Business Resilience

Policy

This policy been prepared by the Bi-Cameral Business Risk and Resilience Group and endorsed by the Management Boards of both Houses. It is effective from December 2010 to November 2011 and provides the framework for the development of business resilience for the House of Commons and Lords services. These development initiatives include an Incident Management Framework, Departmental business continuity plans and alignment to industry standards.

Copyright Statement

© Parliament 2010

Document Control Information

Issue No.	Description of Change	By	Date
v0.1	Initial draft	[s.40]	1st July 2010
v0.2	Revision with comments from BRRG Members post BRRG July and September Meeting	[s.40]	14th September 2010
v0.3	Revision with final comments from BRRG Members post October meeting	[s.40]	18th October 2010
v0.4	Further draft amendments from BRRG Members	[s.40]	11th November 2010
v0.5	Final amendments from BRRG Members post November meeting	[s.40]	15th November 2010
v0.6	Final amendments from BRRG Chair	[s.40]	23rd November 2010
v0.7	Minor amendment from DCCS Clerk Assistant & Director General	[s.40]	24th November 2010

Distribution List

Name	Role	Purpose

Documentation Sign - off

Name	Title	Signature	Date
Jill Pay	BRRG Chair		

Document Location

Locations of where this document is held

Locations
To be published on the Intranet
BRRG shared folder
OCE home drive

Table of Contents

1   Introduction

Business resilience can be defined as the ability of an organisation to resist being affected by an incident. If an unforeseen incident occurs, the services of the two Houses of Parliament (to be referred as "House Services") must be resilient enough as an organisation to:-

- Respond to the incident in order to protect staff, its environment and the services it provides.
- Minimise disruption to Parliamentary business.
- Recover from the incident and return to normality as quickly as possible.

The House Services recognise that effective business continuity management is vital to achieving their strategic goals and effective resilience. The approach to business continuity management will be guided by the requirements of British Standard (BS) 25999-1:2006 "Business Continuity Management".

This standard 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"[1]. The standard provides a framework for building organisational resilience with the capability for an effective response that safeguards Parliament's reputation and the interests of its key stakeholders and assists the House Services in continuing to provide their core services.

It is also recognised that risk management is a prerequisite of effective business continuity management. The policy and framework for risk management are defined separately (see Related Documents).

2   Purpose

The purpose of this document is to define the policy framework within which the business resilience responsibilities for the House Services will be discharged. It also defines the business resilience objectives, and the scope in which objectives will be achieved.

This document ensures that the House Services are compliant with industry standards and also demonstrates a clear commitment to:-

- Business resilience and the on-going obligation of the House Services to maintain the continuity of service.
- Accepting a duty of care to all persons on its premises.
- Aligning to established industry standards and Government guidance.

3   Scope

This Policy is focused on the business activities undertaken by:-

- House of Commons staff.

- House of Lords staff.

- Parliamentary Information Communications and Technology (PICT) staff.

---

[1] British Standard BS25999-1:2006 Business Continuity Management

- Contracted service providers.

Staff of the House Services carry out many activities, some of which are critical activities that can impact on key areas. First and foremost are activities supporting the Chambers, followed by activities that support the Committees, then Members and lastly departmental services that support the public and the heritage of the site.

A generic approach will be taken when developing Departmental Business Continuity Plans. This approach focuses on five core generic scenarios, which could significantly impact the ability of the House Services to carry out its critical activities. These scenarios include:-

- Denial of Access *(to part or all of any of the buildings on the Parliamentary Estate).*

- Denial of Information Technology (IT) and Communications *(to part or all of the IT and Communications network and server based systems and applications).*

- Denial of People.

- Denial of Third Party Suppliers.

- Denial of Utilities *(to part or all of the utilities infrastructure supporting electricity, water, gas and sewage).*

Each scenario is linked to risks identified in the corporate risk register. Additional scenarios may be added once work has been completed on the core scenarios.

4   Objectives

The business resilience aims of the House services are that by 2012 they will:-

"**achieve standards of best practice in developing, maintaining and monitoring business resilience (by aligning against industry standards) and thus become a centre of excellence for business resilience.**"

To achieve these aims, the overall business resilience objective is to ensure that the House Services have a robust business continuity management (BCM) system in place that is able to support the development and maintenance of business continuity plans and respond appropriately to unexpected incidents. It must also interface with risk management.

The approach taken towards achieving the overall objective will reflect the specifications of business continuity management, as described in British Standard BS 25999-1:2006 and includes the following specific objectives:-

- **To ensure the safety of people who work in or visit the premises**
  The safety of people on the Parliamentary estate is the first priority at all times. The House Services have a duty of care to all people on their premises.

- **To ensure that the business of the two Houses and the Services and Departments that support them are protected and continue (Chambers, Committees and Departmental Operations)**
  The House Services will ensure that there are effective mechanisms for identifying, monitoring and mitigating risks. They will also ensure that plans are in place for responding to an incident that disrupts normal operations.

- **To ensure that customers are provided with critical services**

The House Services seek to serve the two Chambers, their Committees, Members and the public. They will identify, categorise, prioritise and establish recovery time objectives (RTOs) and the maximum tolerable outage (MTO) for all critical activities.

- **To provide a generic plan on what to do in a major incident situation**
  The House Services seek to provide a plan that is:-

  - o Flexible, feasible and relevant
  - o Easy to read and understand
  - o Provides a basis for managing issues arising from the five core scenarios (see section 3)

  This plan will take the form of an Incident Management Framework (IMF) specific to the two Houses of Parliament.

- **To review, maintain and test the Incident Management Framework on a regular basis**
  The IMF will be regularly reviewed and maintained to ensure that it is able to meet the needs of the two Houses. This will include an annual IMF exercise and, if required, enhancement of the IMF, following any post-incident review.

- **To review, maintain and test Departmental business continuity plans on a regular basis**
  The House Services will ensure that there are consistent, documented methods for assessing business continuity requirements and that these are used consistently throughout the organisation.

  Departmental Business continuity plans will be documented for all new and existing departments and teams. These plans will be regularly maintained, reviewed and tested to ensure that they are valid.

- **To maintain details of emergency contacts (staff/suppliers/stakeholders)**
  Every plan will contain or provide reference to essential contact details for all key stakeholders.

- **To ensure that staff of the House Services are aware of what to do in the event of an incident**
  The House Services recognise that to be successful, business resilience has to become part of the way that an organisation is managed. They also recognise that raising and maintaining awareness of business resilience with staff is important to ensure that they are aware of why it is important and what their role is during an incident.

5   Business Resilience Policy and its relationship to Risk Management

Business resilience is seen as an integral part of the overall risk management process. Risk management is one of the key management systems that is used to identify and assess those risks that will stop the House Services from achieving their business objectives and identifies or puts in place appropriate internal controls to manage those risks.

Both business resilience, and in particular BCM, are seen as key controls and are in place to manage the risk of disruption to critical services across the House Services and include ensuring plans, such as the IMF, are in place to deliver a rehearsed response to unexpected incidents.

6 Roles and Responsibilities for the Parliamentary Services' BCM Programme

Responsibility for business resilience in Parliament rests as follows:-

Executive and Management Boards

1. The Clerk of the House of Commons and Clerk of the Parliaments have executive responsibility for business resilience in the two Houses of Parliament. This responsibility is discharged through the Management Boards of the two Houses.

2. The Management Boards will delegate strategic responsibility for business resilience to the Business Risk and Resilience Group (BRRG), chaired by the Serjeant at Arms, House of Commons.

Business Risk and Resilience Group

3. The BRRG will act as an internal bi-cameral forum to discuss and manage business resilience issues at a strategic level and to monitor and support the review process.

4. The BRRG will include key representatives from the House Services and PICT.

5. The BRRG will report during the first quarter of the year to the Clerk of the House and the Clerk of the Parliaments on the status of business resilience in the two Houses to feed into the Statements of Internal Control.

6. The BRRG will report and provide assurance to the Management Boards of the two Houses at appropriate times when required.

7. The BRRG will develop and refine business resilience strategy and ensure that documented, tested and robust incident management and business continuity plans are in place to support the corporate business continuity risks in the two Houses of Parliament.

8. The BRRG will discharge the operational requirements for developing and maintaining business continuity plans and the Incident Management Framework to the Business Resilience Co-ordinator.

Business Resilience Co-ordinator

9. The Business Resilience Co-ordinator is the professional lead for business resilience in the House Services and is responsible for:-

   ▪ Reviewing and developing the Business Resilience Policy in line with industry best practice.

- Monitoring standards and compliance with policy.

- Ensuring that each business unit (department or office) is conforming to BRRG requirements and provide assurance to BRRG.

- Provision of support and guidance to each department in business resilience initiatives.

- Reviewing, maintaining and monitoring the IMF and supporting the IMF when required.

- Maintaining the IMF control centres to ensure preparedness in the event of an incident.

- Co-ordinating the development and maintenance of business continuity plans (BCP), supporting Departments where required.

10. The Business Resilience Co-ordinator will ensure that the House Services are aligned to industry standards and take appropriate measures or provide recommendations to the BRRG where non-conformities to the standards have been identified.

11. The Business Resilience Co-ordinator will maintain the Parliamentary business continuity database[2].

Business units

12. Each business unit is required to produce a BCP using the standardised BCP template developed for the House Services. These plans will feed into a bespoke business continuity database.

13. Responsibility for the production and maintenance of BCPs lies with the senior management of each business unit. The senior management may choose to discharge this responsibility by delegation of day-to-day responsibility to a Business Continuity Plan author or champion.

14. The senior management and/or an appropriate and knowledgeable member of staff, not involved in writing the BCP, will independently review the BCP to ensure clarity, consistency and quality.

15. The business unit BCP owner is responsible for ensuring that their BCP is maintained and updated at least every 6 months or when there is significant change to the organisation.

16. The business unit BCP owner is responsible for the rehearsal of its BCP. As a minimum it should be rehearsed annually and comprise at least a walkthrough of the plan.

---

[2] The business continuity database contains all departmental business continuity plans produced by departments of the House Services. The database will be used to produce a wide range of reports to help map critical activities, their location and resource dependencies. These reports will add value to the incident response and planning processes by providing a Parliament-wide overview.

17. Each business unit is responsible for testing its call-out cascade. As a minimum it should be rehearsed annually or when there is significant change in staff.

Internal Audit

18. An audit of the House Services' BCM processes will be undertaken internally at agreed regular intervals. This will form part of the process of aligning to industry standards.

7 Roles and Responsibilities for the Parliamentary Services' Incident Response

The response to an incident by the House Services is outlined in the Incident Management Framework (IMF). The purpose of the IMF is to minimise the impact of any disruption to service delivery on critical activities through the effective and timely implementation of business continuity plans. The IMF consists of an organisation structure and a set of procedures.

The IMF comprises four tiers; super gold, gold, silver and bronze. These tiers relate to different management levels, through which an incident can be controlled and accountability maintained.

Super Gold — Super gold briefs the Speakers of the two Houses, manages the political interface and provides overall direction.

Gold — Gold sets strategic intent, provides leadership, approves communications when appropriate and prioritises the use of resources.

Silver — Silver has authority for the direct management and control of the immediate response and approves communications when appropriate.

Bronze — Bronze teams deliver specific response solutions to an incident within their designated environment by appropriate implementation of BCPs.

8 Related Documents

BSI – British Standard (BS) 25999-1:2006 "Business Continuity Management".
House of Commons – Risk Management Policy and Guidance 2010.
House of Lords – Risk Management Policy and Guidance 2009.
Houses of Parliament – Incident Management Framework 2009.
Cabinet Office – Alignment with BS 25999 2009.
Cabinet Office – HMG Security Policy Framework 2010
Business Continuity Institute – Good Practice Guide 2010.

9 Policy Review

This policy is effective from the date of sign-off and will be reviewed annually.

_____