/IS infrastructure providers – i.e. BT, ATLAS
Other parts of MOD – i.e. Trading Funds, MDPGA, DE&S
Other Government Departments / Other Nations
Emergency Services – Police, Fire & Rescue Service, Ambulance
Local Authority / Local Resilience Forum
MOD
(i.e. TLB/TF, site or BU level)
Supporting MOD preparation for and response to emergencies
On request in civil emergencies
Industry – i.e. contracts for Defence equipment, support/maintenance activities
Other parts of MOD
Other Government Departments / Other Nations
Provision of Military Assistance to the Civil Authorities (MACA)

[8] http://www.aof.dii.r.mil.uk or http://www.mod.uk/aof

Evaluating Risks to Critical Activities

3.22 Investigating BC risks that can realistically be managed should be pursued through existing risk management processes (see JSP 892 for further information). A risk assessment should be undertaken to identify how susceptible critical outputs are to certain events and external factors[9]. However, whilst it is useful to understand some of the more obvious causes of disruption in order to identify ways in which their impact might be reduced or avoided, **BC Planners should not focus on cause. Continuity needs to be achieved in spite of cause, and so it is more important to consider the effects of an incident and the impact it might potentially have upon the organisation**.

3.23 Any disruptive event is likely to have one or more of the following impacts on the organisation's ability to deliver Defence critical outputs (further information on threats and hazards is provided at Annex 3B)**. It is these impacts that BC Planners must consider in the development of their BU or Site BC plans**:

- Temporary or longer-term unavailability / loss of personnel;
- Loss of or damage to buildings and infrastructure (including IT, telecoms);
- Loss of data / information;
- (For Trading Funds) Damage to financial standing;
- Loss of key supplier;
- Damage to reputation.

Determining Risk Management and Mitigation Options

3.24 An essential part of BCM is the review of BC risks. BC risks are essentially no different from other, more familiar business risks, and they should be managed in exactly the same manner.

3.25 Detailed MOD guidance on conducting risk analysis, and implementing risk management and mitigation options, is contained in JSP 892 – Risk Management. The MOD follows the "5T" model set out in the HM Treasury Orange Book for strategies to control or respond to risk: Terminate (suspend or terminate activities); Transfer; Treat (control action); Tolerate (accept); and, Take the Opportunity (gaining additional benefit).

> 3.25.1 Terminate - The option to change, suspend or terminate an activity, process or service, should only be considered when there is no conflict with the organisation's objectives and stakeholder expectation.

[9] Further information can be found in the National Risk Register (http://www.cabinetoffice.gov.uk/resource-library/national-risk-register)

3.25.2 Transfer - It may, in certain circumstances, be appropriate to transfer risks. Risks may be transferred in order to reduce the risk exposure to the organisation, or because another organisation is more capable of managing the risk.

3.25.3 Treat – This is the most likely initial response to risks, and involves taking controlling action – preventative, corrective, directive or detective[10]. There may still be some residual risk after control action has been taken, which may require further use of Treat or Tolerate strategies. In Business Continuity terms, continuity strategies are part of a Treat approach, in that they seek to improve resilience to disruption by ensuring critical activities continue or are recovered to an acceptable level within the timeframes stated in the BIA.

3.25.4 Tolerate - A risk may be acceptable without requiring any specific action to be taken. Even if not acceptable, the organisation may not have the ability to manage the risk, or the cost of doing so might be disproportionate to the potential benefit gained. In these cases, senior management may decide that the level of risk is tolerable and within the organisation's risk appetite.

3.25.5 Take the Opportunity – In mitigating a threat (e.g. transfer or treat), it may be possible to gain additional benefit, i.e. identifying resource that can be used elsewhere to benefit the organisation.

3.26 Risk analysis is likely to identify a number of risks to the normal continuation of TLB/TF critical business. If possible, practicable and affordable, any obvious mitigation work to reduce or remove these risks must be investigated (accepting that it is not cost-effective to protect every activity against every conceivable risk), to reduce the need for recovery action later should that risk materialise. Consultation with stakeholders (customers, suppliers, etc.) will prove useful in this respect. For the more obvious disruptive events, contingencies or workarounds may have already been developed through the normal course of business (e.g. local security arrangements mitigate against attack, compliance with H&S legislation and building regulations reduce the outbreak of fire, etc.).

3.27 In exploring options, it is important to be realistic about risk. Non-operational support activities may not justify elaborate contingency planning. Nevertheless, maintaining business continuity in key non-operational activities is important because of the knock-on effect of a major disruption on operations and the adverse impact on efficiency and budgets. Another example is a single point of failure for a critical system which may not, during normal operations, present a problem but which could be significant in the context of BCM – e.g. a relatively small localised incident, if focused at this weak point, could inflict significant disruption. There will be a compromise between investing in preparations that reduce the cost of responding to a disruption and accepting a risk that will incur higher penalties should it occur.

3.28 TLBs/TFs and Business Units should use the result of the Business Impact Analysis and the risk assessment to identify measures that:

[10] See JSP 892 Chapter 4 for further information on Treat activities.

- Reduce the likelihood of disruption;
- Shorten the period of disruption; and
- Limit the impact of disruption.

3.29 TLB/TF (and HLB/BU as appropriate) Senior Management should sign-off the BIA and the risk assessment to indicate that the risks to the organisation have been correctly identified and that the risk management and mitigation options have been accepted. This sign-off also gives clear indication that Senior Managers endorse the organisational approach to BCM.

3.30 In summary, the following are some approaches/factors that may help to reduce MOD BC risk:

- Visibly committed Senior Management support;
- Improved linkage between TLBs and industrial partners, stakeholders, customers;
- Affording BC the same status in MOD as Safety and Security;
- Promoting awareness and training;
- A clear focus on time critical activities that support critical outputs;
- Explore and understand interdependencies;
- Incorporating BC into existing management processes and corporate cultures;
- Effective communications (both internal and external);
- Build-in resilience, rather than bolt-on (proactive rather than reactive);
- Awareness of other/future challenges – e.g. partnering, outsourcing, supply chain disruption, restructuring, contractorisation.

3.31 A simple (3x3) risk assessment matrix is provided at Annex 3C.

ANNEX 3A

BUSINESS IMPACT ANALYSIS TEMPLATE AND FURTHER GUIDANCE

Scope and Scale

- BIA can be done at any level within the organisation. TLB-level BIAs (to feed into the TLB BC Strategy) may be less detailed and more strategic than those carried out at lower levels – where the level of detail will be important for the formation of contingency plans.

- Determine whether the BIA will be single-site or required to cover more than one location.

- Identify the key business objectives of the organisation and the success criteria of each. Information collection methods may include workshops, questionnaires and interviews (structured and unstructured).

- If necessary, agree and sign-off the terms of reference for the BIA with the sponsor (e.g. TLB/TF Management Board, or nominated representative).

Conducting a BIA

(Serial numbers relate to the BIA template contained in this Annex)

Serial 1. Identify the activities (outputs, processes etc) across the organisation, the owners of these processes and the number of people employed on the activity during normal operations. (Subject matter experts within the TLB/HLB/BU should be able to provide supporting information on these activities.)

Serial 2. Identify any supporting or dependent activities – these may be within the same organisation (i.e. TLB, unit or team) or in another.

Serial 3. Determine the timescale within which the interruption of each activity becomes unacceptable to the organisation – this is known as the maximum tolerable period of disruption.

Serials 4 and 5. Determine the target time (the Recovery Time Objective) for the resumption of the activity at a minimum level (this must be less that the maximum tolerable period of disruption), and also the timescale for the resumption of the activity to normal levels of operation.

Serial 6. Identify all the tasks which support the activity at Serial 1 which need to be undertaken during each time phase. This information will help determine the minimum resources (personnel, IT, information etc) required for each time phase at Serial 7.

Serial 7. Determine the resources which will be required to maintain the activity at an acceptable (minimum) level within the maximum tolerable period of disruption, and the resources required beyond that to return to normal levels of operation. It is important to ensure that there is coherence in the recovery times between the main activity and any supporting or dependent activities.

Outcome

- Obtain sign-off by the activity / task owner to confirm accuracy of the information.

- Present the BIA to the TLB/TF Management Board for approval to proceed to the development of a BCM Strategy.

Example BIA Template

1.	**Activity**	Brief description of the activity and the reason(s) for performing it:
		Owner of the activity:
		Number of staff employed on the activity during normal operations:
2.	**Supporting or dependent activities**	Activities/outputs that must happen or be in place before the activity at Serial 1 can be performed:
		Other activities which are reliant on the activity at Serial 1:
3.	**Determine the timescale within which disruption to the activity (Serial 1) becomes unacceptable**	Less than 24 hours? (RED*)
		1 to 3 days? (RED)
		4 to 7 days? (AMBER)
		8 to 21 days? (GREEN)
		>22 days? (GREY)
4.	**Determine the target time for the resumption of the activity at a minimum level**	
5.	**Determine the timescale for the resumption of the activity to normal levels of operation**	

Completion Notes	
Serial 1	An activity can be a process, a set of processes or a branch/team/unit/function that produces or supports one or more products, services or outputs.
Serial 2	These may be within the same organisation (i.e. TLB, unit or team) or in another. It is important to ensure that there is coherence in the recovery times for supporting and dependent activities.
Serial 3	To ensure consistency, all TLBs and Trading Funds, and subordinate organisations must use the time criticality phases in JSP 503, and repeated in this template.
Serial 4	This must be less than the timescale at Serial 3.
Serial 5	This will help establish the requirement for resources for a staged recovery back to normal levels of operation.

6.	**Provide a brief description / list of the tasks (for the activity under Serial 1) which need to be undertaken during each time phase. This information will help determine the resources (personnel, IT, information etc) required for each time phase at Serial 7.**	**24 hours** **RED***	**1-3 days** **RED**	**4-7 days** **AMBER**	**8-21 days** **GREEN**	**>22 days** **GREY**
7.	**Resources required for activity at Serial 1 and tasks by phase listed at Serial 6**	**24 hours** **RED***	**1-3 days** **RED**	**4-7 days** **AMBER**	**8-21 days** **GREEN**	**>22 days** **GREY**
	Personnel (number required by grade or specific posts)					
	Facilities (buildings / sites)					
	IT (number of terminals and classification)					
	IT software packages (if not standard DII) / **Internet Connectivity**					
	Other equipment / resources (telephones (inc secure					

	telecoms), fax machines, printers, photocopiers etc)					
	Information or any other special requirements					
	Funding (for ad hoc costs arising from incident)					

ANNEX 3B

GENERIC THREATS AND HAZARDS

Understanding the possible causes of disruption (the threats and hazards) will help to:

- identify appropriate risk mitigation measures to reduce the likelihood of the threat or hazard arising, and reduce (or remove) its impact on the organisation should it occur; and,
- develop effective Business Continuity Plans and Site Recovery Plans to manage the impact of disruption.

Threats are deliberate and malicious acts, e.g. terrorist attacks; Hazards are accidental and non-malicious events, including naturally occurring events such as bad weather, flooding etc.

Impact	Examples of Causes (Threats and Hazards)	Type of risk mitigation
1. Short or long-term loss of personnel	• Industrial action: staff strikes, transport (local or national), fuel, protestors outside of bases preventing access. • Bad weather: storms, flooding, snow etc. • Pandemic Influenza, Seasonal Flu, Norovirus etc (e.g. sickness levels above normal rates over an extended period). • Terrorist incidents. • Accidents (including Fire). • Impact of events such as the Olympics 2012.	• BC / Sy • BC / FM • BC • Sy and BC • Safety / FM • BC
2. Loss of access or damage to facilities/sites	• Bad weather: storms/gales, flooding (on-site or surrounding area), severe drought/heat wave, snow and ice (on-site or surrounding area). • Terrorist attacks/incidents, including “white powder” incidents. • Crime – vandalism, theft. • Fire. • Utilities failures – electricity, gas, water and sewerage, heating/cooling systems. • Hazardous material spills/accidents. • Biological hazards, e.g. Foot and Mouth Disease. • Industrial action, protests etc which block access to sites. • Accidents, e.g. road accidents which block access to sites. • Poor infrastructure maintenance.	• FM / BC • Sy / BC • Sy • Safety / FM • FM / BC • Safety / FM • BC • Sy / BC • BC • FM
3. Loss of or denial of access to CIS	• Electricity failures. • Cyber-Security threats, viruses etc. • Damage to IT/IS infrastructure arising from threats/hazards at (2). • Failure of the telephone network (including mobile) – as a result of bad weather (including solar weather),	• FM / BC • Sy • FM / BC • FM / BC

	terrorist incidents, overloading of the network, bandwidth restrictions etc.	
4. Loss of or denial of access to information	• Security breaches, leaks, unintentional and intentional losses of information. • Cyber-Security threats, viruses etc. • IT/IS infrastructure failures at (3) – including loss of Data Centres and Servers. • Loss/damage to paper holdings (fire, flood, accidental disposal).	• Sy • Sy • FM / BC • FM / BC
5. Loss of a key supplier, or interruption to the delivery of critical services / equipment	• Threats/hazards at (1)-(4). • Failure/interruption of the supply chain. • Financial failure / bankruptcy.	• BC • BC • BC
6. Damage to the reputation of the MOD and the Armed Forces	• Terrorist activities - causing damage to MOD property, killing/injuring Defence personnel. • Cyber Threats – causing loss of classified data and failure of MOD IT/IS systems. • Health & Safety failures in the working / operating environment - including CBRN incidents (particularly where impact is also on the general public), infrastructure-related incidents (e.g. fire, building collapse). • Security – theft, leaks, loss of data, fraud.	• Sy • Sy • Health & Safety • Sy

BC = Business Continuity
Sy = Security
FM = Facilities Management

ANNEX 3C

RISK ASSESSMENT MATRIX

Risks to Defence capability are assessed for likelihood (of the risk being realised) and impact (if the risk is realised) against the Defence Board definitions, as detailed in JSP 892 and summarised below:

LIKELIHOOD	**H**	3	6	9
	M	2	4	6
	L	1	2	3
		L	**M**	**H**
		IMPACT		

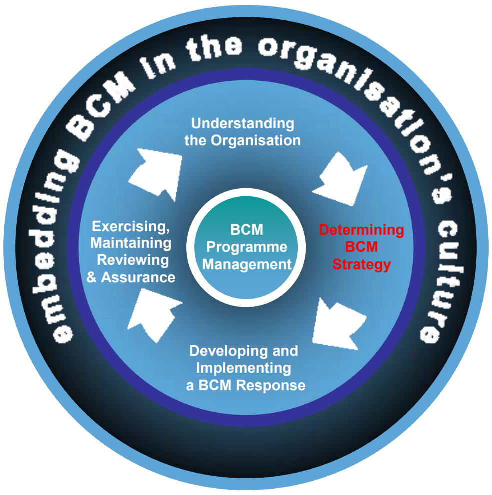
Definitions for LIKELIHOOD assessment:

HIGH	• 60% probability that the risk will occur. • More likely to happen than not. • Risk could occur within next calendar year.
MEDIUM	• 30-60% probability that the risk will occur. • About as likely to happen as not. • Risk could occur within next two to four years.
LOW	• <30% probability that the risk will occur. • More likely not to happen than to happen. • Risk could occur within next four to ten years.

Definitions for IMPACT assessment:

HIGH	• Major impact on achievement of Strategic Aim. Important reduction in performance. • Major management action required if the risk occurred.
MEDIUM	• Significant impact on achievement of Strategic Aim. Moderate reduction in performance. • Significant management action required if the risk occurred.
LOW	• Minor impact on achievement of Strategic Aim. Some effect on performance. • Moderate management action required if the risk occurred.

CHAPTER 4 – DETERMINING BCM STRATEGY


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

Introduction

4.1 This Chapter uses the work undertaken in Chapter 3 – Understanding the Organisation – to choose and develop the most appropriate Continuity Strategy to meet the needs of the organisation.

4.2 It is aimed primarily at TLB/TF Planners, although it may also prove useful to planners from subordinate organisations (e.g. HLBs) that may also be responsible for drawing-up BC Strategies.

4.3 The TLB/TF BCM Strategy should form part of existing management planning documentation and processes, and should be tackled alongside other generic risk management work.

4.4 Larger or more diverse TLB/TFs with a concentrated amount of critical business activity across a number of Business Units may find it useful for lower levels of the organisation (such as HLB Holders) to also undertake the BCM Strategy process. This is an acceptable approach; however, it is important to ensure that:

- BCM retains an appropriate level of attention at TLB/TF level.
- Regardless of any delegations adopted, TLB Holders and TF Chief Executives remain ultimately responsible for the delivery of appropriate BCM and planning within their organisation, and this responsibility may prove more difficult to discharge if not led from the top of the organisation.
- The linkage between BCM and other Corporate Governance work streams is maintained, and the handling of BC risks is aligned with the management of wider business risk.

Determining Strategy Options

4.5 In general, the approach to determining the Strategy (or Strategies) should:

- Implement measures to reduce the likelihood and potential impact of incidents;
- Take account of resilience and mitigation measures;
- Provide options for the continuity of critical activities during and following an incident;

- Take account of the activities which have not been identified as critical;
- Set out how relationships with key stakeholders and external parties will be managed during and after an incident.

4.6 TLBs/TFs (and HLBs as appropriate) should determine strategic options for their critical activities, and the resources that each activity will require upon resumption. The most appropriate Strategy will depend on factors such as the maximum tolerable period of disruption to critical activities (see Annex 3A), the cost of implementing a Strategy or Strategies and the consequences of doing nothing. Specific Strategies may be required for the following:

4.6.1 People – i.e. maintaining personnel core skills and knowledge (including stakeholders and contractors). This might include strategies for the multi-skilling of staff, the separation of core skills and succession planning.

4.6.2 Premises – to reduce the impact of the unavailability of the normal place of work. Strategies could include relocating to alternative premises/locations (including “budging-up”) within the TLB/TF or to facilities provided by another TLB/TF or third party[11]; working from home or at remote sites and the use of an alternative workforce in an established site.

4.6.3 Technology – Given the importance of the Information Technology (IT) systems to the delivery of Defence critical outputs, TLBs and TFs must understand the continuity and recovery time objectives for IT systems and applications. In the case of DII (Defence Information Infrastructure), ATLAS Consortium is responsible for agreeing with users a DII BC and Recovery Plan for each Defence site/establishment.

4.6.4 Information – to ensure that information that is vital to the organisation is protected and/or recoverable within timeframes identified in the BIA. This should include details of the appropriate method for copying and secure storage of information (physical/hard copy and virtual/electronic formats) at a safe location away from the normal work location.

4.6.5 Supplies – TLBs/TFs should maintain a list of core supplies that support critical outputs and activities. Strategies may include storage of additional supplies at another location; just-in-time or short notice delivery of stores/supplies; diversion of deliveries to other locations, and the identification of alternative sources of supply. As TLBs/TFs may be reliant on particular suppliers (often single sources of supply) for specific or specialist supplies, consideration should also be given to increasing the numbers of suppliers (or identifying alternative sources of supply); encouraging suppliers to have their own Business Continuity Strategies and Plans[12], and having contracts or Service Level Agreements in place with key suppliers.

[11] If staff are to be moved to alternative premises, these should be close enough that staff are willing and able to travel there (but not so close that they might be affected by the incident). Where alternate premises are provided by another TLB, or are to be shared with other organisations, the arrangement should be properly documented and agreed with all parties.

[12] Commercial Policy Statement on Business Continuity, Commercial Toolkit on the AOF

4.6.6 Stakeholders – when determining appropriate BCM Strategies, TLBs/TFs (and subordinate units) should consider the management of relationships with key stakeholders, industrial partners, contractors and suppliers.

4.7 Further suggestions on options for mitigating the risks in these broad categories can be found at Annex 5B.

Writing the BCM Strategy Document

4.8 A BCM Strategy need not be a long document, but it should contain at least the following:

- A high-level statement on the need for effective BCM and planning, referring to this JSP where appropriate.
- A statement on the resources required to deliver the Strategy.
- The roles and responsibilities for effective BCM and associated planning, including who will undertake the role of TLB/TF BC Focal Point and what their Terms of Reference will be (see Chapter 2 Annex 2A).
- An explanation of the linkage between BCM and other Management Planning, assurance, risk management and TLB Corporate Governance activity.
- A statement on BC priorities, drawing on the outcome of the Business Impact Analysis (see Chapter 3 Annex 3A).
- A statement as to whether lower level planning (HLB/Agency) is required, in addition to the mandatory Business Unit and Site planning.
- Instructions on how often BC Plans and Strategies should be exercised and reviewed.
- Statements on BCM training requirements and awareness activities.
- Details of any new delegations, or other BC-specific guidance, on the local handling of disastrous events.

4.9 There may be areas where managers need assurance that they are adequately empowered to take decisions in the event of an incident/emergency (e.g. managers feeling able to send staff home when it is obviously the best thing to do following an incident **but only if safe to do so with the agreement of the emergency services**). The BCM Strategy should include a statement on such matters, even if only to formally delegate resolution to a lower level as part of the Site Recovery Planning process. The overall aim is to enable all planners within the

TLB/TF to take as many decisions as possible in advance of a disruption taking place, thereby reducing the need for crisis management.

4.10 TLB/TF (and HLB) Planners may also find it helpful to consult each other, share experience and knowledge and compare Strategic approaches. This should help to ensure coherence, particularly with regard to inter-TLB/TF activities/service provision, between Strategies. A coherent BCM approach should allow TLBs/TFs to achieve the maximum recovery outcome for the minimum level of resources, thus reducing the overall effect of the disruption on the Department.

4.11 A BCM Strategy document check list is provided at Annex 4A, with further guidance on Strategy document contents and structure provided at Annex 4B.

BCM Strategy Endorsement

4.12 TLB/TF Holders are responsible for the delivery of appropriate and effective BCM and planning within their organisations (chiefly through the existing Statement of Internal Controls reporting mechanism). It is therefore appropriate that they, or their TLB/TF Management Boards, approve and sign-off the documented BCM Strategy. This provides top-level endorsement that the Strategy has been properly developed, and is adequate and appropriate to meet the needs of the organisation (particularly in relation to the delivery of critical outputs).

ANNEX 4A

BUSINESS CONTINUITY MANAGEMENT STRATEGY CHECK LIST

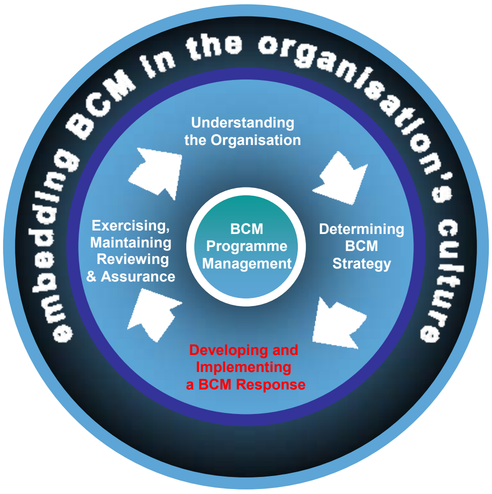
		Tick
1	Does your Strategy document make reference to the Departmental BCM (sub-)Strategy and JSP 503?	
2	Have you consulted widely within your TLB/TF to build-up your strategy?	
3	Have you used your Business Impact Analysis (together with your TLB Balanced Scorecard and/or Management Plan objectives/targets) to determine your BCM Strategy?	
4	Have you identified critical business functions and outputs and the minimum level of output necessary following a disruptive event?	
5	Have you prioritised these critical business functions for recovery?	
6	Does your Strategy take account of less time critical (or non-critical) activities?	
7	Does your Strategy meet the BC needs of your organisation, and the expectations of your stakeholders?	
8	Does your Strategy set out how relationships with key stakeholders and external parties will be managed during and after an incident?	
9	Does your Strategy set out the requirements for sub-ordinate level strategies and plans, and for exercising, maintenance and auditing?	
10	Is your strategy thorough? Does it include all the detail necessary to support lower-level BC planning?	
11	Does your Strategy identify the roles and responsibilities for effective BCM and associated planning, including who will undertake the role of TLB/TF BC Focal Point?	
12	Does your Strategy set out the TLB's/TF's requirements for BC training and awareness raising activities?	
13	Have you set out how the Strategy will be kept up to date?	
14	Have you made sure that the BCM Strategy is an integral part of your TLB/TF's normal business planning and risk management processes?	
15	Will it be endorsed/signed-off at an appropriate (TLB Management Board) level?	
16	Is your Strategy readable?	

ANNEX 4B

BCM STRATEGY DOCUMENT CONTENTS GUIDANCE

OVERALL APPROACH
TLB/TF/HLB BC Policy Statement
Strategy Outline
BC Focal Point Details
Degree and Level of Planning
Exercising and Plan Maintenance Regime
Linkage to Management Planning Processes
Linkage to Risk Management Strategies and Corporate Governance
Linkage to other TLB/TF/HLB/Site/BU BCM Strategies and Plans
BC Roles and Responsibilities, covering Planners, Senior Management, Focal Points and general staff.
Training requirements and awareness activities
Reporting Structures
CRITICAL BUSINESS
Business Impact Analysis Results
Prioritised Objectives & Outputs
Key Stakeholders and external parties

CHAPTER 5 – DEVELOPING AND IMPLEMENTING A BC RESPONSE


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

Introduction

5.1 This Chapter covers the development and implementation of appropriate plans and arrangements to ensure the continuity and recovery of Defence critical activities.

5.2 It explores some of the main BC issues faced by Business Unit (BU)[13] planners and provides step-by-step guidance on how to approach the task of developing Business Continuity and Site Recovery Plans.

Incident Management Plans (Emergency and Disaster Plans)

5.3 The purpose of an Incident Management Plan (IMP) (often referred to in MOD as an Emergency and Disaster Plan) is to allow the organisation to manage the initial phase of an incident, including:

- Containing and controlling the incident so as to minimise the effects to staff, environment and property;
- Implementing measures to protect staff and the environment from the effects of accidents;
- Communicating the necessary information to staff, the emergency services and authorities, and the public;
- Providing for the restoration and clean-up of the environment following an incident.

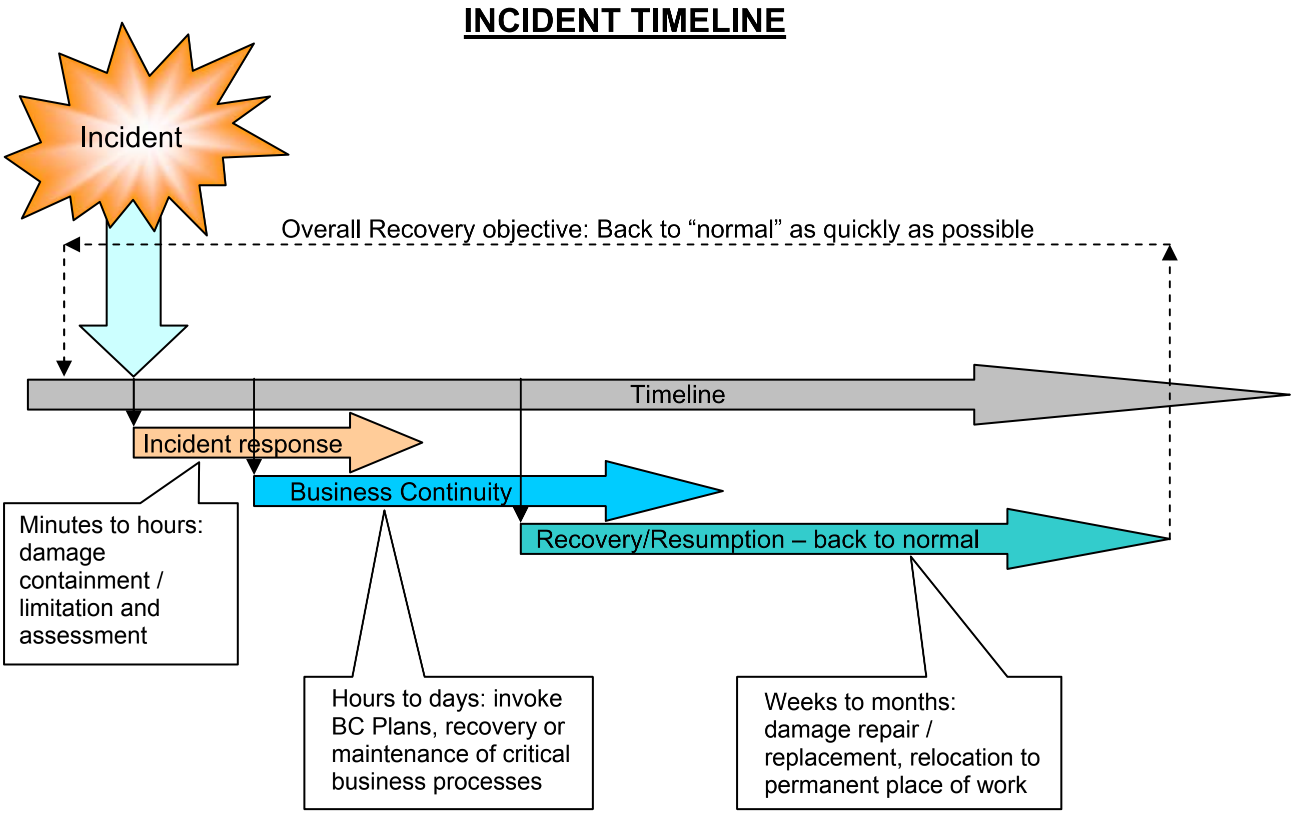
5.4 Further information on IMPs and Emergency and Disaster Planning can be found in JSP 375 Volume 2 Leaflet 1.

5.5 The responsibility for incident and business continuity management may be vested in a single individual or team, or in a tiered approach where different teams focus on incident management, business continuity and business recovery phases. These teams may themselves be supported by other teams with specific

[13] In this JSP, the term Business Unit (BU) covers a range of lower level organisations (normally the lowest level) and can include IPTs, Directorates and Units, and even whole establishments where they are small and all involved in the same basic output.

responsibilities for activities such as Facilities Management, IT and communications and HR/welfare issues. Both approaches can be effective as long as there is a strong linkage between the activities/actions required in each phase of an incident. In some cases, activation of the incident management, business continuity and business recovery plans may occur in rapid succession or even simultaneously.

Figure 3


INCIDENT TIMELINE
Incident
Overall Recovery objective: Back to "normal" as quickly as possible
Timeline
Incident response
Business Continuity
Recovery/Resumption – back to normal
Minutes to hours: damage containment / limitation and assessment
Hours to days: invoke BC Plans, recovery or maintenance of critical business processes
Weeks to months: damage repair / replacement, relocation to permanent place of work

Business Continuity Plans

5.6. It is important that any BU BC Plan is driven by the business priorities detailed in the TLB/TF BCM Strategy, or, where applicable, the subordinate HLB or Agency BCM Strategy. **The over-riding reason for conducting any BC Planning must be to ensure the safe and secure continuation of critical business activities and outputs in the event of a disruptive event or disaster**. It also important that BU BC (and Site Recovery) Plans are developed **to manage the impact of a disruptive event on the organisation's ability to deliver critical outputs, rather than focus on the cause of the disruption**.

5.7 The following documents (there may be others) will assist in the development of the BC Plan and ensure that it meets business needs:

- The Departmental BCM (sub-)Strategy, and this JSP;
- The TLB/TF BCM Strategy document (and the TLB/TF Plan as appropriate);

- If stipulated within the TLB/TF Strategy, the HLB or Agency BCM Strategy document;
- The Agency's Framework document;
- BU (or local area) Management Plan and/or Business Plan;
- If in existence, the current area/BU BC Plan and the current Site Recovery Plan;
- Relevant Incident Management and/or Emergency & Disaster Plans;
- Any other related recovery Plans, e.g. IT/IS.

5.8 BC Plans should contain the following elements:

5.8.1 Purpose and Scope. These should be well-defined, agreed with Senior Management and understood by those responsible for putting the Plan into effect. The BC Plan should detail the relationship with other relevant Plans or documents, and where these can be found. This section should also set out prioritized objectives[14] in terms of:

- the critical outputs/activities to be recovered;
- the timescales in which they are to be recovered;
- the (minimum) recovery levels needed for each critical activity; and
- the situations in which the Plan should be utilized.

5.8.2 Roles and Responsibilities. The Plan should set out the roles and responsibilities of the people/posts or teams that have authority during and following an incident. The BUs or Site covered by the Plan should also be clearly defined.

5.8.3 Plan Invocation. The Plan should identify the circumstances in which the Plan should be invoked, and by whom. It should also set out the process for standing down the team(s) once the incident is over.

5.8.4 Owner and Maintainer. There should be a primary owner of the Plan, and a nominated individual responsible for exercising, reviewing, amending/updating and re-issuing the Plan at regular intervals[15].

5.8.5 Contact Details. The Plan should contain essential contact details (not Home Address details) for key members of staff and stakeholders.

[14] This information can be determined through Business Impact Analysis (BIA) as set out in Chapter 3.

[15] Plans should be reviewed at least annually. They should also be reviewed after an incident, or when there is organisational change (including change of location), change of key personnel, or the introduction of new processes or systems (including IT).

5.9 In identifying local activity in support of TLB/TF critical outputs and processes, BUs must look carefully at exactly what they do that is truly critical to the successful completion of these outputs, and what aspects can realistically be omitted in times of crisis. It may be easier to do this on a post-by-post basis rather than team-by-team. It is unrealistic, and a waste of resources, to attempt to construct a BC Planning approach aimed at maintaining the full range of BU outputs, both critical and non-critical, regardless of whatever type of disaster might occur.

5.10 If, due to the nature of the TLB/TF's business, not all of the BU's critical activities can be decided upon in advance, mechanisms to identify the most critical activities in the event of a disruptive incident will be needed. This does not mean the burden on BU BC Planners (see Chapter 2 Annex 2B for ToR) is reduced, if anything their job becomes more complicated, as they must ensure their BU is capable of delivering any combination of the likely activities, in the required timeframe, which would be decided upon in the event of a disruptive incident. If this proves to be too complicated and costly, they must go back to the BCM Strategy Planner, and attempt to get a more precise picture of what critical activities will be required. **The underpinning concept behind BC is planning to continue critical business**, consequently, if during the planning phase it appears an organisation's approach cannot deliver this, the approach - including whether further resources are required - must be revisited.

5.11 Even if it is not clear whether a BU contributes towards the TLB's/TF's most time critical outputs and objectives (as set out in the TLB/TF BCM Strategy), a basic level of BC Planning is still necessary, for a number of reasons:

- Others need to be made aware that, for the purposes of BC planning, the BU is not deemed to be very time-critical. This allows Senior Managers and Site Planners the opportunity to develop the most effective local BC response, for example through the redeployment of BU manpower or resources to other more time critical BUs/areas.

- Confusion on the day will be reduced if all staff know where they and others stand in terms of business criticality.

- Even less time-critical activities need to be recovered eventually. Therefore, the BC Planning process and the resulting prioritisation of BU objectives will, in itself, aid recovery should a disaster occur.

- Priorities change and the BU may become very time-critical.

- The existence of a BC Plan, even an abridged version, leaves no one in doubt that BC Planning has taken place.

5.12 Once BU critical outputs and objectives have been established, BU planners may find it helpful to follow the Business Impact Analysis approach - as set out in Chapter 3 - to determine the priority order for their recovery, and the resources necessary to deliver them at a minimum level. It will be evident that not everything is needed immediately and that resources can be built up gradually in a phased manner. With regard to IT/IS, it is not enough to have plans in place simply to recover critical systems, the systems must be brought back within a certain timescale and in the correct order of priority so that the business recovery needs of the organisation (business units and/or sites) are fully met. This information will also be invaluable to Site Recovery Planners in enabling them to prioritise their recovery efforts to best match the BC requirement of all local BUs.

5.13 Few BUs will find it possible to develop a feasible recovery strategy without the active co-operation and assistance of neighbouring BUs, particularly where accommodation, services or other resources are shared within a building or on a site. It may therefore be useful to consult with counterparts in other BUs, even those from different TLBs, to ascertain their approach to BC Planning – including whether mutually beneficial arrangements can be put in place to pool certain resources following an incident, or to see if an agreement can be reached whereby work is transferred in times of local crisis.

5.14 Further guidance on the content of BC Plans can be found at Annexes 5A to 5C.

Site Recovery Plans

5.15 In the context of this JSP, “site” can mean a building, a group of buildings in the same general area, an establishment with a well-defined fence-line, or, where in close proximity, groups of establishments. Each geographical site will, in most cases, comprise a number of BUs, with some of them from different parts of the MOD, or from Other Government Departments (OGDs), other nations or commercial organisations. Some BUs may find themselves lodgers on a predominantly commercial site.

5.16 In order to maximise the amount of available real estate with which to work, and to reflect that incidents do not respect established boundaries, it is sensible and efficient (where practical) to consider “clustering” sites and buildings for BC Planning purposes[16]. For example, the two MOD HQ London buildings are covered by a single plan, but other London Defence sites (such as Army Barracks and TA centres) are not included in that plan.

5.17 Site Planners will need to examine their local circumstances and decide on the most effective way of defining a site for the purposes of writing a Site Recovery Plan. In particular, there may be synergies between certain buildings or sites, which would make it sensible for them to be covered by a single Site Recovery Plan, including:

[16] When considering the grouping of close buildings and/or sites for BC Planning purposes, care should be taken to ensure that local Emergency Service incident management procedures are taken into account. Any large scale incident attended by the Emergency Services will be managed in a predetermined way, with an inner and outer cordon raised around the scene (400m and beyond) to enable emergency work and/or investigations to continue unhindered. The local Fire, and/or Police Authority, or Local Authority emergency planning staff will be able to advise.

- Compatibility of IT & Communication Systems - can BUs be easily moved between different parts of the Site to achieve continuity of critical business – can critical staff use the facilities of their non-critical colleagues?[17]

- Diverse levels of business criticality - can a mixture of critical and non-critical BUs be covered by a single flexible Site Plan?

- Organisational similarities – if necessary, can non-business critical staff from one building undertake the critical work of others? And,

- Geographical proximity - can critical staff get to their new recovery location – even in the worst-case where local transport infrastructure has been disrupted?

5.18 The Site owner or the Defence organisation with the largest physical presence will, in consultation with site BUs, nominate an individual to be responsible for co-ordinating Site level BC Planning activity. The Site Recovery Planner (see Chapter 2 Annex 2C for ToR) will be responsible for gathering relevant information on local BU BC recovery requirements and developing the best possible Site Recovery Plan – one that best meets the BC needs and critical business requirements of the MOD as a whole. Where contractors are involved in the operation of a site, close liaison with the contractor and the relevant MOD Contract Manager (and/or Customer Focal Point) will be necessary to ensure that Site Planning across all organisational boundaries is coherent.

5.19 Those BUs who are lodgers on commercial, OGD, or other MOD sites, still have a responsibility for underpinning their critical business functions with effective BC Planning. Against this background they must ensure their BC requirements can be met within their Site owner's local BC Plans, or that they have developed their own plans.

5.20 Agreement also needs to be reached as to who should lead on implementing the Site Recovery Plan – the Site Recovery Manager – should an incident occur. It may be appropriate for the Site Planner to fulfil this role, or at the very least be a close adviser to the Site Recovery Manager and his/her supporting teams. The Site Recovery Manager will need expert advice and support in order to successfully implement the Site Recovery Plan – and therefore teams may need to be established to cover the main areas of implementation (everything from recovery of IT services to liaison with the media)[18].

5.21 Although responsibility for Site Recovery Planning falls to the Site owner, costs arising from BC Planning activity fall to those BUs benefiting from those

[17] Conversely, buildings in the same area may be dependent on the same (affected) IT/IS.

[18] The Site Recovery Planner, Recovery Manager, and members of any supporting teams, need to be able to focus completely on the effective implementation of the Site Recovery Plan should a disaster occur. Nominated personnel should not have critical business functions to carry out should an incident occur (or their critical duties must be covered by others in their absence on BC recovery duty). All such arrangements should be clearly outlined in the relevant BC Plans belonging to the BUs from which the personnel come.

arrangements. BC costs are part of the normal cost of doing business and should not be treated any differently from other business costs.

5.22 The content of **Site Recovery Plans is driven by the BC priorities of BUs normally resident on the site and those who may move to it if their site is denied to them because of a disaster.** A good Site Recovery Plan will:

5.22.1 In the short-term, enable as much, if not all, of the Site users' critical work to continue despite a disruptive event.

5.22.2 In the medium-term, help recover the Site back to a fully operational state, which includes restoration of IT and other systems, buildings and other infrastructure, and, where necessary, the provision of aftercare to any affected staff and/or their families.

5.23 Site Recovery Plans should be written for use 'on the day'. Background and supporting information that will not be required when the Plan is implemented should be included in annexes or in a separate document. Those implementing the Plan may be under significant pressure, or it may be that those who have to implement it are standing in for more experienced colleagues, so this should also be borne in mind. The use of diagrams, checklist guides and coloured pages will increase the 'user friendliness' of the Plan.

5.24 The Plan should be written around the time criticality phases that will be required to maintain or recover the business (see Chapter 3, Table 1), and ensure the delivery of Site-level resources necessary to maintain and restore critical business functions in the required timeframes. The time criticality phases should, where possible, correspond to those defined in the TLB/TF BCM Strategy, BU BC Plans and other related Plans (e.g. infrastructure providers).

5.25 BUs should work closely with the Site Planner to ensure that their BC requirements (i.e. recovery requirements in terms of accommodation, services, IT, communications and other equipment) are understood and are reflected (where possible) in the Site Recovery Plan. While the Site Planner's aim is to meet the critical business recovery aspirations of all BUs on-site, this may not prove possible (e.g. where BU requirements are so specific or bespoke that they cannot be met on-site, or where critical staff identified by BUs far outnumber the likely site resources available following an incident). In these circumstances, BUs will need to have investigated off-site solutions to their BC needs beforehand (reference to these alternative arrangements must be included in the BU and Site Plans). This may lead to a planning assumption being adopted that would see a small number of BUs moving to another site after a disaster in order to make the BC Planning for the rest of the site viable. Any disputes that cannot be resolved at local level should be escalated. In many cases the most logical course of action will be obvious – i.e. where a BU is a minority lodger on a large site operated by another TLB/TF, the lodger should have an agreed BC solution with its parent TLB/TF on one of their core sites.

5.26 It is important to identify exactly what degree of impact will trigger the invocation of Site Recovery Plans and related processes, and who will make that decision: everyone must be clear on how an incident escalates to an emergency, and from there to a disaster. It is likely that different personnel and Management chains will be involved at each level. There must therefore be clarity as to when one Plan and responsibility starts, and another finishes. This clarity will help remove indecision, and with it delay, and permit the recovery of critical business functions as quickly as possible.

5.27 Further guidance on Site Recovery Planning can be found at Annexes 5D to 5G.

ANNEX 5A

WRITING THE BUSINESS CONTINUITY PLAN

5.A.1 The BU BC plan does not need to be a long document. The success of the plan will depend upon how easily and quickly it can be followed in sometimes pressurised situations. The following are some useful guidelines:

- Keep the plan simple as complexity is likely to hamper the response.
- Use diagrams and checklists instead of lengthy text.
- Design the Plan for 'on the day' use, rather than being full of supporting background material.

5.A.2 However, it does need to cover the following areas:

- Statement on the need for effective BCM and Planning, referring to this JSP and Departmental/TLB/TF/HLB BCM Strategies where appropriate.
- State where responsibilities lie for effective BCM and associated Planning.
- Contact details (but not Home Addresses) for those with roles and responsibilities under the Plan.
- Where possible, incorporate flowcharts detailing the process to be followed.
- Statements about BC priorities, with reference to the local BCM Strategy and Management Plan, detailing:
  - The functions (if any) which are undertaken in support of identified TLB critical defence outputs and activities.
  - The minimum level of resources, including the identification of those resources, required to deliver these functions across the period of recovery.
  - Whether contingency plans exist (and are adequate) for corporate or other critical IT and communications systems.
  - The local BC risks, and what risk reduction or mitigation measures, if any, are being taken.
- Planned BC communication and awareness activities, including testing and exercising of local arrangements.
- The requirement for and frequency of BC training, and staff attendance at local BC awareness events.

- How often the BC Plan should be reviewed.

- How the BC Plan interacts with other plans (Emergency Plans, Site Recovery Plans, etc.), and where division of responsibility lies.

- How personnel with BC responsibilities interact with others on site (e.g. Heads of Establishment, MDPGA, DIO/Facility Managers, Commanding Officers, etc.), and where responsibilities lie, including any new delegations (or other BC-specific guidance) on the local handling of disastrous events.

- How the Business Unit would respond should a disaster occur, linked to the provisions within the local Site Recovery Plan and Incident Management Plan. This should not only detail how critical outputs and systems will be recovered but also how staff will be informed and supported. It should also highlight where individuals are involved in implementing the local Site Recovery Plan and (where appropriate) how their normal critical day-to-day duties are to be undertaken in their absence.

The Extent of Business Interruption

5.A.3 All Business Unit Planners should note that all BC Plans should include arrangements for **local incidents** that do not require the invocation of wider site BC arrangements. Examples of these may be power failures, localised flooding and unexpected loss of key personnel.

5.A.4 Regardless of how much planning is undertaken it is not possible to prepare totally for every possible eventuality. Therefore, should a disaster occur, Managers will need to remain flexible and react to prevailing conditions, tailoring their BC recovery response in light of the actual impacts of the event.

Protective Marking

5.A.5 BU BC Plans and other related recovery plans should be protectively marked in accordance with the instructions contained in JSP 440. Where possible though, and to ensure that they can be made easily accessible to staff - particularly during an incident, BU BC Planners should aim to keep the classification no higher than Restricted.

Data Protection

5.A.6 Within most, if not all, Plans it may be necessary to include personal information (names, telephone numbers, etc. – but not home addresses), and it is likely that elements of the Data Protection Act will apply[19]. Planners will need to ensure that any personal data is properly safeguarded, only used for the purpose

[19] JSP 400 refers. See also 2010DIN05-065 Requirements for Privacy Impact Assessments (PIAs)

collected, and that any statements required to conform with the Act are included within Plans. Further information can also be found in the Cabinet Office publication "Data Protection and Sharing – Guidance for Emergency Planners and Responders"[20].

Check Lists

5.A.7 Once a draft BU BC Plan has been produced, Planners may find it useful to go through the check list at Annex 5C and contents guidance at Annex 5G.

Further Assessments

5.A.8 If the BC Plan being invoked results in a significant change in working practices, whether in terms of location or ways of working, further assessments may be required. These may include a workplace H&S risk assessment or, if the BC Plan requires staff to work at home for a lengthy period of time, it may be necessary to undertake a risk assessment, Occupational assessment and Security assessment on the home location to fulfil the MOD's obligation to its staff. Further information can be found in JSP 440, the Defence Manual of Security, and JSP 375 Health and Safety Manual.

5.A.9 BC Plans must also take full account of both the legal and MoD Policy requirements in respect of Equality and Diversity issues. The EADIAT (Equality and Diversity Impact Assessment Tool)[21] should be used by Planners to ensure that BC Plans have been developed and written in accordance with legal requirements, that they take account of MoD Policy on Equality and Diversity and that the Department's business is as inclusive as possible.

[20] http://www.cabinetoffice.gov.uk/resource-library/data-protection-and-sharing-%E2%80%93-guidance-emergency-planners-and-responders

[21] http://defenceintranet.diiweb.r.mil.uk/DefenceIntranet/Library/CivilianAndJointService/BrowseDocumentCategories/Personnel/EqualOpportunitiesAndDiversity/EqualityAndDiversityImpactAssessmentTooleadiat.htm

ANNEX 5B

BC PLANNING REQUIREMENTS & OPTIONS

Security

5.B.1 Security regulations covering the movement and handling of classified material are contained in JSP 440. BC Plans must comply with JSP 440 unless prior agreement has been given by the appropriate security authority to do otherwise.

Alternative/Emergency Accommodation & Furniture

5.B.2 Some BUs may be able to secure alternative office accommodation at locations operated by internal or external suppliers and/or customers: for example DE&S teams may be able to agree to have certain key personnel operate temporarily from their contractor's premises, or their primary Military customers may be willing to offer some temporary accommodation if it improves the chances of continuity of service. There might also be scope for BUs distant from each other to agree some form of reciprocal arrangement whereby each is prepared to house the critical staff of the other should a disaster occur.

5.B.3 Structural and damage assessment engineers can be engaged either through the Regional Prime Contractor or Principal Support Provider Contract implemented by Defence Estates. Further guidance can be provided by Defence Infrastructure Organisation (DIO).

5.B.4 Enquiries concerning emergency accommodation requirements should, in the first instance, be directed to the DIO Secretariat Directorate. If DIO is unable to assist from within their own holdings, they should be able to act as a broker with other potential government accommodation providers, such as the Crown Estate. The most time-consuming part of acquiring any property is negotiating the lease and associated legal documentation. Accommodation acquired from another Government source can normally be occupied in a much shorter space of time as all parties are part of the Crown, and therefore are classed as the same single legal entity for the purposes of legal title, thus significantly simplifying the paperwork.

5.B.5 Office furniture can be acquired through framework contracts managed by Buying Solutions (BS). Security furniture can be purchased through Security Services Group (SSG) part of DIO. Further information on both can be found in JSP 384 Defence Accommodation Stores Policies and Procedures, Volume 1 (Part 1), Chapter 3 – Supply Arrangements.

5.B.6. General stores, ranging from curtains to cookers can be procured via DE&S's Medical & General Supplies IPT (MGSIPT).

Hot Sites and Warm Sites

5.B.7 With unlimited resources, it would be very much easier to develop a BCM Strategy covering the vast majority of potentially disruptive events: simply establish a duplicate facility, with all the necessary equipment, data and trained staff, and have it sitting empty waiting to be used if and when needed. This is known as a "Hot Site", and for a small number of private sector companies this approach makes sound business sense. Other organisations use "Warm Sites", facilities that are partially equipped and so provide the opportunity for a relatively quick recovery after some additional preparatory work has been completed to make the facility useable.

5.B.8 It is unlikely that MOD BUs will be able to make the business case for a Hot Site arrangement, but some BUs may be able to explore Warm Site options as part of their BC recovery planning. Another option is for an arrangement between sites (or BUs), whereby staff doing lower priority work on an unaffected site make way for staff from a disrupted site whose work is of higher priority to Defence.

Working From Home or Elsewhere

5.B.9 Much will depend upon the type of critical work that needs to be undertaken, but for some BUs it may be possible to consider having some staff work from home as part of their BC recovery planning. Placing copies of key documents at home may also be appropriate. Alternate/home working arrangements must be in accordance with the relevant Security and Health, Environment and Fire Policies[22].

Transfer of Critical Work/Functions

5.B.10 Rather than try to underpin critical work locally, it may be possible for BUs to agree to transfer responsibility for critical outputs to another more distant BU capable of absorbing the task, perhaps at the expense of their own non-critical work. For example, it might be possible and more cost-effective, to plan on transferring the critical elements of a Policy/Secretariat function temporarily from Whitehall to the PJHQ at Northwood. Some cross training, and perhaps other work to permit access to critical data, will probably be necessary to make this type of approach work.

Critical IT, Communications & Other Systems[23]

5.B.11 Contingency planning for critical IT, communications and other systems, for Business Continuity purposes and more generally, is the responsibility of the relevant System Service Manager who should consult with DISS (in DE&S). Central guidance for use by these managers is published as part of JSP 602[24], and includes direction on how to approach contingency planning.

5.B.12 Some form of basic contingency planning, for service continuity purposes, should already exist for all systems, but BUs will need to check with their respective Service Manager that contingency measures are adequate and meet the critical BC needs of the organisation. If there is a gap between requirement and capability then this will need to be filled, either through an improvement in the level of contingency, a workaround established (perhaps a paper-based process as a short-term stop-gap),

[22] JSP 440 (Security) and JSP 375 (Health & Safety)

[23] This section will be updated in due course

[24] JSP 602 – Information Coherence Directions – Directions and Guidance / Managed Services / Business Continuity

or a reappraisal of the BC requirement to see whether the level of recovery can be reduced.

5.B.13 Smaller systems may exist which are managed locally and deemed critical for BC purposes. Local contingency planning should be based upon central guidance and best practice as published in the JSP 600 series (Information Coherence Directions).

5.B.14 While access to the Internet from MOD IT systems has traditionally been a "nice to have" rather than a critical enabler, in some parts of the Department use of the Internet is very much part of business or operational procedures (e.g. DE&S Project Teams' contact with Defence contractors), and the loss of connectivity could result in considerable business disruption. In these areas, BC plans should be developed to enable the continuation of critical activities after the loss or partial loss of external connectivity. Options could include: the use of telephone/facsimile; use of standalone internet accounts/computers (i.e. those which are completely separate from MOD IT/IS connections).

Manual/Paper-Based Workarounds

5.B.15 MOD BUs have become more and more reliant upon their IT systems, either because all of their key data is invested within these systems, or because key processes have now been automated and alternative ways of working no longer exist. For many, the potentially long-term loss of IT services therefore represents a major risk to continuity, and total reliance upon IT system contingency plans may not be prudent.

5.B.16 As a result, BC Planners and local Management may find it fruitful to explore, as a contingency, alternative ways of working should IT systems fail or should staff find themselves working elsewhere where access to IT, or at least the necessary specialist or bespoke applications, is restricted. Any workarounds that are developed need to be regularly tested, not only to ensure that they work but also to give staff the chance to practice their implementation and to get used to working in this different way.

Battle-boxes (Data Stores)

5.B.17 Access to key data (in paper or electronic form) is likely to be vital for the continuation of critical business activity following disruption. Some BUs may wish to consider storing a certain amount of key data off-site so that it may be accessible to the BU should a local disaster occur. As a disruptive event could affect the availability of MOD IT/IS (DII), consideration should be given to storing laptops and (encrypted) USB sticks which have business-critical documents/data pre-loaded on them. Examples of data/information for a Battle-box (data store) might include: Policy and Reference documents; Reports; Submissions; PQ answers/templates; BC Plan; Telephone/Email Contact Lists for key MOD personnel and other business contact details. **The data stored in the Battle-box must be kept up-to-date if it is to be of any use in an emergency.**

5.B.18 Such an approach will not suit everyone. Those reliant upon data which is constantly changing (see Grab-bags below), or those dealing with significant amounts of data, will not easily (or cheaply) be able to replicate this data off-site in a meaningful way, but for some BUs this may be an appropriate BC planning option.

5.B.19 In exploring this approach it should be remembered that many disruptive incidents will involve the call-out of the Emergency Services, and in dealing with such incidents the normal protocols involve the erection of cordons, which can extend 400m or more from the affected area depending upon the circumstances. In some cases, there may be no damage to the site but access could be restricted or denied for long periods of time (e.g. Police preservation of a crime scene). Therefore, careful thought needs to be given as to the location of Battle-boxes, so that they are far enough away not to be affected by a cordon, but close enough to allow staff easy, secure and relatively quick access.

Grab Bags

5.B.20 Grab-bags are similar to Battle-boxes, but are small portable stores of key data or equipment [25] which should be held within the BU so that they can be easily grabbed by personnel if and when an emergency occurs (e.g. such as a fire alarm)[26]. Should reoccupation not be possible (and it is worth reminding staff that they should assume all directives to evacuate a facility are genuine and that re-entry may not be possible for some time) then the BU has access to key material to allow critical activity to continue elsewhere.

5.B.21 This approach can be a bit limited as it is only of any use if personnel are in the building when the emergency occurs and are able to gain easy access to the Grab-bags (personnel should not delay their evacuation of the building in order to collect Grab-bags); however, it is probably easier to ensure that the Grab-bags contain the very latest information/data, particularly if the data changes frequently. To ensure that critical activities can continue following disruption (both during and outside of office hours), BUs may wish to have both a Battle-box and Grab-bags. An individual (or individuals) should be responsible for ensuring that the contents of the Grab-bags are kept up-to-date.

Cross Training of Staff

5.B.22 In order to provide a greater level of 'personnel resilience', Managers and Planners might also wish to consider whether additional local cross training is called for. If a small amount of critical work is undertaken by one or only a handful of people, there is an inherent risk to continuity in having so much vested in so few individuals, particularly if they are all located closely together. If a disaster were to strike their part of the building, would it be possible to continue to deliver the BU's critical outputs without them? At the very least, consideration should be given to having these individuals put together some hand-over notes, desk instructions or standard operating procedures, and to keep them up-to-date. This need not involve

[25] JSP 440 sets out Departmental Policy relating to laptop computers

[26] This approach should also be followed for personal items (house keys, travel cards, money etc) as well, in case staff are sent directly home from the external assembly point

a great deal of extra work, as if this work is so critical then there are likely to be reports already compiled on a regular basis – therefore you need only ensure that the information can easily be found in the aftermath of a disaster, permitting alternate staff to 'hit the ground running' and maintain continuity of critical business.

Shadows and Stand-ins

5.B.23 Finding the right staff to cover critical posts at short notice has now been made much easier. As part of the Civilian Annual Staff Reporting process, staff are required to complete competency-based Personnel Skills Profiles and to have Post Profiles (completed by Line Managers) for the post they fill. Following the launch of the Civilian Casualty Information Service (CCIS)[27] on HRMS in September 2007, it is now possible for Civilian Staff – and for Military Staff with accounts on HRMS – to have their post's business criticality recorded (see Chapter 3 Table 1 for criticality categories). CCIS enables staff with a recorded BC role (and subject to appropriate authorisation[28]) to access Personnel Data in the event of an emergency (or as part of normal BC Planning and exercising processes) – including the identification of staff with the required skills to replace incapacitated or missing staff for business critical posts.

Legal Obligations to Staff

5.B.24 Whatever options are explored, managers must remember that they and the Department retain responsibility for ensuring that all staff, wherever they are required to work, have a right to a safe working environment, and the tools necessary to undertake whatever tasks are expected of them. Unless dispensation has been agreed with relevant Policy Branches and, where necessary, the Trades Unions, BC Plans must adhere to all relevant employment rules, regulations and UK and European Law.

[27] DIN 2007 DIN 01-043 – PI 104/07 Civilian Casualty Information Service (Level 1)

[28] See Policy, Rules and Guidance – Accessing Information in the Event of an Incident or Emergency.

ANNEX 5C

BC PLANNING CHECK LIST

		Tick
1	Have you identified the owner of the Plan, and who is responsible for reviewing and updating it?	
2	Does your plan set out the roles, responsibilities and authority of individuals during and after an incident (for example, those responsible for dealing with internal and external (media) communications)?	
3	Have you used your parent TLB, HLB or Agency BCM Strategy document and JSP 503 as a guide to determining your BC requirements, local critical business functions and critical staff?	
4	Have you identified the criticality of your business functions and outputs as per the BCM Strategy?	
5	Have you prioritised all of these business functions?	
6	Have you phased your recovery requirements accordingly – what needs to be operational straight away and what can wait a few days or weeks?	
7a	Have you identified the minimum resource levels required to maintain critical work…… in terms of manpower?	
7b	…… in terms of basic accommodation?	
7c	…… in terms of IT and communication services?	
7d	…… in terms of key data and files?	
7e	…… in terms of specialist facilities?	
7f	…….in terms of essential materials, spares and consumables?	
7g	…….in terms of essential services and utilities (power, water etc)?	
8	Have you identified critical business systems (e.g. IS/IT), and checked that contingency plans for these systems meet your minimum service requirements?	
9	Have you explored paper-based ways of working as a fallback to the loss of IT or other systems?	
10	Have you identified how the plan would be invoked, by whom and in what circumstances? Have you also set out the stand-down arrangements?	
11	Have you considered a localised incident, one that will not invoke your Site Plan?	
12	Have you undertaken an exercise to assess risk?	
13	Have you identified ways to manage or mitigate risks identified?	
14	Have you explored the provision of Hot and/or Warm Sites as a BC option?	
15	Have you looked at off-site storage options, and/or ‘Grab Bags’?	
16	Have you explored the possibility of transferring critical work elsewhere in the event of a BC incident?	
17	Have you considered whether your succession plans might assist in filling critical posts, or whether cross-training of staff within the BU may be necessary?	
18	Does your plan include essential contact details, e.g. for key stakeholders and service providers?	
19	Have you liaised with other BUs and Site Recovery Planners?	

		Tick
20	Are you content that the Site-level support assumed in your plan can be delivered by the Site Recovery Planner?	
21	Have you identified the fall-back location(s) for your BU?	
22	Does your plan provide for the welfare and safety of staff?	
23	Is your Plan readable?	
24	Does your plan fit in with other local plans and Management publications?	
25	Do you have a strategy for testing your Plan (and people) and keeping it up to date?	
26	Do you have a strategy for maintaining awareness of BC Planning arrangements within your BU?	
27	The Plan is structured as per the BU column of Annex 5G.	

ANNEX 5D

WRITING THE SITE RECOVERY PLAN

5.D.1 Site Recovery Plans should include the following:

- A short statement on the need for effective BC Planning, referring to the TLB/TF BCM Strategy where appropriate.

- A statement on where responsibilities lie for effective Site Recovery Planning.

- The level of impact that constitutes a disaster, and who is empowered to make the decision to invoke the Site Recovery Plan.

- Details of any plan phases and/or timescales.

- The roles, responsibility and management structure of the group(s) responsible for the efficient management of and recovery from a disaster or incident. The group(s) should be able to manage the following areas:

    - Personnel and Welfare.
    - Security.
    - Damage Assessment.
    - Facilities Management.
    - Finance.
    - IT and Communications.
    - Press, stakeholders, and other disaster-related liaison.
    - Logistics.

- Details of the critical staff, systems and business functions resident on the site, and how and in what order they are to be recovered; and

- Details of how the Plan is to be exercised and maintained (see Chapter 6 for more detailed guidance).

5.D.2 Annex 5F provides a check list covering the issues raised in this Chapter, and Annex 5G provides contents guidance for Site Recovery Plans.

ANNEX 5E

SITE RECOVERY PLANNING – DETAILED GUIDANCE

5.E.1 The Site Recovery Planner will need to gather information from a number of sources before attempting to construct a Site Recovery Plan, primarily:

- Drawings etc of the site showing the location of buildings, services (water, gas, electricity) and other key facilities (including sensitive or potentially dangerous areas, e.g. chemical stores);
- All BC Plans belonging to BUs operating within the scope of the Site Recovery Plan, and details of a focal point in each with whom to liaise;
- All Emergency Plans (e.g. Fire Evacuation) – or other relevant SOPs – in force on the site, including arrangements for the handling of CBR[29] attacks, and details of key individuals such as the Commanding Officers/Heads of Establishment, Head of Security, Head of Safety, etc;
- All other Contingency Plans (e.g. for IT systems) in force on the site, or access to the relevant service provider(s);
- Security Plan(s) in force on the site, or access to the local security adviser(s);
- All other site-level plans, including statutory ones (e.g. MACR[30]), or access to the relevant experts who are willing to provide advice.

5.E.2 Site Planners also need to acquire information on relevant external contacts with whom they must liaise, including the local authority Emergency Planning Team, Focal Points within the Emergency Services (primarily Police and Fire and Rescue Service), and the regional Welfare Advisers of the Occupational Welfare Services (OWS). If the site is shared with non-MoD organisations (including contractors) their needs must also be taken into account.

Key Data and Information

5.E.3 Technology improves efficiency, but loss of electronic data and other information can reduce output to virtually zero. Planners should ensure that key information needed in the hours following a disaster is, as far as is practicable, available in the form of back-up disks, is on alternative servers or in hard copy. Also, where reliance on key telephone lines and/or mobile phones is high (in terms of managing recovery activity) steps should be taken to ensure that they operate as expected under all circumstances.

[29] Chemical, Biological and Radiological material.

[30] Major Accident Control Regulations.

5.E.4 Site Planners must also check that contingency measures are in place for any corporate or other local IT, communications or other systems deemed critical (see Annex 5B).

Site Recovery Options

5.E.5 The range of BC recovery options available will be dictated by the type and size of site, and the amount of critical activity within it. For example, Planners on a large green field site might feel confident in assuming that most potentially disruptive incidents are likely to only affect part of the site, leaving the unaffected area available for the re-housing of critical staff. Others planning for single buildings or more compact sites might feel that their options are significantly reduced.

5.E.6 It is important that the Site Recovery Plan dovetails with all other extant site-wide plans. Site Planners need to liaise closely with other stakeholders on-site to ensure that all local inter-related planning is taken forward in a coherent manner. For example, the interface between BC Plans and Emergency Plans is very important, as emergencies may develop into business continuity events.

Site Recovery Teams

5.E.7 Prudence dictates that there should be at least one nominated “replacement” for each Site Recovery Team member. Consideration should also be given to the location of Site Recovery personnel during implementation of the Plan (e.g. where the Recovery Command Centre is to be located) and, bearing in mind that all or part of the site may be inaccessible as a result of the incident, alternate locations. In addition, there may be a need to sustain the recovery effort for an extended period.

5.E.8 A watch keeper should be appointed to record in a log all key decisions and actions taken by the Recovery Teams. The log will be useful during the recovery phase, and will be invaluable later for evaluating the success of the recovery, and in dealing with any formal or informal inquiries, and audits.

Empowerment

5.E.9 Consideration should be given as to how disaster recovery staff are going to be empowered to enable them to act quickly, and in the best interests of the Department, should a disaster occur. For example, in the hours and days following a disaster, expenditure should not necessarily be constrained on grounds of affordability, particularly where staff welfare issues are being addressed. It is nonetheless essential that other forms of scrutiny be applied, to the extent possible in the circumstances. These include scrutiny of the requirement; ensuring that propriety and regularity are observed, proper records are kept, and that value for money is achieved.

5.E.10 The scope of the delegated authority required to empower individuals must be clearly defined. Letters of Delegation can be used to achieve this. They should set out the conditions in which the delegated authority will be invoked, the scope of the authority and any Corporate Governance requirements that might apply.

Emergency Planning Arrangements

5.E.11 Sites that hold large enough quantities of dangerous substances to trigger the minimum threshold requirements of MOD's Major Accident Control Regulations (MACR) should have more developed Emergency Planning provisions than is the norm. BC staffs at these locations should therefore take care to ensure that their BC-focused plans are complimentary to existing MACR[31] Plans. Where there is conflict, MACR requirements take primacy.

Communications

5.E.12 Personnel on the Site, those in the command chain and in the wider MOD, and stakeholders (internal and external), will wish to know what is going on, and the Plan should have a strategy for dealing with all of these audiences. It may be decided that individual BUs should deal with managing the expectations of their own specific stakeholders, but it is likely that a more co-ordinated approach will be needed - particularly with external communications with the local and/or National Press. The Site Recovery Plan should state clearly who will be responsible for internal communications, for the management of the interface with the media, and for any enquiries from distressed relatives and other stakeholders.

5.E.13 It is important that if an incident occurs the organisation affected can provide timely information bulletins to staff and to wider MOD audiences and, if necessary, a statement to the media (as the media can provide valuable support in a disaster situation). For these reasons, Site Plans should contain basic templates for internal and external bulletins and statements. A range of template statements may be required to cater for the types of incident in which the media might take an interest - ranging from a catastrophic event on a site, to more minor incidents such as protests blocking access to a site or the local disruption of power supply.

Personnel and Welfare

5.E.14 Welfare issues are often overlooked by organisations new to BCM, and for many it is viewed as a secondary activity behind the restoration of infrastructure and systems. Should a serious incident occur, and BC Plans be invoked, everyone will be affected. Even if there is no loss of life, the emotional upheaval of such an event may take its toll. Personnel and Welfare staff locally should be encouraged to do as much preparatory work as possible to ensure that should the worse happen, suitable internal and external resources can be brought to bear.

5.E.15 It is likely to be frantic in the first few hours and days following an incident and everyone will be focused on getting their particular job done. It will be stressful. Site Planners will need to consider the following issues with regard to their recovery staff:

- Has enough manpower resources been allocated to the recovery task, enough to ensure undue pressure does not fall on key recovery personnel?

[31] JSP 498 refers.

- Do arrangements need to be made for meals or other facilities or services?

- Is it likely, at least initially, that the recovery effort will be a 24 hour activity – if so, additional / alternate staff may need to be found?

ANNEX 5F

SITE RECOVERY PLANNING CHECK LIST

		Tick
1	Have you used local BU BC Plans, the TLB/TF BCM Strategy and JSP 503 as a guide to determining your Site's BC recovery requirements, and made adequate reference to these documents?	
2a	Does the scope of your Plan take account of: ... the mixture of critical and non-critical BUs on the Site?	
2b	…the compatibility of IT and Comms systems across the Site?	
2c	…organisational synergies across the Site?	
2d	…geographical proximity for fall-back options, in particular to ensure that they will not be impacted by the likely location of Emergency Service cordons?	
3	Does your plan detail all critical staff and/or functions?	
4a	Have you identified the minimum recovery levels required to maintain critical work on Site…in terms of manpower?	
4b	…in terms of basic accommodation?	
4c	…in terms of IT and communication services?	
4d	…in terms of key data and files?	
4e	…in terms of specialist facilities?	
4f	…in terms of essential materials, spares and consumables?	
4g	…in terms of essential services and utilities (power, water etc)?	
5	Have you liaised with on-Site contractors, and those with FM or other site-wide responsibilities?	
6	Have you phased your recovery requirements – identified what needs to be operational straight away and what can wait a few days or weeks?	
7	Have you planned against a small number of potential impacts, rather than a large range of specific events (effects not causes)?	
8	Have you undertaken an exercise to assess risk?	
9	Have you identified ways to manage or mitigate risks identified?	
10	Does you plan clearly spell out responsibilities, roles, and accountability, and does it explain the escalation process from incident to emergency to disaster, and how BC Plans are to be invoked?	
11	Can you meet the recovery aspirations of all local BUs? And if not have you told them?	
12	For those not catered for, does your Plan list what BC recovery action they are taking on their own behalf?	
13	Do you have a strategy for internal and external communications (including the Press and other stakeholders), and have you identified the staff responsible for dealing with these issues?	
14	Have you identified key external contacts (Emergency Services, Local Authorities, etc.) and detailed them within your Plan?	
15	Does your Plan set out the process for standing down once an incident is over?	
16	Is your Plan thorough? Does it include all the detail necessary to permit recovery of your Site?	
17	Is your Plan readable?	

		Tick
18	Does your Plan fit/de-conflict in with other local Plans and Management publications?	
19	Do you have a strategy for testing your Plan (and recovery team(s)) and keeping it up to date?	
20	Do you have a strategy for maintaining awareness of BC Planning arrangements within your Site?	
21	Has a suitable Site Recovery manager been appointed?	
22	Have support teams been identified and properly resourced?	
23	Have you identified alternative support team members?	
24	Have you thought about the physical needs of your recovery personnel (food, etc.), especially if recovery work needs to be on a 24-hour basis?	
25	Do you have a base of operations – a Recovery Command Centre – and is it properly resourced?	
26	Is there an alternate Recovery Command Centre should the incident occur close-by?	
27	Have you nominated a watch keeper to keep a formal record of the Site Recovery?	
28	The plan is structured as per the Site column at Annex 5G, and contains Recovery Support Team details as per Annex 5H.	

ANNEX 5G

BC DOCUMENTS – CONTENTS GUIDANCE

The following should be used as a guide to what should be included in each of the three main BC documents.

	STRATEGY	BCP	SITE
OVERALL APPROACH	●	●	●
TLB/TF/HLB BC Policy Statement	●		
Strategy Outline	●		
BC Focal Point Details	●	●	●
Degree and Level of Planning	●		
Awareness Strategies	●	●	●
Exercising and Plan Maintenance Regime	●	●	●
Linkage to Management Planning Processes	●	●	●
Linkage to Risk Management Strategies and Corporate Governance	●		
Linkage to other TLB/TF/HLB/Site/BU BCM Strategies and Plans	●	●	●
BC Roles and Responsibilities, covering Planners, Senior Management, Focal Points and general staff	●	●	●
Levels of Financial and other Delegations	●	●	●
Reporting Structures	●	●	●
Flow chart showing the process to be followed		●	●
CRITICAL BUSINESS	●	●	●
Business Impact Analysis Results	●	●	●
Prioritised Objectives & Outputs	●	●	●

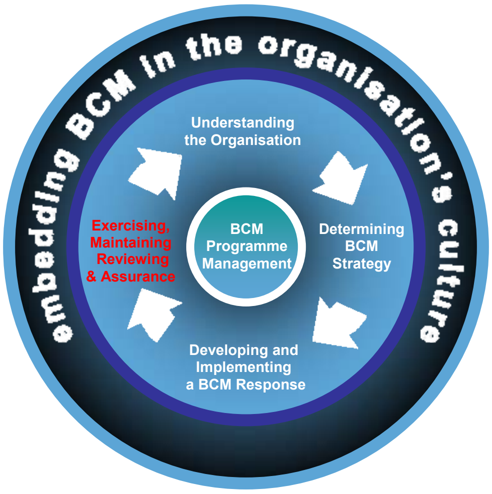
RESOURCE REQUIREMENTS		●	●
Teams and Individuals		●	●
Business Units			●
Sites		●	●
Processes		●	●
Data		●	●
Materials, spares, consumables		●	●
Essential services, and utilities		●	●
IT, Comms & Other Systems		●	●
Off Site Arrangements, where appropriate		●	●
PLAN INVOCATION		●	●
Trigger Arrangements / Stand Down		●	●
Planning assumptions (e.g. effects not causes)		●	●
Key Recovery Personnel		●	●
Call Cascade Data		●	●
Communications, including Management of Stakeholder Expectations/Relations		●	●
Site-level Liaison Arrangements		●	●
Critical Business Recovery Checklists		●	●
Arrangements for Transfer of Critical Work		●	●
Longer-Term Recovery Arrangements			●
Recovery Support Teams (See Annex 5H)			●

ANNEX 5H

RECOVERY SUPPORT TEAM PLAN CONTENTS

	DAMAGE ASSESSMENT	PERSONNEL & WELFARE	SECURITY	LOGISTICS	FACILITIES MANAGEMENT	FINANCE	INFORMATION TECHNOLOGY & COMMUNICATION SYSTEMS
Action Plan	●	●	●	●	●	●	●
Roles and Responsibilities	●	●	●	●	●	●	●
Resources	●	●	●	●	●	●	●
Check lists	●	●	●	●	●	●	●
Access to Key Data	●	●	●	●	●	●	●
Liaison with key Groups	●	●	●	●	●	●	●
Strategies for protecting damaged sites/facilities			●		●		
Strategies for protecting sensitive data			●				
Strategies for supporting staff (counselling, etc.)		●					
Liaison with shipping companies				●			
Strategies for moving large amounts of people /equipment over potentially large distances in short timeframes				●			
Strategies for recovery of site utilities					●		
Strategies for recovering damaged buildings & facilities					●		
Strategies for recovery of site-wide services					●		
Bespoke BC recovery financial delegation letters						●	
Financial strategies for recovery of key business						●	
Financial strategies for supporting staff in immediate need						●	
Strategies for enabling access to / recovery of Key Data, Voice and IT communication							●
Analysis of single points of failure (resilience)							●
Access to cash & other purchasing routes (i.e. procurement cards)						●	

CHAPTER 6 – EXERCISING, MAINTAINING, REVIEWING & ASSURANCE


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

Introduction

6.1 An organisation's Business Continuity (and Incident Management) arrangements cannot be considered reliable until exercised and unless their currency is maintained. Exercising is essential to developing teamwork, competence, confidence and knowledge – which are vital at the time of an incident.

6.2 Planning arrangements and assumptions are verified through exercising, audit and other self-assessment processes to ensure that they are "fit for purpose".

Exercise Programmes

6.3 Well-developed exercise programmes provide objective assurance that BU BC and Site Recovery Plans will work effectively, and as anticipated, when required. They should:

- Exercise the technical, logistical, administrative, procedural and other operational systems of the BC Plan;
- Exercise BC arrangements and infrastructure – including roles and responsibilities, Incident Management locations, etc;
- Validate the recovery of IT/IS and communications, including the availability and relocation of staff.

6.4 In addition, exercise programmes can lead to improvements in BCM capability through:

- Practising the organisation's ability to recover from an incident;
- Verification that the BC Plan incorporates all organisational critical activities, and their interdependencies and priorities;
- Validation of the effectiveness and timeliness of restoration of critical activities;
- Highlighting assumptions which need to be questioned;
- Instilling confidence amongst exercise participants;

- Demonstrating/developing the competence of Recovery Teams (and their alternates); and

- Raising awareness of Business Continuity throughout the organisation (including at Senior levels) through publicity activities and/or involvement in the exercise.

6.5 The programme should take account of the roles of all parties, including key contractors/service providers, who would be expected to participate in recovery activities. These third party organisations should be invited, where practicable, to take part in the exercises.

Exercising BCM Arrangements

6.6 No matter how well designed and thought-out a BC Plan or BCM Strategy is, a robust and realistic exercise will almost always identify areas of improvement. Conversely, a completely flawless exercise is more likely to indicate a failure in the exercise process (i.e. not challenging or realistic enough) rather than confirm the total adequacy of Plans.

6.7 Every exercise must have clearly defined aims and objectives, be realistic, and carefully planned and agreed with stakeholders so that there is minimum risk of disruption to business processes or the likelihood of an incident occurring as a direct result of the exercise. The scale and complexity of the exercise should be determined by the maturity of the BCM arrangements (including the skills and knowledge of the team), and be appropriate to the organisation's recovery objectives. It is probably best to start with a simple proof-reading of the Plan, before moving onto more challenging testing. The type of exercises most commonly used include:

- Proof Reading Exercise.

- Desktop Exercise.

- Simulation.

- Live Exercise.

6.8 A Table of the types and methods of exercising BCM arrangements can be found at Annex 6A. Detailed guidance on the types of exercise, and how to facilitate them is provided in the MOD's Guide to Exercising BC Plans, which is available on the Business Continuity Communities of Practice website on the Defence Intranet.

6.9 It is very important that exercises are conducted regularly – at least annually – that those actually tasked with effecting recovery participate (i.e. not a lower level representative), that they truly test the Plan and the people, and that lessons identified are fed back into the Plan maintenance process, via the production of a post-exercise report containing post-event actions.

Maintaining BCM Arrangements

6.10 It is important that plans are kept up-to-date and keep pace with organisational or other (internal and external) changes as and when they occur. As a minimum, all Plans (TLB/TF, BU and Site) are to be reviewed and updated at least annually, in line with the objectives flowing from Management Planning activities. However, depending upon the level of critical activity locally, the complexity of the activity undertaken, and its sensitivity to time delay and/or external factors, managers might decide to review their BC arrangements on a more regular basis.

6.11 In addition to scheduled reviews, managers should revisit BC Plans whenever the organisation undergoes a significant change – for example the installation of a new corporate IT system, the transfer in or out of one or more Business Units, or a physical move to a new building or site. Any of these events is likely to render some or all of a plan obsolete – in a perfect world the organisation will have planned the change with BC in mind and avoided all obvious BC pitfalls.

6.12 Risks to continuity also rise and fall in size, number and importance over time, largely as a result of external factors. As far as is practicable, organisations need to be sensitive to this and be flexible in their BC planning – it helps if a “continuity culture” exists (see Chapter 7) as this increases the chance of this flexibility happening organically rather than being driven by management or BC Planners.

6.13 It is the responsibility of all staff that opportunities to improve BCM are taken and, where possible, lessons identified are incorporated into BCM activities and products.

Reviewing and Assurance

6.14 As part of MOD Corporate Governance procedures, annual assurance reports to show that robust BC measures are in place must be provided to TLB/TF Audit Committees (ACs), and in turn the Defence Audit Committee (DAC). Lessons learnt from BCM activities and the assurance process should then form the basis for improvement activities (see Annex 6B).

6.15 TLB/TFs must ensure they undertake an annual BCM assurance process. TLB/TF ACs must have the responsibility to review TLB/TF BC as part of their Terms of Reference. The format of TLB/TF assurance reports will depend on the requirements of individual ACs.

6.16 The following should be used as a guide for what should be covered in a BC assurance report:

- Confirmation that effective BCM arrangements are in place within the organisation and that they meet the requirements of this JSP, including:
    - All key products and services and their supporting critical activities and resources have been identified and included in Strategies and Plans;

    - Strategies and Plans accurately reflect organisational priorities and requirements, and are appropriate to the level of risk faced;

- Assurance that BC products are regularly and comprehensively exercised and updated.

- Confirmation that all staff involved in BC have undertaken the relevant training.

- Identification of unresolved risks that:

    - Will affect the TLB/TFs' ability to continue critical business, e.g. lack of a suitable fallback location.

    - Pose a threat to the continuation of normal business, e.g. IT single points of failure.

6.17 TLB/TFs are also required to provide an input to the Annual Departmental BCM Assurance Report to the DAC, compiled by the BC Policy Team in DBR. The format/content and timing of the inputs to the annual report are notified to TLBs/TFs by the BC Policy Team in October/November each year. TLBs/TFs may use the information gathered for the annual report to meet the reporting requirements of their own Audit Committees.

6.18 In addition to TLB/TFs auditing their own arrangements, BCM audits are also undertaken by the Defence Security Assurance Services (DSAS) and the Directorate of Internal Audit (DIA).

6.19 DSAS (part of CIO), at the request of DBR, conduct audits of TLB/TF BCM on a rolling 3 year basis, with reviews of Action Plans being conducted during the intervening period. These are not inspections, but audits that concentrate on the strategic arrangements in place, with a strong emphasis placed on understanding the resilience being built into the achievement of TLB/TF and Departmental objectives. The key areas that will form the basis of audit reviews and resulting reports are listed at Annex 6C.

6.20 Requests for independent audit of BCPs can be made to DIA, but priority will usually be given to audits that cover more than one TLB and which are sponsored by the appropriate Process Owner.

External Auditing and Certification

6.21 Trading Funds may choose to make use of external auditors, in addition to the audits undertaken by DSAS / DIA.

6.22 The Cabinet Office (Civil Contingencies Secretariat) has indicated that it is not planning to direct UK Government Departments to seek formal certification of their BCM arrangements against BS 25999. However, the Cabinet Office can arrange for an "independent" review of BCM to be undertaken by the Emergency Planning

College (EPC). It should be noted, however, that the EPC review is not free of charge.

ANNEX 6A

TYPES AND METHODS OF EXERCISING

Complexity	Exercise	Process	Variants	Frequency
(1) Simple	Review or Proof-Reading of Plan	Review / amend BCP content	Update / validation	At least annually
		Challenge content of BCP	Audit / verification	Annually
(2) Medium	Desk-Top or Walk-through of Plan	Challenge content of BCP	Include interaction and validate participants' roles	Annually
	Simulation	Use "artificial" situation to validate that the BCP(s) contains both necessary and sufficient information to enable a successful recovery	Incorporate associated Plans	Annually or twice yearly
	Exercise Critical Activities	Invocation in a controlled situation that does not jeopardize "business as usual" operation	Defined operations from alternative site for a fixed time	Annually or less frequently
(3) Complex	Exercise full BCP, including incident management	Building / Site / exclusion zone-wide exercise		Annually or less frequently (see further comments below)

Simple

6.A.1 A review or proof-read of the Plan will provide assurance that:

- The Plan is clear and makes sense to someone else (i.e. someone not involved in writing the Plan);
- All BC/recovery roles and responsibilities have been included;
- Potential communication problems (e.g. Telephone numbers) are identified;
- Gaps in the Plan are identified.

Medium

6.A.2 A desk-top exercise is a walk-through of the Plan with the participants (possibly at the designated Recovery Command Centre), testing assumptions in the Plan and the participants' understanding of roles, responsibilities and procedures.

This can be useful in identifying gaps in knowledge, incorrect or flawed planning assumptions, and can also help to build teamwork where people are working together for the first time.

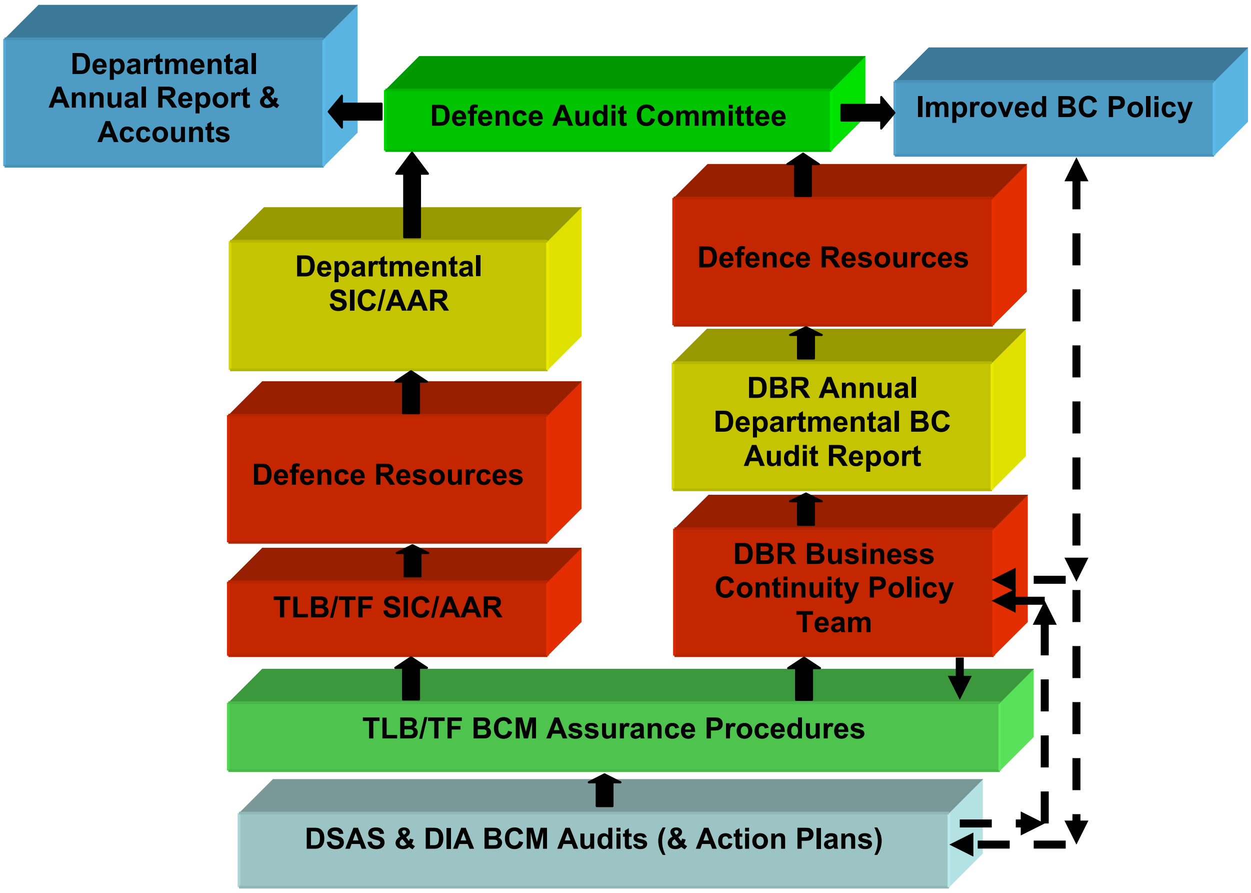
6.A.3 Simulation exercises are based upon an enactment of events as they might unfold in a crisis (from crisis/incident to invocation of the BCP). The simulation exercise will require Site Recovery Teams to work from their designated Recovery Command Centre. The exercise is controlled by a team working to a script. Simulation exercises can be made quite realistic and therefore test people much more thoroughly, but they are clearly more labour intensive and may cause some disruption to the normal business (although efforts should be made to minimize the impact).

Complex

6.A.4 Complex or “live” exercises are the most thorough form of testing, but they are likely to disrupt the whole area being tested. They are **only recommended if deemed truly necessary and are within the capability of the organisation and BC Planners to manage**. For example, a live test might involve the no-notice closure of a building, BC Plans being invoked, and all previously identified non-critical staff being sent home.

ANNEX 6B

MOD BCM ASSURANCE PROCESS


Departmental Annual Report & Accounts
Defence Audit Committee
Improved BC Policy
Departmental SIC/AAR
Defence Resources
Defence Resources
DBR Annual Departmental BC Audit Report
TLB/TF SIC/AAR
DBR Business Continuity Policy Team
TLB/TF BCM Assurance Procedures
DSAS & DIA BCM Audits (& Action Plans)

Notes

SIC – Statement of Internal Control
AAR – Annual Assurance Report

Trading Funds' SIC/AAR do not form part of the Departmental Annual Report & Accounts; instead they are contained within the TFs' own Annual Reports and Accounts. However, given that MOD is a major stakeholder in the TFs, their agreed AARs are provided to PUS.

ANNEX 6C

DSAS AUDITS – KEY AREAS FOR REVIEW[32]

Leadership

6.C.1 Do Senior Management support and promote active BCM?

- Is there a BC Champion at board level?

People

6.C.2 Are people equipped and supported to manage BCM?

- Is there a nominated BCM Management team?
- What are their resources and influence within the organisation?
- What levels of awareness are seen in the organisation and what is done to promote this?

Strategy and Policy

6.C.3 Is there a clear BCM strategy and supporting policies and plans?

- Are the mandated elements of the Departmental Strategy and the JSP 503 in place?

Partners

6.C.4 Are there effective arrangements for managing partners?

- Are internal and external stakeholders aware of what actions the organisation will take if BCPs are activated?
- Has the BC status of the supply chain been considered?

Processes

6.C.5 Do the organisation's processes incorporate effective BCM?

- Do BCPs exist that are designed to maintain critical activities at an appropriate level and within appropriate timescales?
- Is there an ongoing review, maintenance and audit process for BCP?

[32] This section to be updated in due course

Resilience Management

6.C.6 Is resilience embedded and continually tested?

- Is there an established and ongoing programme for exercising BCPs?

- Is there a process for lessons learnt from exercises?

- What actions have been taken to integrate these into BCPs?

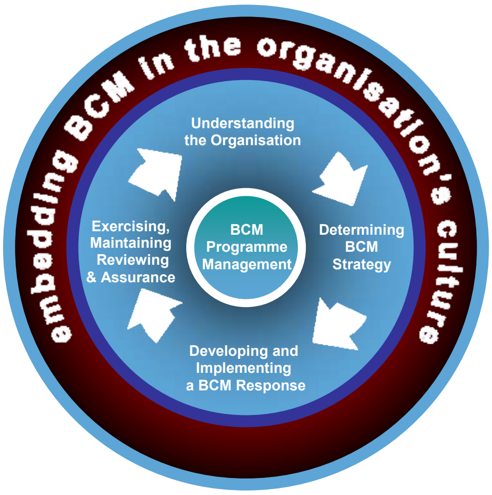
Outcomes

6.C.7 Does BCM contribute to achieving outcomes?

- Have critical activities and the resources needed to deliver them been identified?

- Is the resilience of business critical outputs increased by these activities?

CHAPTER 7 – EMBEDDING THE BCM CULTURE


embedding BCM in the organisation's culture
Understanding the Organisation
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining Reviewing & Assurance
BCM Programme Management

Introduction

7.1 Building, promoting and embedding a BCM culture within an organisation ensures that it becomes part of the organisation's core values and effective management.

7.2 This Chapter is for everyone involved with BC. It explores in detail the importance of raising awareness of BC Plans and issues, and establishing a culture of continuity within the organisation. If everyone is thinking "continuity" in their day-to-day work then this will have a positive effect on the organisation, improve the way risks are managed, and increase the effectiveness of local BC Plans and their implementation.

7.3 Most organisations that fail in their BC planning have allowed their BC plans to stagnate and not keep pace with the organisation as it and the environment in which it operates changes. An organisation that lacks a 'continuity culture' is one that views BCM as a one-off activity. The key messages are:

- BCM is a continuous process – it does not begin and end at the production of a BU/Site Plan or a Strategy document.
- BCM is the concern and responsibility of everyone. It is not a service that someone else provides for you.

7.4 An organisation with a positive BCM culture will:

- Develop a BCM programme more efficiently;
- Instil confidence in its stakeholders in its ability to handle business disruptions;
- Increase its resilience over time by ensuring BCM implications are considered in decisions at all levels; and
- Minimise the likelihood and impact of disruptions.

Promoting BCM Awareness and Understanding

7.5 In the aftermath of a disaster there will be a great deal of confusion. A well thought-out Plan should prevent that general confusion from overwhelming those tasked with leading a recovery. However, the effectiveness of the Plan will be greatly enhanced if everyone is aware of, and understands the BC Plan content, knows what is happening, what their roles and responsibilities are, and are all pulling in the same direction. Organisations with employees who appreciate the importance of BC are more likely to make day-to-day decisions that increase the resilience of business processes and systems. This obviously has a positive impact on the organisation.

7.6 Staff should be (regularly) reminded that BCM is as much a proactive discipline as a reactive one. It is preferable to avoid the impacts of a disruptive event than to successfully recover from it. Staff should be encouraged to think about the continuity consequences of their day-to-day decisions, and publicly praised for good decision-making that results in an overall improvement in local resilience. The aim is to avoid the situation where a new process or system is implemented only for the local BC Planner to have to amend it later in order to manage the resulting BC risks – the constant building and defusing of ‘continuity time bombs’ is wasteful.

7.7 Staff involvement in the development of Plans is important. They often have the most relevant information and the best ideas and, following a disaster, their co-operation and enthusiasm will be invaluable. If they helped construct the plan they are more likely to want to take part in implementing it. Some examples of BCM awareness activities can be found at Annex 7A.

7.8 Achieving cultural change is a difficult and lengthy process, and must be tackled from every angle.

7.8.1 The TLB/TF Management Board through the endorsement and issuing of the TLB/TF BCM Strategy.

7.8.2 Senior Managers have a part to play in keeping BC issues high on the day-to-day agenda, and should be actively encouraging their teams to consider resilience and BC issues alongside other, more familiar, management considerations.

7.8.3 Local BC Planning staff, through their awareness programmes, should aim to influence staff at all levels. Given the subject matter, it is easy to become labelled the deliverer of bad news, therefore every opportunity to expose good news – BC success stories, or particularly well thought-out BC Plans – should be grasped and maximum benefit gained from them.

Skills Training

7.9 The MOD requires that all staff with responsibilities for Business Continuity Planning undertake the one-day MOD Principles of Business Continuity course (Ref S049) provided by the Defence Academy College of Management Training[33]. Further information can be found on the Defence Academy website (www.da.mod.uk/cmt), or by contacting the Defence Academy on 01793 314485 or 96161 4485.

[33] To note, this course may not be run beyond the end of 2011.

7.10 The skills/competence of staff with specific roles/responsibilities in BC and Site Recovery Plans should be developed through workshops and practical training (including participation in exercises).

7.11 To raise awareness of Business Continuity Management across the MOD, a 30-45 minute e-learning BC Awareness Course is also available from the Defence Academy (VS033)[34]. This can be accessed through the Defence Learning Portal (www.dlp.dii.r.mil.uk/). All Defence personnel (Civilian and Military) are encouraged to complete this course, and it is a prerequisite for attendance on the one-day course.

7.12 In addition to this, a Business Continuity awareness presentation called "Protecting Defence Capability: An Introduction to Business Continuity Management in Defence" is available on the Business Continuity – Departmental Guidance page on the Defence Intranet. The presentation can be used either for personal development (desk-based training) or delivered as a group presentation (guidance notes for presenters are provided).

7.13 Information on external sources of BCM training can be found at Annex 7B.

[34] To note, this course will be removed from the DLP when the licence expires (date not known).

ANNEX 7A

BCM AWARENESS ACTIVITIES

7.A.1 Let everyone have access to local BC Plans. If necessary have two versions – one version containing personal data for those who need that level of detail, and an abridged version (possibly in the form of a leaflet) for everyone else.

7.A.2 Talk through Plans with staff regularly so they know what can be expected should a disaster occur, and understand what they would need to do.

7.A.3 Ensure staff know and understand the business criticality of their post (including those in non-critical posts). If they don't know their criticality, they probably won't be there when you need them. Also watch morale – emphasise that non-business critical does not mean less important. If some of your critical staff are victims of the disaster, and cannot come to work, you will be relying on the rest to fill the gaps – they are therefore still important.

7.A.4 Include BC as a topic for away days, team meetings and other team events.

7.A.5 Update induction material to include details of local BC arrangements.

7.A.6 Consider producing a small information card, perhaps credit card-sized, for all staff to carry detailing basic emergency numbers and other relevant BC information.

7.A.7 Consider producing a static display and position it regularly at building entrances or other shared areas, reminding staff of BC arrangements and likely recovery responses.

7.A.8 Consider mounting a local poster campaign – perhaps with a local or topical flavour.

7.A.9 Invest in training and exercising for your BCM planners and site recovery personnel – get them used to working together.

7.A.10 Publicise BC exercises (e.g. through in-house publications) – staff will be interested.

7.A.11 Latch onto other BC awareness initiatives, either locally or nationally (for example the BCI-sponsored annual BC Awareness Week) to help promote BC arrangements.

ANNEX 7B

EXTERNAL SOURCES OF BCM TRAINING

7.B.1 A number of commercial organisations provide training courses, seminars and other events on BCM, ranging from those new to the subject to the more experienced practitioner. Anyone looking for advice on the most suitable type of BC training to be undertaken should contact their BC Focal Point (listed on the BC Communities of Practice page on the Defence Intranet) or the DBR BC Policy Team (via the BC pages on the Defence Intranet). Any external training will, however, be subject to the normal budgetary approval.

7.B.2 The ***Emergency Planning College (EPC)*** is the Government's centre of excellence for crisis management and emergency planning. The majority of courses are designed for those with a role under the Civil Contingencies Act (particularly emergency responders); however, there are a number of courses which may be of interest to MOD Staff. Detailed information on the College and its current Prospectus can be found at www.epcollege.gov.uk.

7.B.3 The ***BCI*** accredits courses provided by external training providers, which may be of particular benefit to those who have a specific training requirement. Further information on these courses can be found on the BCI's website (www.thebci.org) or on Continuity Shop (www.continuityshop.com).

CHAPTER 8 – SOURCES OF INFORMATION AND GUIDANCE

Introduction

8.1 This JSP provides sufficient basic information on BCM and associated planning processes for newcomers to get started, but beginners and experienced practitioners alike may need to supplement this through further research and reading. This Chapter provides pointers to an assortment of material and other information on BCM.

Sources of Information on wider UK Government Resilience

8.2 Government-wide BCM matters, as well as policy for planning a response to national crises and disasters, is the responsibility of the Cabinet Office. They maintain a website on the Internet (www.cabinetoffice.gov.uk/ukresilience) which contains information on measures being taken to improve the resilience of Central Government and the wider-UK, including:

- Civil Contingencies Act 2004 (and Enhancement Programme)
- National Risk Register
- Emergency Planning
- Local Resilience Fora[35]
- National Exercise Programme
- Infrastructure Resilience
- Pandemic Influenza National Framework

Sources of BCM Information within the MOD

8.3 All the key documents, information and guidance on MOD BCM (including Pandemic Influenza Planning and Preparedness) can be accessed through the Business Continuity pages on the Defence Intranet. It is regularly updated with the latest information on BCM.

8.4 The following Defence publications (some of which are referred to elsewhere in this JSP) cover a number of related disciplines:

8.4.1 Health and Safety

JSP 375 – MOD Health and Safety Handbook.
Volume 2 – Leaflet 1 – Emergency and Disaster Planning Strategy.
Volume 2 – Leaflet 41 – Home Working.

8.4.2 Security

JSP 440 – The Defence Manual of Security.

[35] LRFs can provide information on community risk registers and local resilience planning, which may be useful for Site BC & Recovery Plans.

Part 5, Section 2, Chapter 5 – Home Working (Security Considerations).
Part 8, Section 4, Chapter 4 – The use of Private Computers for Official Purposes.

8.4.3 Major Accident Control Regulations

JSP 498 – Major Accident Control Regulations (MACR).
Chapter 5 – On-site Emergency Plan (if covered by COMAH/MACR).
Chapter 6 – Off-site Emergency Plan (if covered by COMAH/MACR).

8.4.4 Corporate Governance and Risk Management

JSP 525 – Corporate Governance
JSP 892 - Risk Management

8.4.5 Selection of Managed Services for network-based services, applications, and equipment

JSP 602 – Information Coherence Directions – Directions and Guidance**.**

An Instruction on Business Continuity (particularly with regard to Service Level Agreements) has been published within this series under 'Managed Services', which includes guidance on best practice for Contingency Planning for CIS systems.

8.4.6 Managing Patterns of Work

Policy Rules and Guidance[36] on Home-Working.
Policy Rules and Guidance on Working Time Regulations.

8.4.7 Liaising with TUs over BC Arrangements

Policy, Rules and Guidance: Our Approach to Employee Relations.

This document covers Consultation Agreements with Trades Unions and general procedures for proposals affecting civilian staff. Although most BC/Disaster Recovery Plans should not trigger the automatic requirement for TU consultation, Business Units may find informal discussions with the TUs useful (possibly through local Whitley Committees) as part of the wider plan development and communication process. TU consultation should not be viewed as an alternative to consulting staff directly.

8.4.8 Welfare

[36] Policy, Rules and Guidance Documents can be found on the People Services Portal on the Defence Intranet

Civilian Staff can access advice and guidance on welfare issues through the People Services Portal and the "Health, Wellbeing and Sickness" page. Military Staff should refer to JSP 770 (Tri-Service Operational and Non Operational Welfare Policy).

For Civilian Staff, information on the actions to take following death in service is contained in Policy, Rules and Guidance: Death in Service.

External Sources of BCM Information

8.5 The leading BCM professional body in the UK is the Business Continuity Institute (BCI). It maintains an Internet website (www.thebci.org) which publishes information on training, seminars, best practice, and nationally-recognised professional BCM standards.

8.6 Other Internet websites providing information on BCM are:

- The Continuity Forum – www.continuityforum.org
- Globalcontinuity.com – www.globalcontinuity.com
- Continuity Central – www.continuitycentral.com

Other Assistance

8.7 Transport - In general terms, and depending on the nature of the event, public transport is likely to either stop completely or remain operating long enough to enable the safe evacuation of people from the network. This would be followed by the restoration of services when it is safe or feasible to do so, or running reduced levels of service (with greater overcrowding). Some networks are difficult to shut down (i.e. roads), but more manageable and likely at local level. Given that transport services in the UK are largely provided by the private sector, their main interest is likely to be the maintenance of their reputation through the restoration of services as quickly as possible. There is no single source of information on transport arrangements following a disruptive event; however, the following websites may be useful:

- Department for Transport: www.dft.gov.uk
- National Rail Enquiries: www.nationalrail.co.uk
- British Airports Authority: www.baa.com
- Highways Agency: www.highways.gov.uk
- Transport for London: www.tfl.gov.uk
- BBC: www.bbc.co.uk

8.8 Software - There are many software tools on the market designed to assist in automating the BC planning process, particularly in handling and storing large amounts of relational data. They can be useful as databases and for report/plan generation, but their upkeep and limited flexibility can also cause problems, and they may not be suitable for hosting on the Defence Information Infrastructure (DII). Further information can be found on the BCI and Continuity Central websites including a directory of BC software packages and suppliers.

GLOSSARY

Terms and Definitions

	Abbreviation	Definition
British Standard for Business Continuity Management	BS 25999	The British Standard establishes the process, principles and terminology of Business Continuity Management. The Standard provides a system based on BCM good practice.
Business Continuity	BC	Strategic and tactical capability of an organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable, pre-defined level.
Business Continuity Management	BCM	A holistic management process that identifies potential threats to critical defence outputs and the impacts those threats, if realised, might cause. It provides a framework for building organisational resilience with the capability to support an effective response that safeguards critical defence outputs and the interests of key stakeholders and reputation.
Business Continuity Management Lifecycle (or Model)		The series of Business Continuity activities which collectively cover all aspects and phases of the Business Continuity Management Programme.
Business Continuity Management Programme (or Framework)	BCMP	Ongoing management and governance process supported by top management and appropriately resourced to ensure the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products, outputs and services through training, exercising, maintenance and review.
Business Continuity Management Strategy	BCM Strategy / BC Strategy	The approach by an organisation (MOD, Top Level Budget, Trading Fund/Agency, and HLB (as appropriate)) that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.
Business Impact Analysis	BIA	Process for analysing business functions and the effect that a disruption might have upon them. It is a means of establishing the critical functions of a business, their recovery priorities and their support requirements.
Business Unit Business Continuity Plan	BU BC Plan / BU BCP	BC Plans prepared at Business Unit, Divisional or Directorate level. Plans contain procedures and information developed (in accordance with the BCM Strategy), compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical outputs/activities at an acceptable pre-defined level. BC Plans let staff know what they have to do in an emergency.

Civil Contingencies Secretariat, Cabinet Office	CCS	Department responsible for Government-wide BCM matters, as well as the policy for planning the response to National crises and disasters.
Cold Site		An alternative site or facility (usually a data centre) equipped with a basic infrastructure. Other equipment has to be delivered and installed before it is ready for use.
Corporate Governance		The system by which organisations are directed and controlled.
Critical/Key Outputs		The most important tasks or operations of an organisation. Defence Critical Outputs are identified in the Strategy for Defence, the annual Defence Plan and lower-level sub-Strategies.
Critical Activities/Functions		Enabling activity required to support and deliver critical/key outputs.
Disaster		An accidental, natural or malicious event of sufficient scale to cause significant damage to an organisation (from the ability to deliver essential services for a length of time, or even imperil the business).
Disruption / disruptive event or incident		Event, whether anticipated (e.g. industrial action) or unanticipated (e.g. electricity blackout) which causes a negative impact on the delivery of an organisation's outputs, activities or services.
Emergency Planning		Development and maintenance of agreed procedures to prevent, reduce, control and mitigate in the event of an emergency (i.e. an event or situation which threatens serious damage to human welfare, security or environment of the UK).
Exercise		Activity in which the Business Continuity Plans are rehearsed to ensure that they contain the appropriate amount of information and produce the desired result when put into effect. Exercises provide the opportunity to identify areas of a Plan requiring development or improvement.
Hot Site		An alternative site or facility that has the equipment and resources to provide almost instantaneous recovery.
Impact		Consequence of a particular outcome (may or may not be expressed purely in financial terms).
Incident Management Plan	IMP	Often also referred to as Emergency and Disaster Recovery Plan. Plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.
Interdependencies		The reliance, directly or indirectly, of one organisation (or one part of an organisation) upon another (including external organisations).
Invocation		Act of declaring that an organisation's BC Plan needs to be put into effect in order to continue the delivery of key outputs/activities and services.
Maximum tolerable period of disruption (or outage)		Period after which an organisation's viability will be irrevocably threatened if activity and service delivery cannot be resumed.

Recovery Command Centre	RCC	The designated location (normally having one or more alternates) from which Recovery Teams work to implement the Site Recovery Plan.
Recovery phase		The period when efforts focus on gradually restoring the infrastructure and business activity to normal, concentrating first on essential services and critical functions.
Recovery Time Objective	RTO	Target time set for the resumption of critical activities, services and equipment (e.g. IT). RTOs are always less than the maximum tolerable period of disruption.
Resilience		Ability of an organisation to resist being affected by an incident.
Risk appetite		Total amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time.
Risk Assessment		Overall process of identifying, analysing and evaluating risks to the organisation. The assessment should also look at ways of reducing risks and their potential impacts.
Risk management		Development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating and controlling the response to risk.
Risk mitigation		Reduction of the exposure to, probability of, or loss from risk.
Service Level Agreement	SLA	A formal customer-supplier agreement between two parties within the MoD.
Service providers		Those who provide the supporting services to the organisation: Facilities Management, Security, Information Services, and Communications. After an incident, other agencies may be called on to provide “crisis” services (e.g. Welfare, Manning, Media Handling).
Single point of failure		A weak point (lack of resilience) in a process, system or equipment which could cause its complete failure/loss during an incident.
Site Recovery Plan		A Business Continuity Plan covering a particular site (or group of buildings), which focuses mainly on recovery activities.
Stakeholders		Those with a vested interest in an organisation’s achievements (e.g. customers, suppliers, partners, employees, distributors, owners etc)
Warm Site		An alternative site or facility (usually a data centre) that is partially equipped with hardware, communications interfaces, power and environmental support so that it can provide back-up operating support.

Abbreviations

(In addition to those provided under Terms and Definitions)

AAR	Annual Assurance Report
AC	Audit Committee
BCI	Business Continuity Institute
BLB	Basic Level Budget
CBR	Chemical, Biological and Radiological
CBRN	Chemical, Biological, Radiological and Nuclear
CCIS	Civilian Casualty Information Service
CIO	Chief Information Officer
CIS	Communications and Information Systems
COMAH	Control of Major Accident Hazard (Regulations)
CSA	Customer Service Agreement
DAC	Defence Audit Committee
DB	Defence Board
DBR	Director Business Resilience
DE&S	Defence Equipment & Support
DCP	Director Civilian Personnel
DIA	Directorate of Internal Audit
DII	Defence Information Infrastructure
DIN	Defence Instructions and Notices
DIO	Defence Infrastructure Organisation
DISS	Director Information Systems and Services
DLP	Defence Learning Portal
DSAS	Defence Security & Assurance Services
EADIAT	Equality and Diversity Impact Assessment Tool
EPC	Emergency Planning College
FP	Focal Point
FM	Facilities Management
H&S	Health & Safety
HLB	Higher Level Budget
HoE	Head of Establishment
HQ	Headquarters
HRMS	Human Resources Management System
IS	Information Systems
IT	Information Technology
JSP	Joint Services Publication
MACA	Military Assistance to the Civil Authorities
MACR	Major Accident Control Regulations
MDPGA	Ministry of Defence Police & Guarding Agency
MOD	Ministry of Defence
NED	Non Executive Director
OGD	Other Government Department
OWS	Occupational Welfare Service
PFI	Private Finance Initiative
PJHQ	Permanent Joint Headquarters

PRG	Policy Rules & Guidance (issued by DCP)
SIC	Statement of Internal Control
SOPs	Standard Operating Procedures
TA	Territorial Army
TF	Trading Fund Agency
TLB	Top Level Budget
ToRs	Terms of Reference
TUs	Trades Union
UORs	Urgent Operational Requirements