Case Study: Reviewing Business Continuity Management

Department of Parliamentary Services

Audience

This information sheet is intended to assist Commonwealth officials at the following level:

Specialist level: Job role specialists, who are required to design, implement and embed an entity's business continuity framework.

At a glance

The Department of Parliamentary Services (DPS, '*the department*'), supports the functions of the Australian Parliament and the work of parliamentarians. DPS' activities include the provision of professional services; advice and support for parliamentary operations; and the ongoing maintenance of the Australian Parliament House.

As part of the department's internal audit program, DPS' business continuity arrangements were reviewed leading to an understanding that the business continuity framework needed to be updated to reflect current risks and departmental operations. To ensure that DPS' business continuity framework was fit for purpose and followed industry's best practice approach, the department collaborated with Comcover to undertake a comprehensive Business Impact Analysis (BIA) project.

Outcomes of this project led to:

- a heavily revised business continuity framework that meets the department's needs;
- lessons learned from scenario testing which have further strengthened the department's business continuity framework;
- a greater understanding of Business Continuity Management (BCM) by key staff; and
- an engaged executive with the momentum required to continuously improve BCM in the department.

About business continuity

Business continuity is a program developed to:

- understand potential risks of unplanned disruptions, especially those related to the provision of an organisation's key services;
- identify the organisation's time-critical business processes/activities/functions, required recovery timeframes and hence the restoration priority for business operations;
- provide strategies to 'business as usual' (BAU) within agreed and acceptable timeframes;
- create action-oriented procedures to respond to the disruption in an efficient, effective and timely manner;
- establish principles and capabilities that are dynamic such that they enable the organisation to respond to variety of future disruption events; and
- periodically review, modify, update or revise the business continuity framework to account for new organizational risks.

How DPS manages business continuity

The policies, plans and guidelines through which DPS manages business continuity can collectively be called the *'BCM Policy and Framework'*. This framework enables DPS to demonstrate that a systematic and comprehensive framework is in place to ensure that business continuity is effectively managed in the event of a business disruption.

The BCM Policy and Framework provides for resources to be available to business areas to initiate temporary arrangements to continue delivering its most time-critical business processes.

DPS also provides key services, such as the provision of Information Communication Technology (ICT) services within and beyond the Parliament House in addition to maintaining facilities within Parliament House. These dependencies are considered part of the department's BCM Framework:

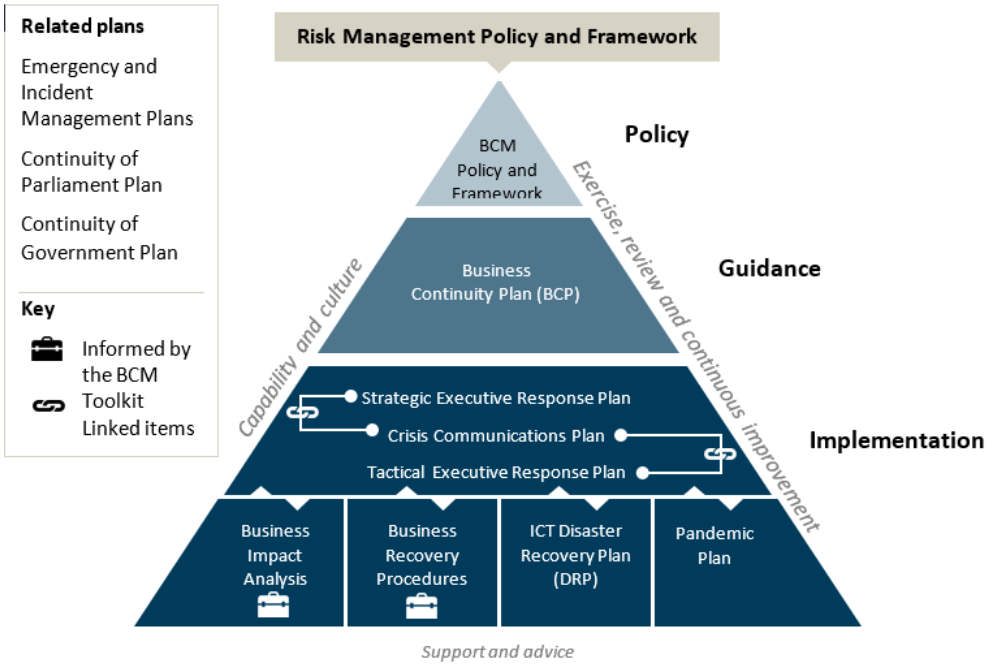

Figure 1: DPS BCM Framework

Steps undertaken in the review

DPS operates within a complex environment. Working in collaboration with the Department of the Senate, the Department of the House of Representatives and the Parliamentary Budget Office (PBO). DPS provides or facilitates the following:

- library and research services;
- information and communication technology services;
- security services;
- building, grounds and design integrity;
- audio visual and Hansard services;
- art services;
- visitor services;
- food and beverage;
- retail, health, banking and childcare services; and
- corporate, administrative and strategic services for DPS.

The department's BCM also links into the Continuity of Parliament (CoP) Plan[1], which necessitates close liaison with the other parliamentary departments and security agencies.

1 – Document review

The first step taken was to review the department's BCM documentation against best practice. While the documents reflected a good general business continuity capability from a high-level enterprise perspective, it was determined that DPS' business continuity framework needed to be tailored and made more specific to the department's business processes through a BIA project.

2 – Establishment of a review framework

As part of the BCM review, a framework was established which included the following aspects:

- A senior executive sponsor was allocated to ensure there was an advocate and executive owner for the project.
- A working group of subject matter experts from relevant business areas was established. These representatives were trained and mentored from early in the project in BCM best practice. This working group participated in workshops and consulted on all activities that aimed to improve the BCM function.
- A project outline was developed including a budget, project schedule, tasks/resource dependencies and project milestones.

3 – Conduct of workshops

Workshops were conducted to define each service (i.e. time-critical business processes, activity or operational process) and to test their resilience and response through Reviewing Scenarios. The workshops were designed to bring together the right people in one room to identify how related systems work together. These included interdependencies (such as timeframe, data and more) and the relevant communication protocols to ensure that relevant personnel are advised if a system is not functioning.

[1] The purpose of the CoP Plan is to outline the arrangements to support the operations of the Parliament at an alternative site in the event that Parliament House is unable to be used for this purpose.

It is important not to underestimate the amount of effort needed to prepare for workshops in order for them to be efficient and effective. A significant effort is also required to then analyse the output of the workshop. The workshops are detailed further below.

Workshop 1: Define the service

The first workshop sought to document the resilience and redundancy limitations of a service defined as a business activity or operation. This included the following areas of discussion:

- Clarification of the service's existing resilience and redundancy levels. This included defining reliant and interdependent services; type of controls and workarounds that can be put in place; and the effectiveness and timeliness of the response and recovery.
- The service's robustness and the impact on clients should it be limited or unavailable. The workshop included a discussion on the ability to replicate the service, existing redundancies and disaster recovery sites.

Workshop 2: Review scenarios, resilience & response

The second workshop focused on time-critical business services and processes including complexities that could increase the risks (threat scenarios) for teams supporting return to BAU.

Failure to deliver time-critical services could seriously disrupt the operability of the Parliament, the ability of Parliamentarians and Parliamentary Departments to conduct their business. This workshop was also used to work through a hypothetical incident and conduct a "fault tree" analysis.

A BIA was undertaken for other sub-services across the department. Information captured from these discussions included were:

- An estimation of each time-critical business service:
  - consequence level timeframes;
  - Maximum Tolerable Period of Disruption (MTPD); and
  - Recovery Time Objective (RTO).
- Identification of vulnerability scenarios, which provided input on:
  - how to respond especially when an incident is compounded and aggregated by other outside events, timing, multi-incidents, duration and external factors;
  - information for development of test scenarios, use cases and exercises; and
  - development of disruption continuity risk controls.

The outputs of these workshops were used to identify a list of key time-critical services and processes with their interdependencies, both internal and external, including third party suppliers, integrity of the ICT infrastructure and a list of systems that support them.

The team used the department's risk management framework and consequence rating description table, to support the development of BIAs using a predefined template applied to each time-critical business process.

4 – Using the workshop findings to establish the list of services

A key component of the workshop process was the work undertaken to identify and understand the time-criticality of each service and the impact of any given scenario on them. The following steps were taken to document the department's critical services:

1. business owners were assigned to each service, system and product;
2. workshops were used to determine what services and processes exist, and identify:
   - those that are within the department's control;
   - all possible disaster recovery activities which may be required in response to an ICT outage and where these activities have interdependencies with other government entities; and

    - those who will be impacted by an outage of a service? How big is the impact in terms of resource and cost? What does this mean to the importance/time-criticality of each service?
3. the services were then prioritised in order of their criticality aligned to the department's business objectives and endorsed by the Chief Operating Officer (COO); and
4. establishment of practical and realistic MTPDs based on the actual service recovery times or estimates provided by subject matter experts.

5 – Scenario testing

A number of BCM desktop exercises were run to practice, build confidence and fine-tune plans and procedures using individual and interdependent service disruption scenarios. The first of these exercises was utilised to stand up (assemble) the Continuity Co-ordination Group (CCG) – Division Heads, for the first time and to trial the Strategic Executive Response Plan (SERP). The exercise delivered a cascading scenario with the purpose of increasing familiarity in using the SERP and to generate ideas in order to facilitate continuous improvement.

The purpose of the second exercise was to road test the Tactical Executive Response Plan (TERP) – Branch Heads, involving the Incident Management Group (IMG). Once again, the exercise encompassed a cascading scenario, which was an extension of the CCG exercise, testing how participants would react as the scenario developed and what actions they would take.

A desktop exercise was run with the Hansard Business Continuity Team. This exercise highlighted that a business continuity incident involving this team could have broader impact on the department than the services delivered by the Hansard team.

The three levels of scenario testing highlighted a number of good practice and procedural opportunities that could be considered by agencies for incorporation into their business continuity planning. These included:

- develop a reciprocal Memorandum of Understanding (MoU) with another agency/department to accommodate interdependencies and ICT infrastructure for critical support staff;
- consider the storage of duplicate critical (hard and soft copy) documents for the activation of the BCP off-site, preferably at another agency/department that is geographically dispersed and that allows easy access. Plan to update the primary and secondary documents at the same time leading to 'a single source of truth';
- allow remote server access to ICT staff, so that BAU can continue insofar as practical;
- consider how media should be included in business continuity processes to avoid speculations and assist in consistent and factual messaging; and
- develop a standard agenda and situation reports (SitReps) that can be used during a significant business service disruption by the CCG, IMG or business recovery teams.

Practical tips

Clarify the relationship between your own BCP and related plans

In the complex environment in which DPS operates, it has proven essential to clarify the scope of DPS' BCP and its alignments with related plans, including those of the parliamentary departments, security and the CoP Plan.

Identify capability and training needs early

The teams that support the currency of the business continuity framework and capability must also continue to refresh their own understanding and proficiency on the subject. Early on in the review, key DPS staff undertook the week long Business Continuity Institute (BCI) training with an examination. This enhanced their ability to effectively undertake reviews and build DPS' BCM capability.

Identify if there is a need for a subject matter expert.

It may be necessary to engage a business continuity advisor and ensure skills/knowledge transfer occurs before the end of the engagement.

Secure an executive sponsor

Having an executive sponsor is critical to a project's success so that it has an ultimate decision maker and receives due priority from other stakeholders. Without executive sponsorship, the project may periodically fail to gain traction. A BCM functional officer should lead the project so that progress is maintained and issues are escalated to the executive sponsor in a timely manner when necessary.

An executive sponsor can also be useful for communicating the benefits of effective BCM to the wider department and can provide regular reports to Audit and other Executive Committees. Staff are far more likely to contribute to BCM if they understand why it is necessary and how it can contribute on both short and long term basis to the resiliency of their entity.

Balance the investment in BCM with the agency's risk appetite

It is important to develop a sense of what you are willing to invest in when managing your business disruption. This should inform the depth and breadth of investment in controls and BCM as an activity and any remediation activities identified during the risk management review process. Any investment decisions should consider if the potential significant business disruption risk is within the agency's risk tolerance or appetite.

Ask workshop participants to prepare in advance

To ensure that the most value is obtained from workshops and exercises, it can be useful to get participants to prepare in advance. In the workshops held with DPS, the business area representatives attending the workshops were asked in advance to come prepared to the workshops with:

- a list of services their Branch provides to Parliament House, parliamentarians, other building occupants and parliamentary departments;
- a list of known services the Branch has with interdependencies in other agencies/departments, and other internal or external parties in order to continually provide acceptable business services;
- two examples of BAU incidents that could escalate into an event which could affect the business of the Parliament;
- relevant documentation and/or knowledge which described the resilience and redundancy capability built into the services, including known limitations within the services, such as issues with infrastructure, staffing and knowledge management; and

- information on any new programs or mitigation activities that may update or impact on their time-critical business services.

Engage with other entities and Community of Practice

Seek advice from other government entities and learn from their experiences in reviewing or activating their business continuity framework. Engaging with the APS Business Continuity Community of Practice can be one way of sharing/gaining ideas, and learning/developing best practice.

Undertake regular scenario exercises

Regular scenario based exercises are important to build confidence and continue to refine your BCM processes and procedures. In DPS, regular exercises and ICT testing has helped mature DPS' BCM arrangements, and has proven essential so that key staff have their BCM knowledge and awareness refreshed.

Scenario exercises can also identify issues that may not have been captured otherwise, such as:

- confirming that emergency deployable laptops are running the correct standard operating environment with latest system updates;
- whether facilities at offsite locations operate as expected (security, speed of access, capacity, internet coverage etc.); and
- understanding the impact on staff of running operations under stressful or adverse conditions. For example, is there a need for rotational/staggered shifts to cope with resource shortages?

The use of external facilitators and external observers can also give these exercises additional credence, as they are impartial and may provide insights missed by internal staff.

Record lessons from an event or exercise

Exercises demonstrate the practical application of business recovery procedures and can be a useful way to identify improvements to the procedures.

For an event or exercise, log all significant business disruptions or near misses with issues arising in an incident recording system, if electronic, or a record book and on a whiteboard. This enhances visibility to CMG, IMG and concerned business recovery teams and provides an update at a glance of the event status. Where an event has occurred, record the actual outage impacts and elapse time before BAU. Circulate the lessons learned with appropriate staff and with the Risk and Audit Committee. After an event has been resolved store lessons in incident documents within a record keeping system.

Don't wait until it is perfect to test it

Scenario based exercises are designed to be an opportunity to learn, therefore avoid the temptation to wait until the BCM framework is perfect before testing.

DPS found that applying a rule of thumb of '80% complete and 100% operational' helped business areas finalise their business recovery procedures to 'be fit for purpose' rather than delaying to achieve a 100% perfect set of documents. Feedback from subsequent exercises is intended to identify continuous improvements to their business recovery procedures.

Maintain a close relationship between BCM and risk management

While effective risk management focuses on identifying risks and managing them before they can affect the organisation, BCM focusses on implementing measures to reduce the impact should a significant business disruption occur. For BCM, maintaining awareness of changes to operational risks can highlight which business owners managing time-critical business processes may require additional resources to focus on their business continuity.

Keep it simple

Keep BCM documentation as simple and practical as possible. This is particularly important when providing incident management guidance to executives. During a real crisis, too much information will be difficult to comprehend so try to keep it short, simple and diagrammatic.

As part of its incident management guidance, DPS has developed a simple checklist of expected actions for executives to follow during an incident, which has been attached to both the SERP and TERP.

Contact

If you have any questions or feedback in relation to this information sheet, please contact Comcover at comcover@comcover.com.au.

Use of this information sheet

Comcover's series of Risk Management Information Sheets are designed to be used as learning resources and are not mandatory.

It is important that entities develop risk management frameworks and systems that are tailored to the needs of their organisation. Entities may elect to adapt the concepts contained in this information sheet to suit their specific needs or use alternative methodologies.