Management Board

Update on business resilience capability and annual approval of Business Resilience Policy

Paper from David Leakey, Chair of the Business Resilience Group
For the meeting on 12 December

Purpose

1. This paper provides an update to the Management Boards of both Houses regarding Parliament-wide business resilience activities and for the Boards to undertake the mandated annual review of the Business Resilience Policy.

2. The Board is invited to take note the content of this update and approve the revised Business Resilience Policy November 2013 – November 2014 presented in Annex A.

Consultation and equality analysis

3. The Business Resilience Policy has been discussed and approved by members of the Business Resilience Group.

4. Equality analysis will be conducted on work carried out by the business resilience team and decisions of the Business Resilience Group.

Background

5. The Business Resilience policy states that the "Management Boards will delegate strategic responsibility for business resilience to the Business Resilience Group". BRG directs the work of the Business Resilience team. This includes developing business resilience policies, procedures and contingency plans, maintaining a Business Continuity database, providing training and exercising, and ensuring that resilience issues are taken into account in management decisions.

6. The Business Resilience team currently comprises three individuals who work on a bicameral basis.

a) The Business Resilience Coordinator is a full time position and is tasked with developing and maintaining the Parliamentary service's capability to respond to, and recover from, a major incident.

b) The Secretary to the Business Resilience Group also provides general support to the Business Resilience Programme on a basis of 0.2 FTE.

c) Further support is provided by an additional member of staff who spends 0.5 FTE on providing assistance to implement the Programme.

7. Resilience has been further increased by the successful recruitment and training of a number of individuals to fulfil the roles of on-call Chief of Staff and Support staff. This has provided Parliament with a 24/7 capability for supporting the response to incidents on an on call basis when the IMF is activated. Additional support has been provided by procedural representatives from both Houses.

Update

8. The main developments since the last report to the Management Boards are as follows:

a) The Incident Management Framework (IMF) has been substantially revised, and a number of staff from both Houses has been recruited to fill the on-call Chief of Staff and Support Staff positions in the Incident Management Team (IMT). All individuals have taken part in a sequence of training sessions to develop the skills essential for their roles and on a number of occasions when the IMF has been activated. This innovation has been effective and successful.

b) Comprehensive information, contacts list and guidance pack has been developed to support the role of Duty Silver and the Duty Chief of Staff. A similar pack is under development for Gold.

c) The Business Continuity and Disaster Recovery (BCDR) database which is used to coordinate departmental plans has been reviewed as part of an ongoing programme to ensure it still met the needs of both Houses. Further work has been commissioned to improve the usability and accessibility of the system.

d) Heritage salvage arrangements have been re-invigorated and the link to business continuity structures and the IMF have been strengthened. As a result of discussions between the Chair of BRG and the Director General of Facilities (Commons), agreement was reached that Heritage Salvage arrangements would be co-ordinated by facilities staff. They would manage the resources, training and collaborative workings of the Heritage Groups and act as the link to the IMF.

e) Regular workshops, including on the lessons from recent real incidents, have been held throughout the year to support the training and currency of Duty Silvers.

f) A range of formatted documents and procedures have been created to support the speed and communication of decision making during an incident and to ensure that it is accurately captured and auditable.

g) WIS has now enabled business critical information to be duplicated onto the intranet from the internet site. This has strengthened the resilience to ensure continued access to business critical information in the event of a failure.

h) In October 2013 another BC Forum was held and attended by BC plan owners and authors across both Houses This facilitated a group discussion to take place on appropriate ways for departments to validate their plans. The 'How To Do Business Continuity' training courses have also been repeated this year. They have been increasingly well attended and well received.

i) Protocols for website resilience have been agreed to ensure a clear decision making process is in place, in the event of the failure of the internet site for whatever reason.

j) A review was carried out on the implications of the ICT Strategy on Business Continuity. This provided sufficient assurance that business continuity issues had been factored in as part of the work being carried out on the ICT strategy.

k) Technical resilience ratings (Power, Utilities, Fire suppression etc) of Parliamentary buildings have been agreed by BRG, subject to further work to be carried out by PED. These have ensured, at a minimum, we are in line with industry standards although in many cases go beyond.

l) BC and BR Audit actions that arose from audits by both Houses have been completed in line with agreed dates.

m) In measuring and benchmarking progress and development of BR by both Houses, significant progress has been made to align with the ISO22301:2012 standard. Initial work is now complete in preparation for an initial external audit to take place in December by the BSI (British Standards Institution).

BR Policy

9. The mandated annual review of the Business Resilience policy has been undertaken and approved by the BRG. **The Board is invited to take note the content of this update and approve the revised Business Resilience Policy November 2013 – November 2014 (attached in Annex A).** Proposed changes to the document are shown in tracked changes for ease of reference.

Risk management

10. BRG review compliance of work carried out for the group with the risk management systems of both Houses. The resilience team assess compliance with the risk management systems as part of the quality assurance process of departmental plans.

Legal implications

11. This paper raises no legal issues.

House of Lords implications

12. This paper had been discussed and approved by the House of Lords on Wednesday 4th December.

David Leakey
Chair of the Business Resilience Group
4 December 2013

Business Resilience | Policy

This policy has been prepared by the Bi-Cameral Business Resilience Group and endorsed by the Management Boards of both Houses. It is effective from December 2013 to November 2014 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.

Document Control Information

Issue No.	Description of Change	By	Date
v0.1	Initial revised draft		31st Oct 2011
v0.2	Revision with comments from BRG Members post BRG October Meeting		14th Nov 2011
v0.3	Updated for 2012/13 following BRG annual review		22 October 2012
v0.4	Policy reviewed		4 November 2013

Distribution List

Name	Role	Purpose

Documentation Sign - off

Name	Title	Signature	Date
Robert Rogers	HoC Clerk of the House		
David Beamish	HoL Clerk of the Parliaments		
David Leakey	BRG Chair		

Document Location

Locations of where this document is held

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

Table of Contents

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 the International Standard (ISO22301:2012) "Business Continuity Management" (BCM). This new standard replaces the British Standard BS25999 which Parliament is currently aligned to.

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).

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:-

---

[1] British Standard BS25999-2:2007ISO 22301:2012 Business Continuity Management

- 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.
- Continuous development of contingency plans including, in the worst case, relocation.

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.**"

The business resilience aim of the Houses' services is to ensure the continuation of parliamentary critical business and supporting activities with a high degree of confidence.

To achieve this the Houses' services will continue to implement the Business Resilience strategy (2012- 2016) and align to the International Standard for business continuity management (ISO22301:2012) by 2016.

The approach taken towards achieving the overall objective will reflect the specifications of business continuity management, as described in ISO22301:2012 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 (the priority being the business of the Chambers, then Committees, then members and then 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 period of disruption (MTPOD) 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 form part 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. It will also include additional exercises and training for incident responders (BRONZE, SILVER and GOLD).

- **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.

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.

- Parliamentary Estates Directorate

- 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), data and Communications *(to part or all of the IT and Communications network and server based systems and applications).*

- Loss of People (*e.g. following an outbreak of pandemic influenza*).

- Denial of Third Party Suppliers.

- Loss of Utilities *(to part or all of the utilities infrastructure supporting electricity, water, gas and sewage resulting in the loss of use of all or parts of the estate).*

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.

Business Resilience Policy and its relationship to Risk Management

Business resilience is 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.

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. Each House and, PICT and PED appoint a senior manager as their respective BCM leader.

2. The Management Boards will delegate strategic responsibility for business resilience to the Business Resilience Group (BRG), chaired by Black Rod, pro tem.

Business Resilience Group

3. The BRG 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 BRG will include key representatives from the House Services and PICT.

5. The BRG 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 their respective Governance Statements.

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

7. The BRG 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 BRG will oversee the operational requirements for developing and maintaining business continuity plans and the Incident Management Framework to be facilitated by 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 BRG requirements and provide assurance to BRG.

   ▪ 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 Incident Management locations to ensure preparedness in the event of an incident.

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

   ▪ Preparing and delivering exercises and training in order to maintain the readiness of the IMF.

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 BRG where non-conformities to the standards have been identified.

11. The Business Resilience Co-ordinator will develop and maintain a Parliamentary business continuity database.

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.

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.

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.

Chief of Staff   Responsible for managing the IMF Secretariat and managing the information flow during an incident.

Related Documents

BSI – ISO 22301:2012 "Business Continuity Management".
House of Commons – Risk Management Handbook 2011.
House of Lords – Risk Management Policy and Guidance 201209.
Houses of Parliament – Incident Management Framework 2009.
Cabinet Office – HMG Security Policy Framework 2010
Business Continuity Institute – Good Practice Guide 20130.

Policy Review

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