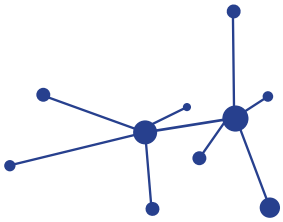


LABCoN

Legislative Assemblies Business Continuity Network

Managing Disruption:
Business Continuity for Legislatures

What this Guide Aims to Do

This guide aims to assist legislatures to mature as resilient organisations by developing and embedding a business continuity management (BCM) capability. Business continuity is the means to maintain urgent, 'prioritised activities' to a predetermined level in the event of a business disruption. By developing such a capacity, legislatures will evolve as confident, competent organisations able to continue to deliver critical services in a coherent manner when business as usual is interrupted.

This guide will aid legislatures in building a BCM programme by providing useful information on the concepts of incident management and business continuity, as well as identifying the essential steps necessary to establish a robust BCM programme in the context of a legislature. This guide is informed by ISO 22301:2012, the international standard for BCM, and the Business Continuity Institute's (BCI) *Good Practice Guidelines 2018*. Using the headings of the BCM lifecycle, we describe the key components of a BCM capability and provide examples of how these might look in a legislative assembly.

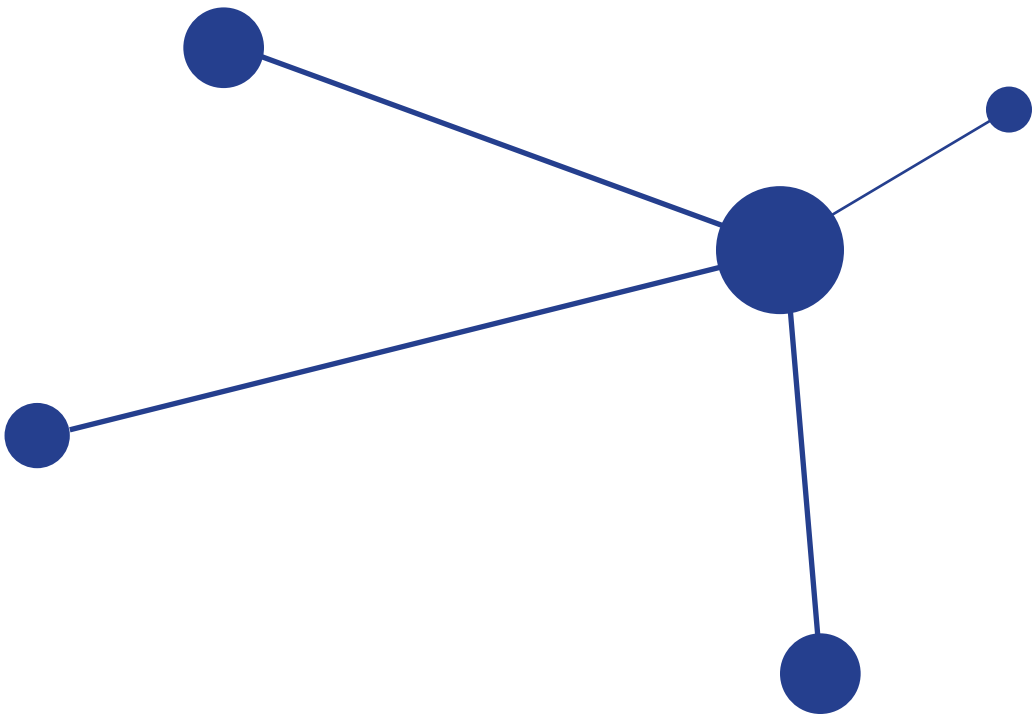
Who We Are

Formed in 2014, the purpose of the Legislative Assemblies Business Continuity Network (LABCoN) is to share best practices for the conduct of a BCM programme in a legislature. It does this through the documentation of benchmarks and the establishment of strong networks between participants who come from legislatures of different sizes from around the world.

The objective for LABCoN is to document the body of knowledge specific to business continuity in a legislative assembly and to make that available to other legislatures. The intention is to develop further guidance as our BCM capability matures. The field of BCM continues to evolve as new industry standards are developed. We therefore intend to update and improve this guide over time.

This guide has been produced by business continuity professionals who work in legislatures and who have shared good practice through meeting together as LABCoN. The UK Emergency Planning College (EPC) have kindly assisted in its production and the House of Commons of Canada in its translation into French.

Contents



Introduction

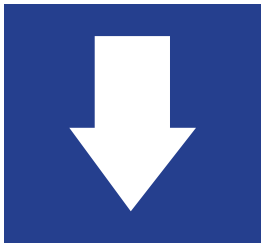
No organisation, including a legislature, is immune from experiencing an incident or a disaster. Indeed, every parliament is at risk of encountering a disruption to its critical business, either from a disaster, such as a natural catastrophe, or from a less significant problem, such as a power or technology failure. In addition, legislative assemblies may be more vulnerable to security-related incidents and cyber-attacks than other organisations. Some of these events could have a significant impact on the safety of parliamentarians, visitors and employees, on the assembly's assets, such as historic buildings, and finally on the legislature's ability to provide critical services to its parliamentarians.

In order to be resilient, any legislature, big or small, must anticipate risks, invest in preventing these, and prepare to respond and recover should they occur. Adopting business continuity management (BCM) ensures that an institution has the resources and information needed to deal with emergencies, and as such, is better predisposed to safeguard the institution's reputation.

As a key organisation, it is critical for a legislature to maintain a good reputation and credibility in a time of crisis. During a disaster or disruption, there would likely be significant public interest and media coverage on the event and on the legislature's response to it. Furthermore, the government, the Speaker and parliamentarians may still want the assembly to sit, perhaps with little time to prepare and in difficult conditions. A strong BCM programme allows parliamentarians and administrators to have confidence in the assembly's ability to continue fulfilling its critical duties despite a disruption of almost any nature.

Chapter 1: Getting started - Business Continuity Management (BCM)

Five key points to note at the start or review of a BC journey:



1. An effective BC capability needs to be driven from the top

This requires the BCM system to appoint a senior manager to have strategic responsibility for and to lead the BCM programme. It also means the top management team need to be actively engaged and that there is documented evidence of this engagement e.g. a BCM policy is in place, management reviews of the BCM programme take place annually, managers take part in the training and exercising programme, managers ensure BC responsibilities are resourced and monitored through performance appraisals, etc.

2. BC capability needs to be proportionate to the risks

This means integrating the BCM programme to strategic planning and risk management processes so that an appropriate response is prepared to both known risks and, by adopting a generic approach to managing the consequences of an incident, to unforeseen risks.

3. A BC manager or coordinator is needed to maintain the business continuity management system (BCMS)

BC involves the whole organisation which includes identifying the non-critical processes that can be suspended following an incident. The managers of the key services provided by the legislature know their part of the business so it is necessary to stress from the start that the BC manager's job is 'to help managers, manage'. This means BC needs to be done by the people responsible for delivering their services but the BC manager coordinates the various BC plans so that interdependencies are identified and the plans work in a coherent manner.

4. While BC is a journey, not a destination, clear milestones / basecamps are necessary to help monitor performance

BCM is a quality management system and, as such, it aims to continually improve over time; one never gets 'there'. It is necessary therefore to set clear objectives over time so that resources can be focussed and progress can be recorded using programme and project management techniques.

5. BCM is a necessary capability for organisational resilience but it is not sufficient

A BCMS needs to be integrated with the other organisational resilience components such as risk management, financial controls, business strategies, physical and information security, robust procurement arrangements, IT disaster recovery capability and supply chain management.

A BCM capability is made up of two core components: incident management and business continuity. BCM gives a clear plan for **what** will be done in the event of a disruption (business continuity planning) and **who** will manage the disruption (incident management planning). Since a major disruption may happen before completing the BCM lifecycle, let's start with incident management.

Managing a Major Incident

Events can, and do, take place that by their nature cannot be anticipated exactly. While the overall approach should follow a consistent methodology, response arrangements need to be flexible to adapt to the circumstances at the time while applying good practice, including lessons from previous emergencies.

Managing any incident comprises four main phases: **preparation** (preplanning); **emergency response** (mitigating an immediate risk or stopping things from getting worse); **continuity** (maintaining critical activities to a pre-determined level); and **recovery** (returning to a new normality, identifying lessons and learning from them).

An incident causing a disruption to a legislature sets three separate but closely related and often overlapping challenges:

These three activities are designed to control and minimise the immediate challenges arising from an incident. The recovery phase formally starts once the situation has been stabilised. However, preparation for the recovery phase should be an integral part of the incident management process and should be considered alongside crisis and consequence management in the early stages of a response. In contrast to the response phase, the recovery process can take a considerable amount of time (weeks or months), as it seeks to support affected business units in the potential reconstruction of the physical infrastructure and restoration of emotional and physical wellbeing of staff affected. Media management is also required at each stage of an incident to ensure the legislature not only manages incidents effectively but is seen to do so in a competent manner.

The key elements of an incident management plan require attention to the following issues:

a. Levels of response: **operational** (following standard operating procedures to address routine incidents); **tactical** (using an incident management team to coordinate the consequence/impact management between business areas following a major disruption); and **strategic** (senior managers, sometimes forming a crisis management team, to set the strategic direction following a major incident) – there is a need to identify how disruptions are escalated from operational to tactical and then strategic;
b. Define the membership of the incident management team (IMT) – what roles need to be represented at the meeting to manage the incident effectively, regardless of its cause;
c. Where the IMT will meet (physically and/or virtually);
d. How communication takes place, internally and externally;
e. The authority of the IMT and escalation processes if the incident continues to develop;
f. A training programme to ensure all those who may be involved in managing an incident are competent.

The core characteristics of effective incident management are :

1 DIRECTION	Clarity of purpose should be delivered through an awareness of the strategic aims and supporting objectives for the response. These should be agreed and understood by all involved in managing the response to an incident in order to effectively prioritise and focus the response.
2 COMMUNICATION	Good two way communication is critical for an effective response. Reliable information must be passed correctly and without delay between those who need to know, including the public.
3 SUBSIDIARITY	Decisions should be taken at the lowest appropriate level, with coordination at the highest necessary level.
4 CONTINUITY	The response to a major incident should be grounded within the legislature's existing functions and its familiar ways of working –although inevitably, actions will need to be carried out at greater speed, on a larger scale and in more testing circumstances during the response to an incident.

5 INTEGRATION	Effective coordination should be exercised with key stakeholders.
6 PREPAREDNESS	All individuals and teams that might have to respond to an incident should be properly prepared, including having clarity of roles and responsibilities, access to resources (equipment, IT, purchasing authority), specific and generic plans, appropriate incident management facilities and periodic rehearsals of response arrangements.
7 COOPERATION	Positive engagement based on mutual trust and understanding will facilitate information sharing and deliver effective solutions to issues as they arise.
8 ANTICIPATION	In order to anticipate and manage the consequences of all kinds of emergencies, planners need to identify risks and develop an understanding, where possible, of both the direct and indirect consequences in advance.

Incident Management versus Business Continuity

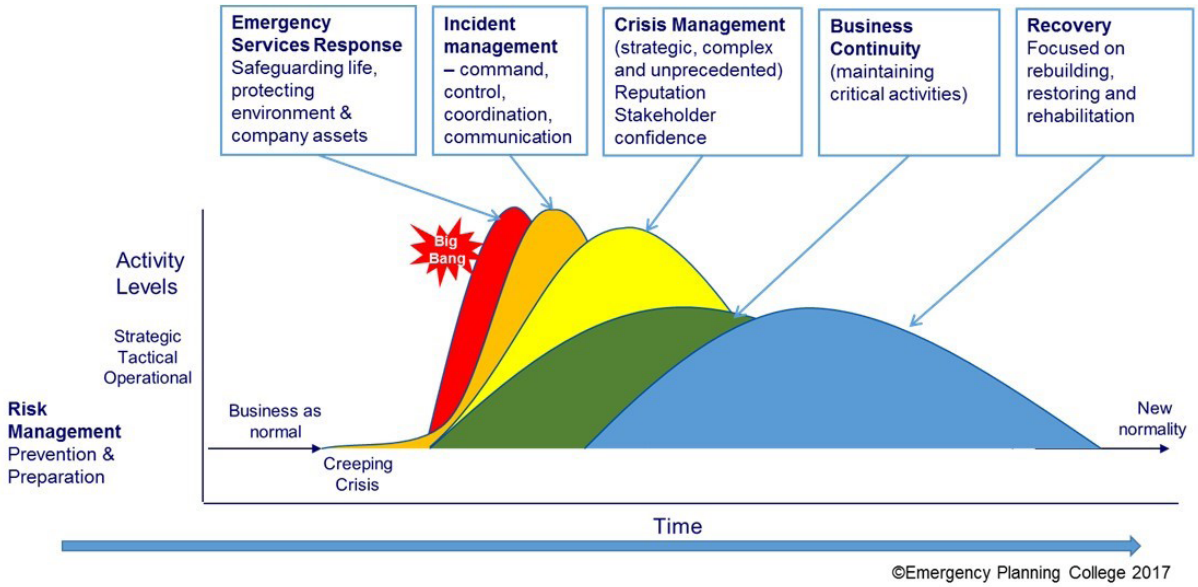
Before going onto details, it is important to define what is meant by the term business continuity management (BCM). The international standard (ISO 22301:2012) defines BCM as the:

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

While this definition is comprehensive it is also valuable to have shorter descriptions such as 'BC is our capability to address **what we would do if…**' Such a statement begins a dialogue with stakeholders as they consider how they would respond to a range of business disruptions.

BCM and Other Resilience Capabilities

A robust **risk management** process anticipates and assesses risks to the organisation. These risks should be mitigated through preventative measures such as 'target hardening', training of personnel, and information security systems. Having worked on preventing the risk materialising, organisations must still be ready to respond and recover from a business interruption, **regardless of its cause**. There are several phases in a response which are summarised in this table.



EMERGENCY RESPONSE	deals with the *immediate impacts* of an incident, a relatively short-term phase that focuses on ensuring people and the environment are made safe.
INCIDENT MANAGEMENT (IM)	outlines how the organisation will *manage the consequences* of the business interruption. IM covers **who is in charge**, how to keep stakeholders informed, escalation processes, coordination of resources, etc.
CRISIS MANAGEMENT	delineates arrangements to manage *strategic, complex and unprecedented* events. It is rarely standalone and will require integration with other disciplines. Note that an incident may require a crisis management response without a BC activation e.g. in the event of major negative media attention about the legislature (a 'big bang' effect). In contrast there may be a 'creeping crisis' where a disruption such as an IT refresh fails and, if not managed effectively, turns into a crisis. The incident response arrangements must be flexible enough to manage both an operational disruption, which may need to be escalated, and a crisis which requires immediate strategic leadership.

Business Continuity (BC)	outlines the arrangements developed, by following the BCM lifecycle, to maintain critical/urgent business activities to a pre-determined level, i.e. **what will be done**. The analysis phase of the BCM lifecycle sets out the recovery time objective, the maximum acceptable outage and the minimum business continuity objective (i.e. level of service) for each critical activity.
Recovery	is of longer duration and involves wider stakeholder engagement. It details the priorities for recovery, i.e. what, how and in what order recovery to the new normality will happen following a disruption.

Response and recovery usually overlap – there is a transitional phase. After each activation of resilience arrangements, a formal debrief should be conducted to identify lessons opportunities for continuous improvement.

Although BCM is a relatively new discipline, it can, when implemented effectively, protect a legislature's reputation and help manage disruptions to the services provided to Members. People notice when an organisation is able to continue to provide key products and services during a disruption when other organisations fail to do so. Building a reputation takes time but it can be lost very quickly if a legislature is perceived to have failed to plan for disruptions to its business. Protecting reputation and maintaining the trust of external stakeholders is perhaps the most valuable part of having operable business continuity plans and a capable incident response mechanism.

It is recognised that a well-developed BCM capability can enable an organisation to respond to a business disruption in a coherent and consistent way. Other benefits that can also be delivered with the implementation of a BCM programme, including finding single points of failure, as well as identifying duplicated business processes and obsolete software packages that are still being supported.

Building a resilient organisation begins at the top of the organisation. BCM provides the framework to enable a legislature to focus its resources more effectively to ensure that business-critical activities are protected. BCM capability will help to ensure a more coherent response to a disruption. Parliamentarians will feel confidence in belonging to an organisation that foresees and invests in their needs. Employees too will feel that they work for a competent, confident organisation that anticipates and plans for business disruptions.

Where to Start with a BCM Programme?

The *BCI Good Practice Guidelines* provide the core elements to be addressed as part of a BCM programme. Each of these elements and their associated activities are described below.

Business Continuity Lifecycle
(from the BCI Good Practice Guidelines 2018*)*

Policy and Programme Management

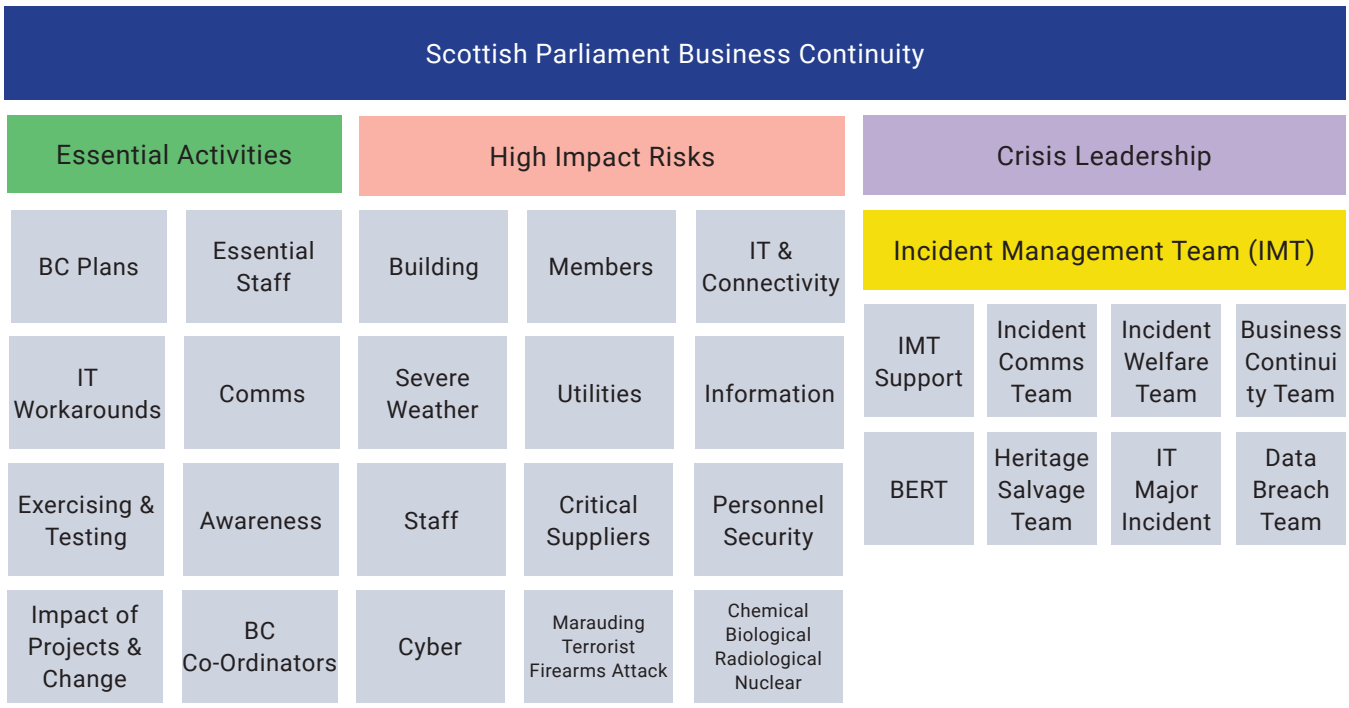
A key success factor in delivering an effective BCM programme is to have the appropriate governance arrangements in place. This includes having a nominated senior manager responsible for strategic leadership of the programme. Legislatures also require other key roles such as a BC manager, a BC steering group, departmental champions, and BC plan owners and authors. These roles and the objective of the BCM programme need to be documented in a BC policy.

Success with BCM requires commitment from the highest levels of the organisation at each stage of development. Programme governance, principles and responsibilities may be set out in policy to encourage common understanding and commitment, leading to successful development, implementation and maintenance.

Embedding

This component of the BCM lifecycle involves raising awareness of BC arrangements and integrating BC aspects into business change activities throughout the legislature. This means training all those with a role in the arrangements and then exercising the plans so that management and staff have confidence in them, as well as ensuring that project management, business change and procurement activities consider BC requirements at the start of each piece of work. The training programme is to ensure that staff are competent (i.e. they have the knowledge, skills and attitudes to fulfil their responsibilities), and the exercising programme ensures the plan will 'work as anticipated' (see the Validation stage).

Example of a BCM Programme Structure



Analysis

The starting point in developing an effective business continuity plan is to analyse what prioritised activities are undertaken to deliver the key products and services in an area of the business: **what** are the critical services, **who** does them, **how** is the service provided, **when** does it need to be provided, **why** are the services needed and **where** does this work have to be done.

Definition of a Prioritised Activity

All the services provided by the different business areas of the legislature are important but some are more critical than others. 'Critical' refers to those activities which, if lost or interrupted, would hurt the organisation the most, in the shortest period. Once the critical activities have been determined, consideration can be given to designing solutions to ensure they can be maintained in the event of a disruption.

To start, a list is drawn of all the functions of a department / office, followed by the question. 'If it were impossible to provide a service, who would notice and how quickly would they notice?' This will help identify the most critical activities that impact the business of the chamber or committees or which have a detrimental effect on other critical services provided by a department. If a service can wait, e.g. an audit can be put off for a week, then this is termed a non-critical activity and a plan for it is not necessary. If, however, a failure of one of the key functions would quickly have a detrimental impact on the business of the chamber or committees then a plan for such an event is necessary.

This process, referred to as a business impact analysis (BIA), will identify top critical/prioritised activities. The organisation should determine how many critical activities are manageable for its business areas. For example, a larger legislature may decide to have up to six critical activities per plan, while for others having fewer than six, even just one or two, could suffice. A plan with more than six critical activities may be difficult to manage, so splitting a business area up into smaller units may be preferable. An example of a BIA is provided below, but this can vary between organisations and must be adapted to the size, complexity and culture of the legislature.

Example of a BIA template

CRITICAL ACTIVITY ONE								
Critical Activity		Timing & Impact Score	Impact on chambers	Impact on committees	Impact on departmental operations	Explanatory comments if high impact has been selected	Is this activity affected by the parliamentary sitting calendar?	
1		1-4 hours					Is this activity affected by other calendar cycles? e.g. financial calendar	
		5-24 hours						
Max. Tolerable Outage	Recovery Time Objective	25-72 hours					Do all key staff/deputies need to be co-located to carry out activity?	
2	3	72+ hours						

KEY STAFF DETAILS						DEPUTIES DETAILS					
Staff Name	Number of desks required	Is home working currently possible?	Do you currently have remote access to the parliament network?	Are there any home working limitations that affect this critical activity?	Are there any non-IT specialist equipment required?	Staff Name	Number of desks required	Is home working currently possible?	Do you currently have remote access to the parliament network?	Are there any home working limitations that affect this critical activity?	Are there any non-IT specialist equipment required?

IT AND RESOURCE DETAILS					BUSINESS INTERDEPENDENCIES			
Key Server Based Systems and Application	Recovery Time Objective	Recovery Point Objective	Key Desktop Applications	Vital Records, Key Intranet Sites and External Links	Name of Business Area/Government Department/Supplier	Contact Name	Impact of Loss of Service	Contingency
			4					

(See also Chapter 3, Section on *Activities of a Legislature*, for more information on BIAs)

1. Critical activity

These are the things a department/office does which, if lost or interrupted, would have an immediate detrimental effect on chamber, committee or departmental business. 'Detrimental' refers to a service whose failure would result in a parliament being unable to sit. Considerations should include (1) Someone could get hurt if the service is not provided; (2) The legislature's reputation would be damaged; (3) Failure to undertake the activity could put the organisation in breach of regulatory requirements; or (4) The disruption could have major financial implications.

2. Maximum acceptable outage (MAO)	This is an estimate of how long the legislature could go without providing a key service before its reputation is lost and extraordinary measures need to be taken. The MAO should be set by senior managers so that BC arrangements can be planned to meet the required time limits.
3. Recovery time objective (RTO)	The RTO is the stated aim of a plan to get the service up and running after a disruption, e.g. within minutes, an hour, a day. The RTO must be less than the MAO. The plan will then include the recovery of the activity within the stated RTO.
4. Vital records, key intranet sites and external links	This is each business area's list of key documents and resources needed to fulfil its responsibilities.

Design

The design stage of the BCM lifecycle identifies the strategies and tactics to be developed that will enable the business-critical activities to be maintained and recovered within the recovery time objectives determined in the analysis stage. The activities at this stage include assessing the options to manage the loss/denial of staff, premises, utilities, information, information technology, equipment and key suppliers. These options are then assessed for appropriateness and subjected to a risk assessment before the strategies and tactics are agreed by senior management. For example, alternative locations to work in can be identified should the usual workspace be out of action, and employees can be trained to undertake a range of duties so that the organisation can cope when some staff are unable to get to work.

Once these alternative arrangements are agreed by senior management, they should be documented in the next phase of the BCM lifecycle, 'implementation', which produces business continuity and incident management plans.

Implementation

This section will help business continuity plan (BCP) owners and authors to complete their plan by explaining exactly what is required in each section.

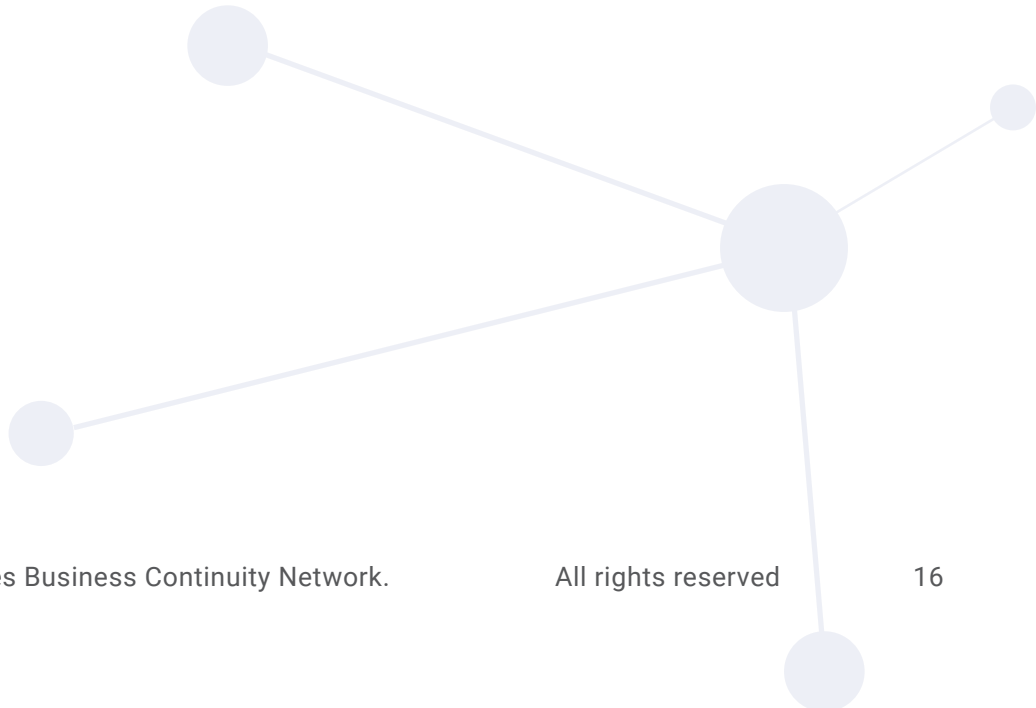
Definition of a BCP

A BCP is a documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable the legislature to continue to deliver its critical services at an acceptable predefined level.

The various parts of the business, which enable the legislature to function, differ in their size, location, and complexity. However, they all have to fit into one standard BCP template. Doing this enables all results to be analysed and interdependencies to be identified. Therefore some discretion may be necessary when developing a standard template. It may not fit a business area perfectly, but there is a huge benefit in everyone taking a standard approach.

Roles and Responsibilities

The role of the BCP author is to complete the plan and the BCP owner is responsible for its content. However, it is important that all staff in the business area contribute to this process of determining what are the most critical things they do, and to record what they might do if normal services are interrupted. There is a logical progression from the BIA to the BCP and key staff should be consulted throughout the process. After agreeing on the list of critical activities and considering options to manage them in the event of a disruption, the BCP should also detail the requirements that follow below.



Location and Contact Details

This section of the BCP simply contains a list of all the employees involved in the delivery of critical activities and how they may be contacted in the event of an incident. A record of relocation points is also necessary in order to carry on delivering key services. The location points should also list an alternative site if the activity is critical. An exercise should be run to ensure the alternative locations identified are suitable for the organisation's purposes.

Incident Response

In the BIA, an analysis is conducted of what a business unit does, who does it, and where they do it. This section contains a record of the plan for managing an incident affecting a business. This should be integrated within a wider incident management plan. It is good practice to identify a leader and two deputies so that absences are covered. Employees need to be made aware that they are named in the plan and that they have responsibilities.

5. Checklist of actions

What tasks need to be done in the event of an incident and in what order?

6. Cascade list

This section may duplicate the list of the people identified in the section on critical activities. However, there may also be other key internal and external stakeholders who should be consulted during an incident. This section should clearly set out who will be informed and how to ensure all relevant stakeholders are informed.

1.CHECKLIST OF ACTIONS TO BE UNDERTAKEN							
	Actions	Who? (up to 5 people)					
1	Account for staff 5						
2	Establish recovery priorities						
3	Establish availability of key staff						
4	Cascade messages to all staff						
5	Contact stakeholders						
6	Establish frequency of meetings of Incident Management Team						
7	Provide Status Report						

2. ARRANGEMENTS FOR CASCADING MESSAGES TO STAFF						
	BCP leader (Initiate call)	Name of staff (to receive call)	Responsibility - Covers which areas?	Office Telephone	Mobile Telephone	Home Telephone
1	Incident Management Team (IMT)	6				
2	Incident Management Team (IMT)					
3	IMT Member					
4	IMT Member					
5	IMT Member					

The section above is about incident management, i.e. command and control – **who** will make the decisions and be responsible for different areas of work. The section below on risk and contingency is about **what** specific things will be done in the event of the scenarios below.

Risk and Contingency

It would be wise to spend some time as a team thinking through how the organisation would react if faced with one or more of the scenarios below and document the steps taken. In a real incident, it may not be possible to follow these generic plans step by step, but the value is in thinking about the issues and working out a basic plan of action outside of the crisis.

7. Denial of access to the premises

What are the options if people can't get into the legislature's building(s) or offices? Where else might they go? A record is kept of appropriate potential venues to host critical activities.

8. Denial of IT/ facilities/equipment	What can be done if certain pieces of equipment fail; what's plan B? What if everything is working but IT goes down? What tasks can be accomplished on standalone lap-tops or manually on paper?
9. Denial of people	This part of the plan follows an analysis of the personnel required to deliver critical activities: How many staff are needed? What competence do they need? Can staff from other areas participate? Rather than improvise on the day of the incident, a BCP should record the actions that could be taken. This may mean putting arrangements in place and seeking agreements from other parties about how it will be managed if, for example, half of the staff are unable to work. Depending on the scope of the BCM system, a plan for a denial of Members and their staff may also be required.
10. Denial of utilities	Considerations may start to overlap at this point, but any special arrangements in place if a building loses power or water should be noted here, e.g. is there a generator? Building managers may be able to help with this planning but they may not know how critical some activities are unless a BIA has been completed and explained to them.
11. Denial of third party suppliers/external dependencies	This section requires the identification of internal and external dependencies and the plans in place to cope with a disruption to **their** services. The more critical the activity, the more work is needed in this area. This might involve going down a supply chain and involving procurement staff in ensuring that key suppliers also have business continuity arrangements in place.

Supplementary Plans, Information and Links

This section contains other useful information that may be referred to in an incident.

12. Supplementary plans

Some business areas will not only have BCPs on their own activities, but will also contribute to the wider response to large-scale disruptions, e.g. the Facilities and IT departments will be heavily involved with setting up at any new location while the Clerk and chamber's staff may have responsibilities after the death of the Head of State.

13. Useful links/ Important sources of information

Some business areas will have a range of internal and external stakeholders who will need to be informed/involved in an incident. Their details should be recorded here.

Finally, once a BCP is completed, it should be stored on a central database. Exercises are conducted to test if the plan works and the findings are recorded. Quality assurance of a plan is essential to ensure it remains fit for purpose.

Validation

This stage of the BCM lifecycle requires the development of a programme to review arrangements and exercise plans. The review process includes auditing and undertaking a management review at least annually to ensure the BCM system is effectively maintained. A key component of this is developing an exercising programme.

BCM arrangements cannot be considered reliable until they are 'exercised' and have proved to be workable. 'Exercising' should involve: validating plans, rehearsing key staff, and testing systems which are relied upon to deliver resilience. The frequency of exercises will depend on the key services a department/office provides, but should consider the rate of change (to the organisation or risk profile), and outcomes of previous exercises (if weaknesses have been identified and changes made). Plans should be exercised annually.

The international standard for BC arrangements (set out in ISO 22301:2012) states that the organisation shall exercise and test its BC procedures to ensure that they are consistent with its BC objectives.

'The organization shall conduct exercises and tests that:

a. Are consistent with the scope and objectives of the BCMS;
b. Are based on appropriate scenarios that are well planned with clearly defined aims and objectives;
c. Taken together over time validate the whole of its business continuity arrangements, involving relevant interested parties;
d. Minimize the risk of disruption of operations;
e. Produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements;
f. Are reviewed within the context of promoting continual improvement; and
g. Are conducted at planned intervals and when there are significant changes within the organization or to the environment in which it operates.'

(ISO 22301:2012 clause 8.5).

How to Test A Business Continuity Plan (BCP)

The BCI *Good Practice Guidelines* suggest building an exercise programme using a range of the following formats:

Discussion-Based

A verbal discussion covering all aspects of the plan with the team(s) that are involved with that plan. This exercise is really asking 'Does the plan make sense?' Any changes to the plan will be identified in the post-test report and incorporated into plans as a matter of priority.

Table-Top

The full team are verbally challenged on aspects of the plan by being taken through imaginary, but realistic, scenarios that involve the loss of skilled staff, loss of IT, data and communications, loss of access and loss of third parties (where appropriate). The team will be required to discuss options and agree on ways forward. Any changes to the plan will be identified in the post-test report and incorporated into plans as a matter of priority.

Simulation or Command-Post

Simulation exercises can involve *players* at operational, tactical and strategic levels where the participants are located at their usual place of work across the whole organisation. The advantage of this type of exercise is that information flows can be tested as emails and phone calls are used to simulate a real incident.

Live

The full team will undergo a simulated exercise that will incorporate external and internal *players* that will make the exercise feel as real as is possible. The scenario will focus on grey areas or weak areas of the plan to determine if there are gaps in provision or any invalid assumptions. Where possible, exercises will also enhance the awareness of the *players'* own business continuity areas of responsibility and their own BCP.

Test

This is an exercise that has a pass/fail element and is used to test plans like an IT disaster recovery plan or plans that have service level agreements relating to provision of resources within specified timeframes. Whatever type of exercise is opted for, it is worth considering inviting other stakeholders and those that are relied on to deliver key products and services. It is also important to record and evaluate the event, through a debriefing immediately after the exercise and then written up in a lessons identified report with actions, if required.

Key Steps in Delivering Business Continuity Exercises

1. Setting the scope and objective of the exercises. This sets out what is exercised, who should take part and how the outcome of the exercise will be assessed (what will 'good' look like?).
2. Choosing the most appropriate type of exercise and resourcing this accordingly.
3. Organising the time and venue and letting the participants know what they need to do to prepare for the exercise.
4. Delivering the exercise.
5. Debriefing the exercise to capture what worked well and what needs to be improved.
6. Completing a 'lessons identified' report, including action points with dates for completion.

Sample – Business Continuity Exercise Topics and Schedule

Name of exercise	When	Type	Scope
Alcatraz	November 2011	Simulation or Command-Post	Response to a wholesale loss/denial of IT service.
California	October 2012	Simulation or Command-Post	"White powder" incident in Chamber and "sit-in" protest.
Chehalis	March 2013	Table-Top	Operation of incident management team and secretariat at alternative location.
Copenhagen	March 2016	Table-Top	Operation of the incident management team and secretariat.
Edinburgh Rock	February 2011	Simulation or Command-Post	Building fabric issues caused by local flooding.
Nevada	October 2014	Simulation or Command-Post	Disturbances across the Parliament, including the Chamber.

Pandemic	March 2008	Simulation or Command-Post	Assessing the impact on staffing following a typical pandemic infection pattern.
Pescadero	April 2012	Simulation or Command-Post	Management of the recovery from fire and operating away from Holyrood.
Rembrandt	March 2015	Table-Top	Impact of evacuation on evening events and welfare of staff and event attendees.
Tiburon	October 2011	Table-Top	Impact on staffing and Member attendance due to transportation disruption after severe weather.
Kolob Canyon	September 2017	Simulation or Command-Post	Response to a cyber incident.
Windhoek	December 2017	Table-Top	Recovery of heritage items after building disruption.
Spectrum	May 2017	Training & Table-Top	Incident management training for IT staff coupled with a Table-Top exercise of IT issues across the Parliament.

This chapter provided the basic knowledge on BCM. Successive chapters will give additional information and resources on how to start building plans and capability based on the contributing legislatures' experiences.

Chapter 2: Governance - Who Does What

A governance framework usually includes:

- mission statement;
- policy;
- scope;
- standards;
- roles and responsibilities;
- reporting mechanisms to track key performance indicators and manage the progress of key BCM activities; and
- communication protocols to maintain awareness and outreach.

The established governance of a BCM programme creates the foundation for the programme by defining a designated reference point of accountability for the creation, implementation, monitoring, testing/exercising and maintenance of the plan. Establishing support from the highest level of management within a legislature is critical. This ensures that management continuously drives programme implementation and monitors/validates the programme performance and outcomes.

Defining who is responsible for BCM plans is different from who is responsible for BCM planning. It is critical that responsibility for planning sits with everyone, but particularly with all department heads and those responsible for providing services and resources that allow the legislature to successfully function. To this end, consideration should be given to how the BCM planning activity is governed through the use of organisational structures and a subject matter expert.

The following questions may help in framing a governance structure:

1. Will the responsibility sit as part of the duties of department heads?
2. Will the responsibility be delegated to specific roles in each department?
3. Will there be an overall corporate role that has responsibility for BCM planning?
4. Should that corporate role be skilled in governance and audit as well as being a subject matter expert for business continuity/resilience?
5. If a central BCM role is created, where will that role sit in the organisation?

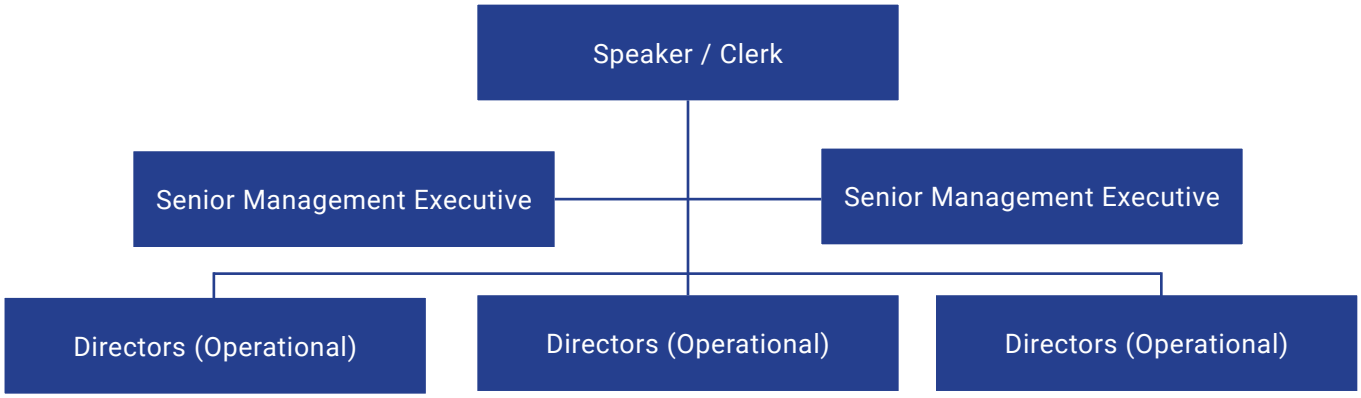
Wherever that role sits, it needs to have authority and direct support of senior managers and the Chief Executive/Clerk. To succeed and become embedded in organisational culture there must be a 'Champion' showing a visible and active commitment to the BCM process at the highest level to reinforce its importance and expected outcomes. The following five key elements will assist with developing a governance framework.

Defining Roles and Responsibilities within the Programme

The legislatures that are part of LABCoN share the same type of BCM progamme that contains a governance structure and operates under a hierarchy-reporting configuration with clearly defined roles and responsibilities.

As outlined below, the level of the decision-making accountability determines the composition of each team. The structure resembles a pyramid-style flowchart in which the starting or pinnacle position has the highest authority or scope of decision-making that filters down to various support level functions.

The terms used to identify the various teams are determined by each legislature's established organisational structure.



Roles and Responsibilities related to this structure may include:

Senior Leadership (Clerk of the Legislature; act as a senior member or lead (ex-officio) of the executive team):

- Determining the acceptable scope and impact of disruption to the 'normal' delivery of the legislature's services;
- Determining if BCPs (and extent) are required to be activated;
- Activating the executive team as required/applicable;
- Responsibility for communication/notification to Speaker, executive team and key stakeholders as applicable; and
- Final authority for a designated course of action, with the exception of the responsibilities that lie with external emergency services.

Executive Team (made up of the senior management, reporting to the Clerk):

- Protecting and preserving the institution's assets and resources;
- Assigning key functional personnel to required roles;
- Protecting the institution from the occurrence and consequences of:
    - Loss / denial of life, injury, and psychosocial trauma;
    - Business interruption;
    - Loss of information;
    - Inadequate protection of assets and resources; and
    - Cyber-related issues.

Steering/Operational Team (middle management level):

- Defining objectives, structure, policies and charter for the BCM programme;
- Providing guidance and oversight for the BCM programme;
- Providing the resources necessary to support the BCM programme;
- Providing input into and approval of BC projects objectives, scope and timeframes;
- Assisting in the definition of roles and responsibilities;
- Providing support for business continuity projects and the business continuity coordinator; and
- Providing coordination and support for plan development.

BCM Programme Coordinator/Lead:

- Providing support and advice to the Clerk, executive team and steering/operational team as required;
- Coordinating meetings of the executive and steering/operational teams;
- Assisting in maintaining and operating the emergency operations centre (EOC);
- Developing emergency messaging and communications for staff as required; and
- Coordinating with appropriate staff, management and stakeholders.

The RACI chart below is an example of how to capture roles and responsibilities related to BCM planning.

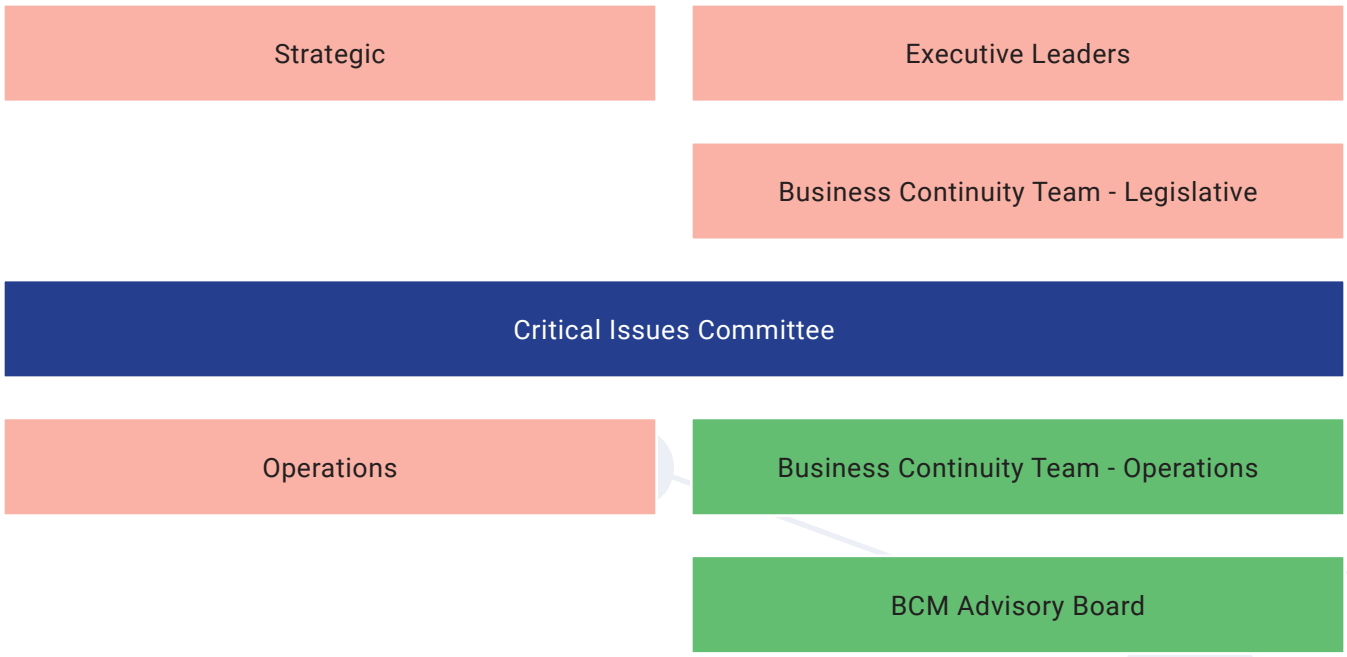
RACI CHART EXAMPLE

R	RESPONSIBLE : Person (s) responsible for doing the work
A	ACCOUNTABLE: Person accountable for signing of the work (max 1)
C	CONSULTED: Person consulted before and during task
I	INFORMED: Person informed of work progress/completion

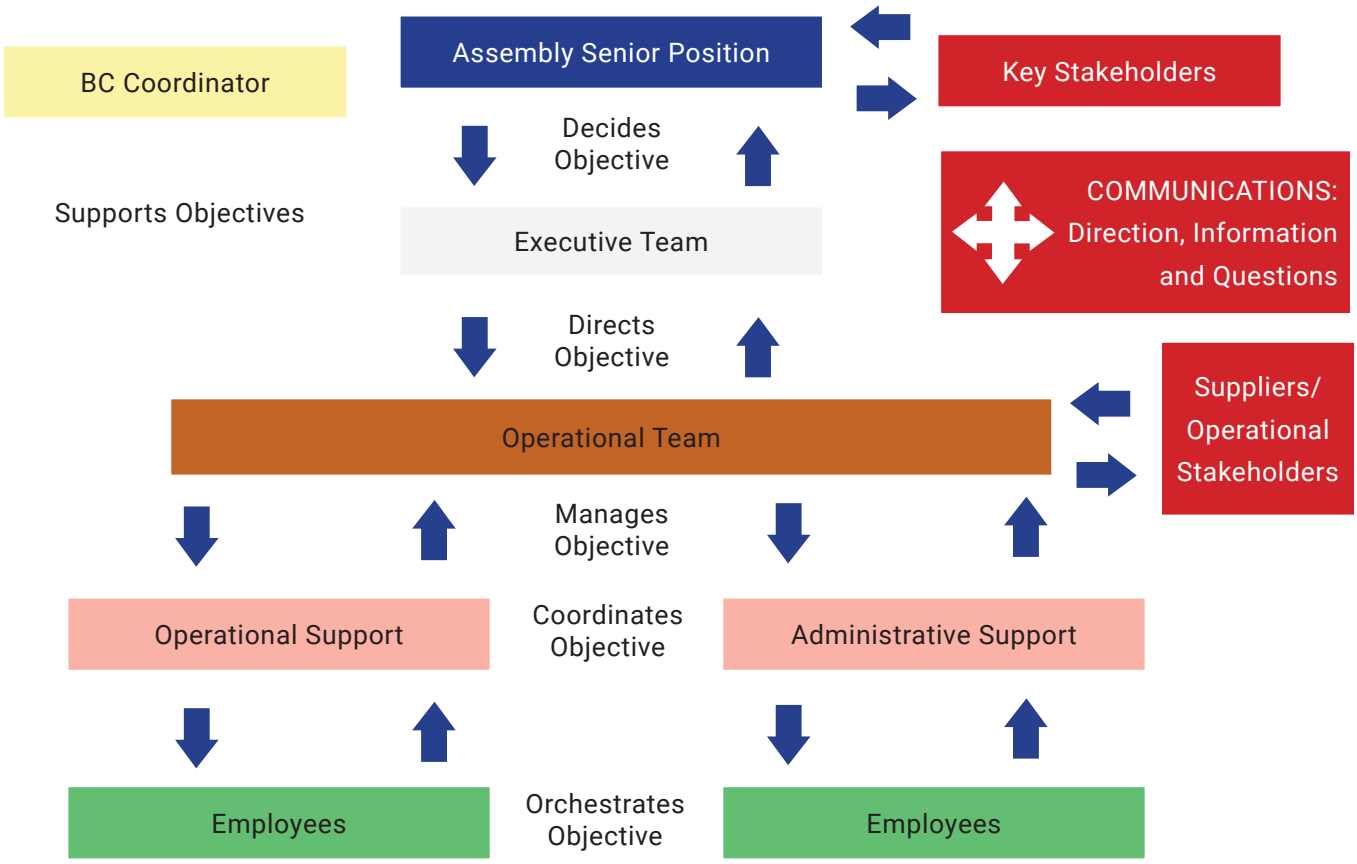
Functional Roles and Responsibilities Analysis

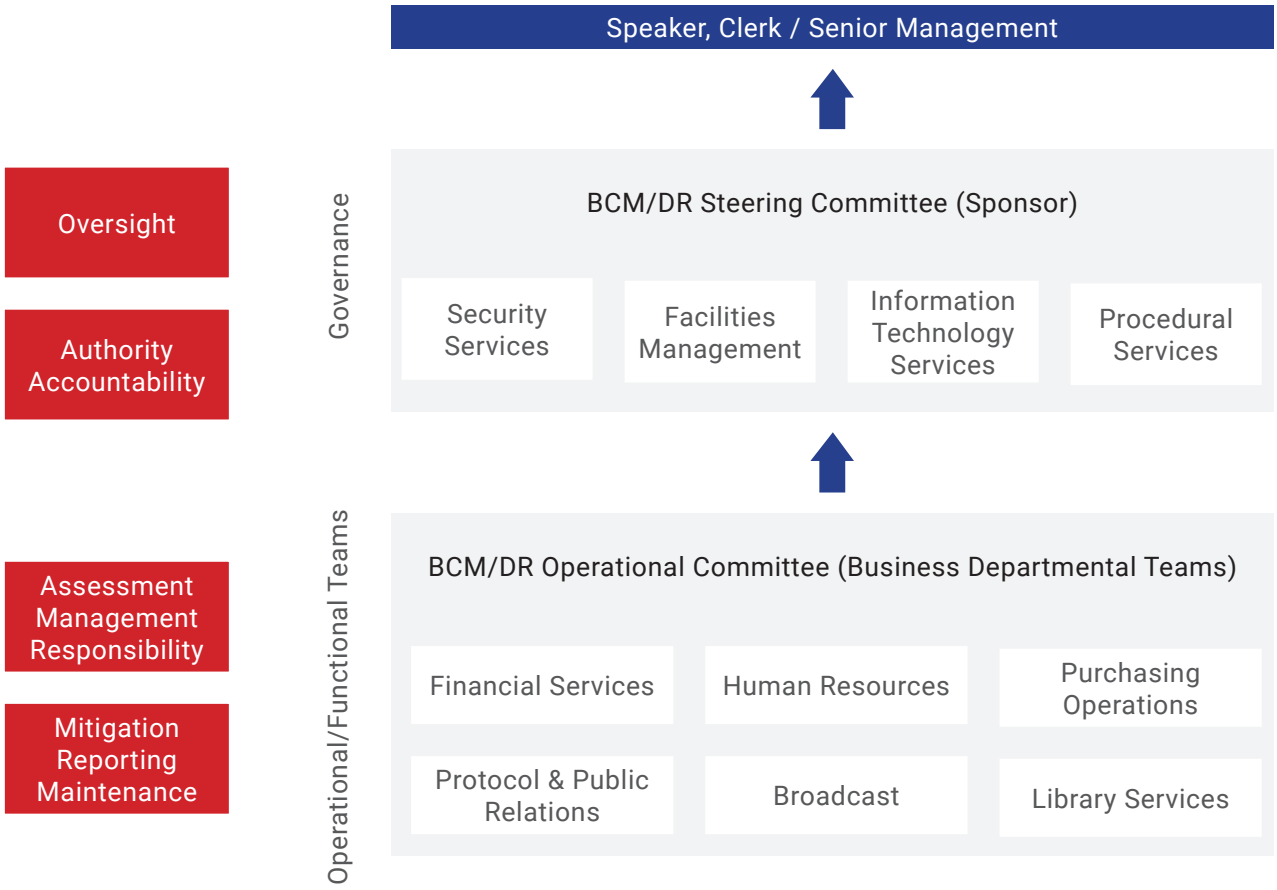
	Leadership				Department Heads				External Resources			
BUSINESS PROCESSES												
Decisions/activities	R	C			R	C			I	I	I	I
Reporting			A	I								

Examples of BCM Governance Structures



Without management support and the proper resources, the programme is stagnant; having support in principle only is not enough. Past experience has shown that different levels of management don't always share a consistent approach to handling situations. This gap can be addressed through policy and training.





Establishing a BCM Policy

The policy will need to be developed based on the unique needs, environment and potentials for business interruptions related to each legislature. The policy statement communicates the principles to which the legislature aspires by outlining the purpose and objectives of the BCM programme, and guiding the integration and coordination of efforts between business continuity, disaster recovery, and crisis/emergency management, working closely with administrative units and departments. A strong programme policy statement should be succinct while also providing necessary programme details against which its performance can be measured.

Excerpts from the Legislative Assembly of Ontario's BCM Policy:

Statement:

The Continuity of Operations Plan (COOP) for the Office of the Legislative Assembly (OLA) is designed to ensure that the Assembly and its committees can continue to perform their functions and dispatch public business, albeit with possibly fewer or minimal resources, or in an alternate location if absolutely necessary. It defines the requirements, strategies and proposed actions needed to respond to emergency events that could impact the critical business activities of the Assembly. The plan provides a governance structure for

the OLA during and after an event and outlines actions and procedures for responding to an interruption.

The plan is designed to minimize the operational and financial impacts of emergency incidents by establishing the recommended organization, actions, and procedures needed to:

- *Recognize and respond to an incident;*
- *Assess the situation quickly and effectively;*
- *Notify stakeholders about the incident;*
- *Organize response activities; and*
- *Support business recovery efforts in the aftermath of the incident.*

Plans:

Each branch is responsible for the creation and maintenance of comprehensive business continuity plans (BCP). When implemented, the plan should include those procedures and support agreements, which insure on-time availability and delivery of required products and services. Each plan must be reviewed annually to ensure accuracy and compliance with the established business continuity objectives for the Assembly.

Policy Leadership:

The OLA responsibility for evaluating the impact of an emergency incident and for activating the COOP, in whole or in part, if required is decided at the Executive Team level (or by their designate). The Executive Team consists of the Clerk, the Sergeant-At-Arms and the Executive Directors of the Legislative Services Division, the Administrative Services Division and the iDivision. In the event that members of the Executive Team are unavailable, their designated alternates will be called upon to fulfill their roles on the team.

The "OLA Central COOP – Plan Activation and Deactivation" document defines the process employed to resolve the issue or situation affecting the delivery of services of the Assembly.

Policy Compliance:

All those responsible for the creation and maintenance of a BCP will ensure the continued accuracy and relevance of their plan content. In order to meet compliance requirements, each plan should include those appropriate procedures, staffing level, tools and the workplace planning necessary to meet approved deliverable requirements of each area pertaining to the individual Branch or Central plan. The format of the BCP documentation must follow the defined plan template requirements. Plans will be maintained and updated as operational changes dictate. To ensure compliance plans will be reviewed and filed annually.

Policy Compliance Support:

The Legislative Assembly of Ontario recognizes the importance of a comprehensive business continuity programme (or COOP) to insure the safety, health and continued availability of employment of its employees as well as quality goods and services for those we serve. We require the commitment of each employee, branch and external partners in support of the objectives required to protect and ensure the continuance of the Assembly.

Determining the Scope and Objective of the Programme

One of the first critical steps is to define what the BC plan is designed to protect and the maximum extent of damage, loss/denial or interruption the organisation can realistically survive. This will be uniquely different for each legislature. For example, British Columbia and New Zealand prepare for earthquakes and Ontario prepares for interruptions related to attacks and pandemics. Planning for specific interruptions helps determine the focus and resources of what is most important and time-sensitive, and avoids planning activities occurring outside of the approved programme boundaries.

All Assemblies' primary focus should be the resumption of parliamentary business when the House is in session or, when it is not in session, to return the organization to normal operations. By supporting the parliament, we ensure we are focused on planning and being prepared to respond to any disruption

Some programme's objectives are:

a. Identifying and putting in place Business Continuity plans for essential activities;
b. Creating specific plans for Chamber relocation;
c. Establishing an Incident Response Framework to deal with strategic and operational decisions taking place during an incident;
d. Determining the capability of each branch to communicate, react and resolve an incident.

To meet objectives, all Assembly departments should create individual plans to define and establish essential activities that are critical to their business area/function. Assembly Senior Management are required to review and determine the overall essential activities.

Legislative Assembly of Ontario

Providing the Resources Required for the Programme

For the BCM programme to succeed, it needs to have dedicated or committed resources assigned to it. The senior management team should set in place the necessary resources to proactively manage, maintain and grow the programme within the legislature. The support and resources dedicated to the programme will ensure that those planning for or responding to situations which cause a disruption to the delivery of the legislature's services will have required resources readily available to respond to the incident and transition to recovery.

Types of resources provided to the programme:

- Oversight and accountability for decisions, agreements or contracts necessary to relocate or obtain materials needed;
- Established lines of authority and delegation;
- Budgetary funds, with pre-established spending limits and signing authorities;
- Dedicated human resources or the ability to assign people as required;
- Supplies, services and equipment (on site or at an alternate site); and
- A room equipped for crisis management.

A formal BCM programme budget needs to be established at the onset. Determining an appropriate budget is difficult as there is no formula for planning for the unexpected.

The BCM budget may provide for:

- Ongoing operational planning and preparedness review and maintenance to ensure readiness;
- Ongoing training and education for all staff;
- Regular maintenance of the internal alert messaging system (to inform occupants of situations occurring within the precinct), ensuring constant and continued technological connectivity through an array of mediums, platforms and devices;
- The arrangement of alternate sites (primary and secondary) if the operations of the legislature (including the chamber) need to be relocated to an off-site location;
- Equipment/supplies for emergency operational centres (initial and backup) within the precinct; and
- The availability and storage of equipment/supplies required to operate an alternate site facility.

Establishing Oversight and Accountability

The final step is to ensure that the programme achieves the established objectives and is compliant with internal/external policies, standards, regulations and laws. It needs to be regularly reviewed, evaluated and managed. Senior management determines how the programme will be managed and establishes the accountability process.

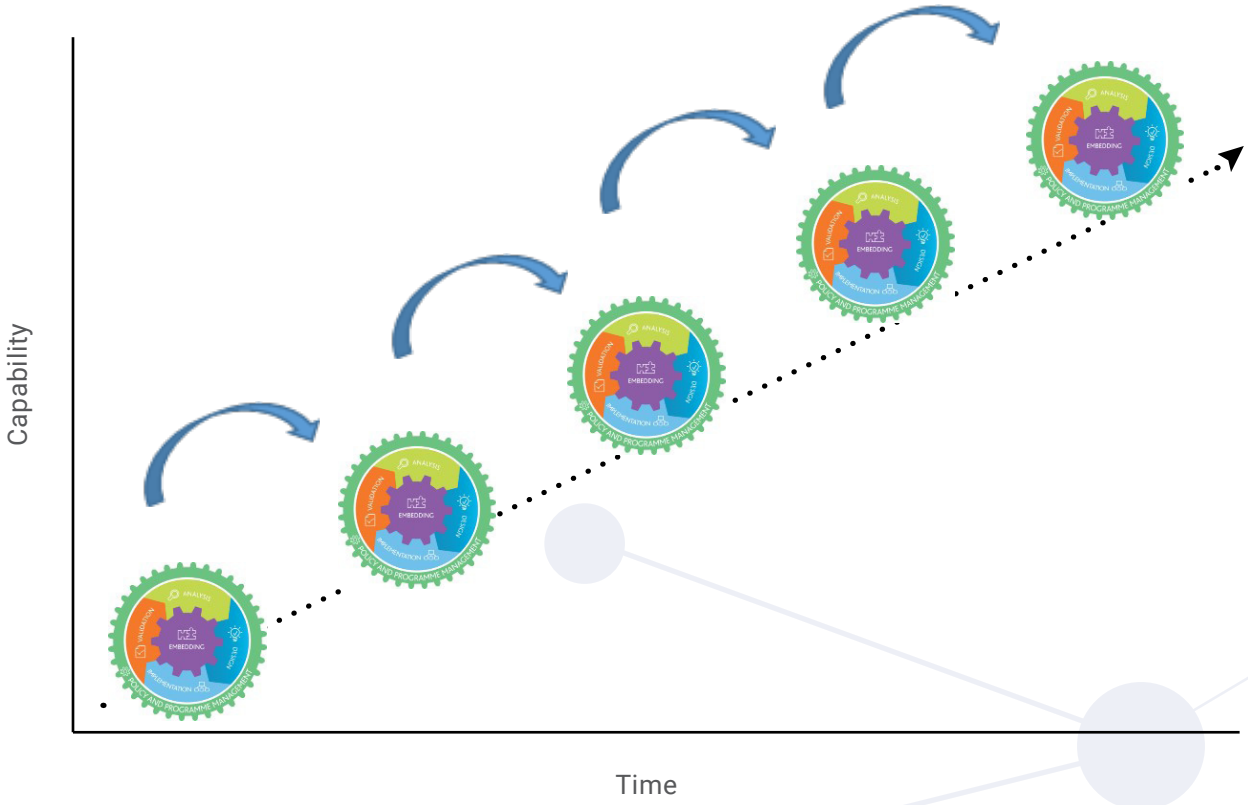
Training and testing of the programme ensures that established objectives are current and achievable, that employees are aware of what is required and how to respond. Ensuring incident debriefings occur assists in identifying areas for improvement and the requirement of plan/policy revision.

The most significant lesson learned from all assemblies involved in this guide would recommend that having a dedicated resource with subject matter expertise in business continuity is critical to ensuring success.

Chapter 3: Planning a BCM Journey: What to do

When implementing or maintaining a business continuity capability, legislatures must be aware that, to be of any value, BCM is not a 'one-off' activity geared at fixing emergent issues. Rather it is a discipline that, when applied appropriately, can add genuine value to the robustness, integrity, resilience and reputation of the organisation. BCM must not be seen solely as a governance activity; rather it is about getting service/process/system owners to think about how to keep their critical services available to stakeholders in time of disruption.

Short-term gains can and should always be sought, but it is in the longer term that the BCM lifecycle can really help a legislature. For that to happen, an iterative approach that is geared towards continuing improvement is the best route to take when implementing a BCM programme.



Time v BCM Capability Improvement (using the BCI Lifecycle Diagram as an example)

When to Plan

Each legislature will have its own business cycle and pattern of activity that is broadly the same for each year or even each parliamentary session. As stated earlier, a regularly recurring BCM lifecycle is far better than a 'one-off' or 'snapshot', but the frequency of that planning cycle and at what points in time the bulk of the planning work or refresh takes place is vital to the success of the BCM programme. The more frequent and robust the delivery of a BCM lifecycle, the quicker it is likely that organisational BCM capability will mature and improve (i.e. the steeper the angle will be in the figure above).

Consideration should be given to other governance work in the organisation and to when those tasks take place. It may be beneficial for BC planning to coincide with other work but it also may be better to avoid overlap with other work that puts a strain on those responsible for BCM planning. All legislatures have other work to do, some - and the perception may be most - of which will take precedence over progressing BCM activity. A robust policy supported by an active senior sponsor is a visible demonstration of the importance that the legislature places on BCM. Progressing plan development or maintenance must be factored into work schedules, priorities and planning. This is a mandatory item, and not one that can be ignored/set aside at the discretion of individual areas. BC planning is only successful if all of those with that responsibility know what they need to do, how to do it, when to do it and to what standard. So timing is important to ensure the work is done, but that does not mean BCM should be subservient to other, perhaps shorter-term or temporary tasks.

If a legislature is implementing BCM for the first time, it is highly unlikely that the first lifecycle will be perfect but that's why it is a repeatable cycle focussed on continuous improvement and not a one-off event, as demonstrated in the figure above. The BCM programme and its lifecycle follows the common '*plan, do, check/test, act (PDCA)*' model for developing BC plans, and applying that PDCA approach to the BCM programme itself may be worthwhile.

Consideration should also be given to whether the legislature is uni-cameral or bi-cameral. Is there one planning cycle for both houses and will the BCM programme be run separately for each house? If each house uses entirely separate resources, buildings and staffing, then separate BCM programmes may make sense but legislatures should be conscious of the resources and facilities that will be used when disruption takes place. Workarounds for disruption may rely on using the same alternative resources for both houses. If that is the case, who has priority or how is priority decided? It's also likely that government agencies, and perhaps different contractors too, are located with a legislature. How are BCM plans coordinated with third parties?

Activities of a Legislature

Before BCM planning can begin, it is important to determine what a legislature does and what the critical services are in time of disruption. Typically, a legislature will host one or two houses that allow Members to meet, investigate matters of concern to them and their constituents in committee and to prepare, debate and vote on legislation.

At the Scottish Parliament we recognise that everything we do is important and adds value to the overall work of the Parliament, but it is only those essential activities that we will resource and prioritise when faced with disruption. We define our essential (which others may term critical) activities as "activities that support Chamber business or that support our Members in their parliamentary duties". As well as these essential activities there are also enabling activities such as "keep the Parliament safe and secure" and quite a few others that also fall within the scope of our BCM policy, i.e. they may not be "essential" in themselves but do allow our essential activities to take place or to meet any requirements imposed by legislation.

Examples of the differences between essential and non-essential activities could include:

For IT:
- Project management or development of new software is **NOT** essential
- Running the IT Helpdesk **IS** essential

For Research/Library
- Ensuring delivery and distribution of newspapers is **NOT** essential
- Preparing supporting material for Members to refer to in debates **IS** essential

For Finance
- Preparing management reports on budget expenditure is **NOT** essential
- Ensuring rent, utilities and other expenditure for constituency offices is paid **IS** essential

For Human Resources
- Maintaining records of staff time-keeping at work is **NOT** essential
- Ensuring payroll can be run – for staff and Members – **IS** essential

For Facilities Management
- Preparing space plans for an upcoming move is **NOT** essential
- Ensuring that backup power generators are maintained **IS** essential

For Broadcasting
- Production of promotional videos for the parliament is **NOT** essential
- Filming and broadcast of chamber business **IS** essential

It should also be noted that timing can have an impact on whether something is essential or not, i.e. if the monthly payroll has just been run then it won't become essential for a couple of weeks. If the legislature is not sitting, then disruptions might not lead to a BCM response being invoked at all. So, as always, reference to the scope of BCM planning for the legislature is key in directing resultant activity.

---

*TIP: Creating business continuity plans for **everything** that a legislature does may initially appear to be appropriate, but this can be an extremely resource-intensive piece of work and may damage the reputation of the programme within the legislature. Decide what matters most to your legislature and concentrate your BCM planning efforts there.*

Considering the activities that require BCM plans could be identified as part of an initial business impact analysis (BIA). A BIA can be regarded as an activity 'map' of the organisation and should document what the legislature does on a day-to-day basis. It will show the outputs from each activity, the resources (job roles, equipment, IT, contractors, facilities, etc.) used to create those outputs and how long the organisation can tolerate these activities not taking place. The question 'So what if this activity stops?' helps identify if something should have a corresponding BCM plan or not. This question should also give an idea of how urgently the activity needs to be restored, which can then be used to create the BCM plan for the activity.

When preparing this information, those closest to an activity may be inclined to state that only a short period of time can pass without the activity taking place. Assessment of these timescales needs to be done centrally, compared with other responses from across the legislature, and challenged where appropriate. Exercises to 'train the people and test the plans' will help eliminate such assessments. People are bound to overstate the case in early iterations of BCM planning activity.

On completion of the first BIA, it may be that the scope of the BCM policy needs refining as the BIA may identify urgent activities that do require BCM plans that did not previously fall under the initial scope for business continuity. This is normal and is one of the reasons that BCM cannot be regarded as 'one-off' or snapshot activity but should be an iterative process that helps improve service delivery for the whole legislature. Each plan is only good at the time of writing; as soon as it's complete it becomes, a historical document as internal and external factors will have changed which will mean that changes to the BCP, even if only subtle, are required and so again, demonstrates the importance of this being an enduring lifecycle process. A mature BCM programme will see BCP's, or at least critical aspects of plans, updated as things change, not because of a review.

When considering the BIA for a legislature it is important that different times of the parliamentary year and session are considered.

Legislatures should consider periods, such as dissolution/prorogation and recess, as well as any times when the legislative process is more urgent such as preparation and passing of a budget bill. Considerations like this will help decision makers allocate resources if BC plans need to be invoked. For example, during recess there will be far less urgency on chamber activities, but there may be administrative activities that are more important such as finalising the annual report or annual accounts for the legislature.

Assemblies should also consider if their activities have different priority depending upon the day of the week. It may be that if the chamber isn't sitting, priority can be given to parliamentary committee activities, or vice versa.

(See Chapter 1 for an example of a BIA template)

Planning for Disruption

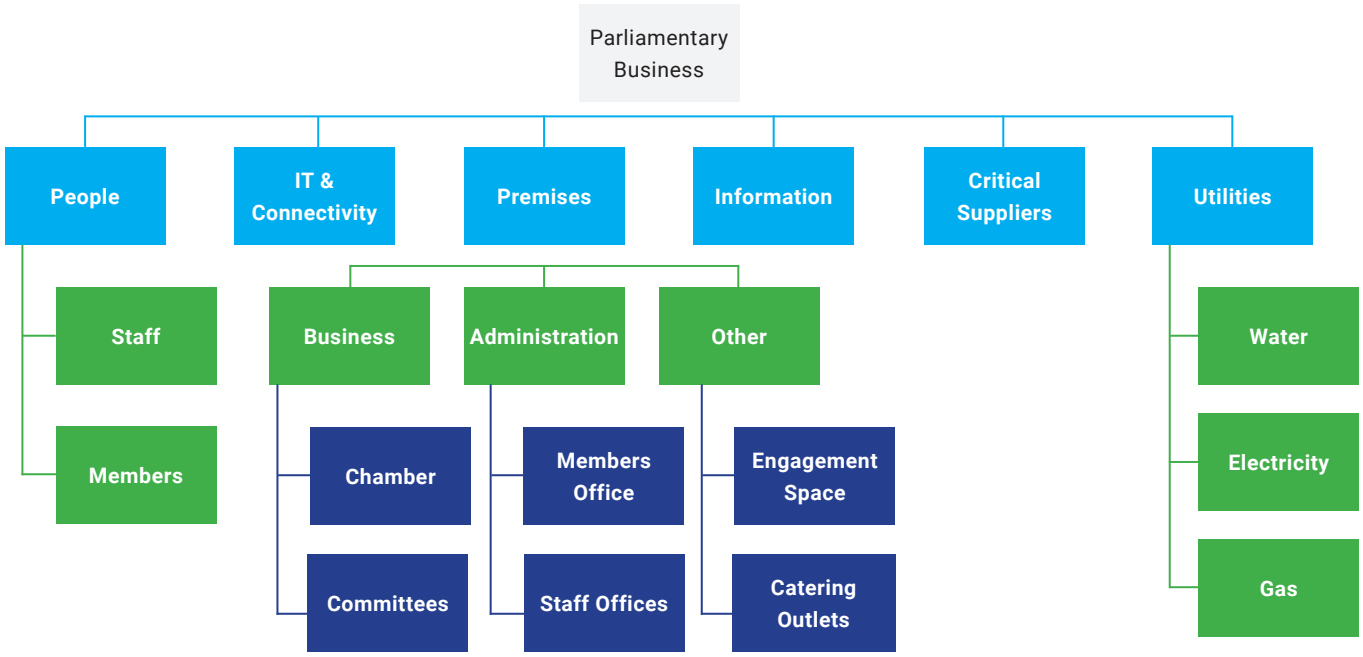
The BIA will provide a legislature with a map of what they do. Once that is known, a BCP will be created for each activity that requires one.

When considering what to plan for, BCM is primarily focussed on the loss of/reduction in/disruption to the normal resources used to carry out an activity. These resources should have already been identified in the BIA. There are many causes that could lead to loss of/disruption to any of these resources. It is important not to attempt developing BCM or risk management plans for every conceivable ***cause*** of a loss/denial, but plan for the ***impact*** of a loss/denial.

There are a range of resources or services, that the loss of or disruption to, must consider when undertaking BCM planning for legislatures. These include, but are not limited to (and in no particular order):

- People
- IT or connectivity
- Premises
- Information
- Critical Suppliers
- Utilities

Map of Typical Resources Supporting Parliamentary Business



People

There are two main groups of people who, if unavailable to attend or support business, may cause that business to be disrupted, delayed or cancelled. Those groups are legislature administrative staff and Members of the assembly.

It is reasonable to assume that whatever the cause of the disruption – weather, transportation, pandemic, etc. – it is likely to affect both groups. The impact on the groups may be different but it is only in the rarest of occasions that this type of disruption will only affect one of the groups.

There is one other group of people who should be considered – contract staff – but they will be considered under the *Critical Suppliers* section later.

When considering how to cope with a loss/denial of people – which will often mean the temporary inability of staff to travel to work rather than anything more permanent – it is the impact of that loss/denial that should be considered rather than if the cause is due to pandemic, industrial action, transportation disruption or anything else.

Staff

If the normal staffing complement aren't available, there are several options open to BCP owners, as long as these things have been thought of beforehand and the necessary mitigations have been put in place. Typical options include, but are not limited to:

- Stopping the activity – Can the activity be set aside, particularly if the disruption is likely to be very short term?
- Replacement staff – Are there desk instructions/manuals/guidance material available for other staff to pick up if the usual staffing isn't available? Have other employees recently carried out these roles and can they be temporarily re-assigned to carry out more urgent work?
- Proactive measures – If a loss/denial is known to be likely to occur because a weather or transportation disruption is predicted, then consider keeping essential staff close to the legislature. Concentrate on the minimum tasks and staffing to meet any business that must take place and keep those staff in local commercial accommodations. All other employees can stay away, minimising risk to them and, if the necessary technology is available, they may be able to work from home.

One tool used in the Office of the Clerk in the New Zealand Parliament is an annual 'staff availability survey'. This quick e-mail survey using voting buttons invites staff to indicate 'likely' availability to support Office activities in the event of a disruption using a traffic light response (green – available, orange – might be available depending on family, etc. or red – not available, e.g. known family constraints will prevent staff member working). Employees are not bound by responses and it is emphasised that it is not a measure of commitment to the Office. Rather it is a tool enabling managers and team leaders to determine in advance any potential shortfalls in core skills needed to deliver critical services and so facilitate consideration and planning of work around solutions. The survey is normally run at the start of the calendar sitting programme when all staff have returned from the long, southern hemisphere summer break.

Members

If Members aren't available, there is very little legislative work that a parliament can proceed with. Depending upon the nature of the 'unavailability', there may also be issues with constituents being able to engage with Members on matters that are important to them.

The standing orders of a legislature should already be clear on the minimum number of Members who need to attend for chamber business to take place or for committees to meet, but even with that, there is some BCM planning required for when there is wholesale unavailability of Members. Aside from absences caused by decisions of political parties, wider unavailability of Members could be caused by travel restrictions,

severe weather, pandemic flu or a multitude of other causes and, as always, such planning should concern itself more with the impacts of a situation rather than the cause.

The BCM response could be as simple as rescheduling the business until more/all Members are available or it could be as innovative and sophisticated as allowing Members to participate in business from one or many remote locations. With respect to participation in legislative activities remotely – something that at the time of this publication we are not aware of being practised – there are a range of factors to consider:

a. The changes to standing orders or legislation to allow such participation to take place.
b. Familiarity – of Members and legislature staff – on how this participation will take place, i.e. time will be needed to train everyone involved on how this approach will work to ensure that it operates as smoothly as possible and that there is enough trust in the integrity of the approach for it to be successful.
c. Remote technology – Such an approach will rely on some form of technology to operate. In any country, the local implementation of a technology such as copper or fibre broadband will vary from location to location so any 'local' issues will have to be identified – and fixed/mitigated against if possible – for the approach to work.
d. Hybrid business – How will remote participation by some integrate with some Members also being in the chamber?
e. Review of the standing orders to take into consideration anything that may affect BCM plans.

Whatever is chosen, it is vital that senior politicians, including the Speaker, are aware of what the plans are and that if those plans have to be used, Members can easily participate remotely in business if required.

Premises

The loss/denial of an entire parliamentary precinct, even temporarily, would be one of the most impactful events that could occur. While a legislature may support many constituency offices for its Members, the legislature itself and the chamber is likely to operate from a single site or even a single building. Where such singularity or concentration of assets in one location takes place, some level of BCM planning is absolutely necessary.

Such planning could fall into two categories:

- The space needed to run parliamentary business – a chamber, committee rooms, etc.
- The space needed for all other enabling activities – administration premises

There will always be 'other' space normally used by a legislature which would typically be used for value-added work such as events or engagement purposes. This may be within the scope of BCM planning, but this space would not normally be regarded as essential or critical unless it is an asset that is used as alternative accommodation for 'actual' essential activities.

Parliamentary Business Premises

Where a Parliament is bi-cameral, an option for managing disruption caused by the loss of one chamber could be to use the other one – even if that, at first, is politically uncomfortable.

When a second chamber can't be shared between houses, it may be that other space within the legislature can be used for chamber business. There may be committee rooms, events space, or large dining areas – either in themselves or in combination – that could be reconfigured to allow chamber business to take place. If alternative spaces are identified for use as an 'emergency chamber', then it is essential that a plan on how to reconfigure the space is developed, roles and responsibilities are identified and that the set-up is tested on a regular basis. Regular testing is needed to retain organisational knowledge and confirm time taken to reconfigure so advice can be provided to Speakers and Clerks on when the legislature might sit after activation of the plan.

If neither of these options are available and parliamentary business must continue, then alternative premises must be found. If so, is any formal proclamation needed to allow the legislature to meet in a separate location or city? If needed, who can make that proclamation and what arrangements are in place to enable it to be recommended and/or made?

Where available, it may be possible to approach government departments, local government councils and organisations, large educational establishments, conference venues or hotels to determine if they can accommodate the legislature. Whether the legislature enters into formal contracts with such venues depends on the risk appetite of that legislature and the likelihood of the whole parliament campus being lost. Whether that is the case or not, legislatures should consider developing plans to show how potential venues could be used and testing those plans wherever possible.

When considering what should be sought from an alternative premises provider, the minimum set of resources needed to deliver a chamber should be the starting point. While it may be convenient to have lots of desk and office space for Members and for legislature staff, it is highly unlikely that a good alternate site will have lots of space like this available. As such, everyone will need to adapt to the new site and to new temporary working conditions.

When considering how an alternative venue may be configured, some questions that might help are set out below:

1. What layout is required? Does it need to replicate the shape of the chamber or can that be adapted, e.g. a European Parliament curve might be the usual shape but a traditional Westminster style may be the only layout possible. Or a 'lecture theatre' approach may need to be taken, particularly if it's a lecture theatre that is being used.
2. Once the layout is decided, how will voting be carried out? Are division lobbies possible or will roll-call, show-of-hands, party voting or some form of electronic voting be used? Do the standing orders support the necessary changes to voting?
3. If filming or broadcasting of the chamber is required – which is surely a 'must-have' for most legislatures – how will that be done? Where will the cameras and microphones be positioned and how will the broadcasting infrastructure be put in place to deliver pictures from the alternative venue?
4. If the public has the right to observe chamber business, can that be cancelled for a period of time or if not, how will that be facilitated securely?
5. How will security be maintained at the venue for the duration of use by the legislature?
6. While it won't be possible to provide office space for everyone, is there dedicated space for the Speaker and for clerks?
7. How will allocation of any remaining available office space be prioritised?
8. What pattern of business will take place? Can the chamber and committees meet in the same venue, or even use the same room, if the normal pattern of business changes? Also, there may be commitments that the alternative venue needs to still meet. Can parliamentary business be scheduled around that? It may be straightforward if other public sector buildings are being used but less so if the venue is being used to host a wedding or an international conference.
9. How will people be fed and watered?

Administration Venue

As stated earlier, it is highly unlikely that any alternative site would be able to host all the chamber and committee needs and also have discrete space for Members, for legislature staff, for events and other areas that might normally be available at the legislature itself. To help with the success of any alternative venue planning, it may be necessary to split the 'administration' from the 'parliamentary' business requirements to have a viable alternative venue plan.

Consideration should also be given to whether technology can be used to allow staff and Members to work at home – or if there are staff who can be 'stood down' for a period and work set aside until normal premises are available again.

Are there reciprocal arrangements that can be put in place with the public sector, or even commercial, organisations to allow for some parliamentary staff to work from their premises? Can any of the suppliers to the legislature accommodate some employees?

As an example of this in action: In August 2018 the Parliamentary Counsel Office, one of the five agencies supporting the New Zealand Parliament, had to evacuate the CBD Building that they were accommodated in following the discovery of large quantities of asbestos in the central core. All building tenants, primarily the Reserve Bank and government departments, had one working day to evacuate before being locked out. To support the accommodation of the Parliamentary Counsel Office, three Select Committee rooms were made available for up to three months along with a range of other spare space on the Precinct. This is an example of agencies working together to share and reprioritise use of available space in response to disruptive events.

IT or Connectivity

Every organisation, not just legislatures, and most individuals are becoming more reliant on connected technology. Such technology is used for a range of activities including accessing work email away from the legislature on mobile or home devices, using bespoke software to manage chamber and committee business, and tools for managing constituency casework or providing wider access and innovative routes to parliamentary business. Aside from legislature-specific needs, technology is also being increasingly used for the automation/control/monitoring of building systems and security. This demonstrates that the loss/denial of IT can have wider implications than just the administrative operations of a legislature.

These different uses of information technology rely on the successful integration and long-term operation of a combination of software, hardware, connectivity (wireless or wired) and the staff needed to develop and maintain these resultant information systems. These systems can be complicated and, just like any other tool, can become unavailable through malicious acts, unintended consequences from change, human error and simple wear and tear. So whenever an information system or technology is being used to deliver or support the delivery of an activity, planning should take place to consider how the functions offered by the technology can be carried out if that technology is absent. These plans are usually known as 'workarounds'.

Typical considerations for establishing workarounds include:

a. Can different technology be used, e.g. can a word processing software and email replace a bespoke procedural system?
b. What manual processes could be used? They may be slower (or maybe even faster!)/less efficient/more cumbersome but will they work? Are these processes documented and able to be used by a wider range of staff than just those who normally manage the relevant process?
c. How and when can these workarounds be tested? Successful testing is the only route to ensuring successful use by all stakeholders when needed.

When there is a wide-scale incident at the usual premises for the legislature, it may be that a wide range of IT services need to be provided from an alternative site. This site is usually called a disaster recovery (DR) site and, once a legislature understands its recovery point objective (RPO) and recovery time objective (RTO), the DR site can help restore IT services.

Recovery Point Objective (RPO)

The RPO is a measurement of the maximum data loss that is tolerable for the legislature, i.e. how much data can be lost before it adversely harms the operations or reputation of the legislature. The RPO is met entirely by technology, i.e. the frequency of backing up all data – weekly, daily, hourly or instantaneous copying of data to somewhere else inside or outside the legislature.

Recovery Time Objective (RTO)

The RTO is a measurement of how quickly data and applications must be made available to and usable by stakeholders. The RTO is met entirely by the recovery plans, currency of data and technology used at the DR site – or even alternative technology, data and systems at the legislature. The nearer a state of usability for all of these, the shorter the RTO.

Example of DR Site Classification

- Only hardware, no data or applications available
- Significant time needed to deliver, load and test data and applications
- Cheapest Option
- Long RTO

- Hardware and some data/applications
- Activated more quickly than “cold”
- Medium RTO

- Hardware and all/most data and applications are avaialble and current
- Requires “always-on” synchronisation between parliament and DR site
- Can be expensive
- Lowest RTO and shortest RPO

No matter what classification of DR site is chosen, it will typically consist of:

a. A range of hardware, software and connectivity configured to deliver some or all the IT functionality that is normally used at the legislature.
b. A method of ensuring that recent data from the legislature can be used as a starting point to get the DR site operational. This data could be restored from backup tapes or it could be 'fed' via communications from the legislature. When using this data to move provision of IT from the DR site, the IT professionals should always be clear as to when that data is from: Is it from last night/last week and all data processed since then is lost or, at best, will need re-keying manually? Is it from an hour before the disruption took place meaning not much data is lost? In the use of any DR site, it is almost always certain that some recent data will not be available.
c. If the IT services are being provided from a different location, it is highly likely that they will not have the full range of capacity or capability – at least not straight away. So who can access the services from this site, do they know how to do that, and how will increased capacity and capability be introduced to meet the needs of the legislature?

There should also be consideration to how users of the technology can connect to the 'normal' technology and the workarounds that might be used if that technology fails. Subject to privacy and data security concerns, organisations are increasingly enabling staff and Members to work remotely using portable devices and moving information into 'the cloud'. (The cloud, we should always remember, is just some other organisation's larger computer room, somewhere in the distance).

The use of portable and mobile devices to access services in the cloud typically relies on the use of wireless networks to connect to those services. When Wi-Fi is available – and the availability of this service seems to be increasing continually – it gives Members and legislature staff a huge amount of flexibility in how they can carry out their duties, which can be particularly helpful when working with constituents. When the Wi-Fi fails, it almost always renders the portable devices incapable of using up-to-date information.

Thought should be given to the following connectivity aspects of technology use:

a. How is the wireless network at the legislature maintained? Are there overlaps in the reach of wireless transmitters to allow one to fail but still maintain service? Is there redundancy in the wireless supply, particularly for chamber and committee business?
b. The wireless part of the network always relies on a 'wired' connection to the internet service provider (ISP). Can more than one connection to the ISP be put in place so that if one fails the other kicks in? It is suggested to ensure that the other route to the ISP has the same capacity and that there are no changes that end users must make to use that alternative.

c. The ISP will have their own contingency planning for how they deliver their services to the legislature. It is recommended to find out what those are and try to identify single points of failure in their approach.
d. Moving away from the 'normal' provision of Wi-Fi: Can Members or staff use their mobile phones to connect their PCs to the internet? If that's possible, do they know how to do it?

Means of Communication in a Time of Crisis

In certain instances, during a natural disaster for example, the mobile network gets closed down or overloaded rendering it ineffective. Other options (preferably more than one) may be considered for key people in the organisation to able communicate with each other, such as satellite phones (limited number), priority calling with phone company, and special SIM cards.

In August 2018, the Parliamentary Service and Office of the Clerk on the New Zealand Parliamentary Precinct were in the process of introducing satellite phones to provide an option for communicating in any disruptive event where the landline and/or mobile networks are unavailable. Satellite phones will be issued to members of the leadership of both organisations and the Speaker of the House of Representatives and other key staff. The phones are identical to the model used by the New Zealand Ministry of Civil Defence and Emergency Management (who manage national responses from the Precinct) and other Precinct Agencies (e.g. the Department of the Prime Minister and Cabinet). This will help facilitate coordination of response activities in any disruption. A process to conduct regular testing of the phones is being developed.

Safeguarding Information

Legislatures store, manage, create and share masses of information as part of the normal parliamentary process and when engaging with constituents. It can be stored in paper form (letters, books, reports, hand-written notes etc.) or electronically (emails, documents, websites, wikis etc.) and should be regarded as a precious resource that is used as part of the day-to-day operation of the legislature. As such, plans should be in place for when access to that information is denied and, particularly so, when the information is lost or misplaced.

Most countries will have data protection legislation in place and many countries, even those outside the European Union (EU), have adopted the General Data Protection Regulation (GDPR) that came into effect within the EU in May 2018. Each legislature should be aware of the particular statutory regulations they have to comply with and build on that to establish their own processes and plans for how to deal with disruption to or loss of information.

A particular requirement of a legislation, as is the case with GDPR, may be to set up a particular team to handle losses of information, with this loss usually being termed as a 'data breach'.

The term ‘data breach’ may lead one to automatically think of a loss of information as being something that should be the responsibility of the IT department or provider. That should not always be the case, if at all. While it is completely sensible to involve IT staff when a data breach of electronically stored information takes place, the data breach could just as easily take place when printed documentation is mislaid or stolen, and this is most definitely not the remit of IT staff.

Having some form of ‘data breach’ team or identifying staff responsible for managing such an incident is a sensible step, as is training and exercising that team. This can be done by using specific examples relating to the legislature’s environment and/or it can be done by taking examples from the media – these seem to be occurring on an almost daily basis.

Critical Suppliers

Every legislature will rely on contractors for some part of their operations. This could be externally sourced security staff – perhaps supplied by the police – or expertise in the areas of IT and building maintenance to contracts that deliver catering and porterage resources.

Some of these contracts will be in place to help deliver the critical activities of the legislature and will be critical to that service delivery, and some won’t. It’s important that the contracts involved with delivery of critical activities are identified and that BC plans are created for the services delivered under those contracts. There are two main elements to this:

Stage One - Pre-Contract Assessment

Most contracts will be put in place after a procurement competition. This will involve a specification being created and an objective assessment of bids based on questions that will critique those bids. For all contracts, but particularly for critical contracts, a proportionate level of BC requirements can be included in the specification. The more critical the contract, the more detail that can be requested from bidders and the higher the weighting that can be given to assessment of the returned information.

Questions to the bidders should include what BC plans they have for their overall organisation and, separately, the plans they will put in place for the delivery of the specifically contracted services to the legislature. This should include the identification of the resources used within that contract (people, assets, infrastructure etc.) and how availability of those resources or appropriate alternatives will be maintained.

Stage Two – During the Life of the Contract

It is straightforward for any bidder to put information into a contract bid that will say what they intend to do if they win the contract. The value in that is only realised if the contractor delivers on what they have promised.

Any BC plan proposed in a bid will have to be refined as part of the implementation phase of the contract being brought on line. This is normal and will ensure that any misconceptions or assumptions used in creating the initial bid plan can be ironed out.

In year one it is reasonable to expect that a relatively good BC plan will be in place but, just like the BC plans for other resources for critical activities, that plan will need to be updated and demonstrably tested to give the legislature assurance that the supplier is capable of continuing to deliver their service during and after a disruption. This update and testing regime should be part of both the ongoing contractor performance management of the contract and part of the regular monitoring of the efficacy of all BC plans. It might even be worth considering, depending on the nature of the contract and its criticality to supporting the legislature, involving key contractors in the legislature's own BC exercising and testing regimes to provide assurance of the robustness of key external services or providers.

Conclusion

This chapter sets out what a typical legislature might want to consider for its BC planning areas. Each legislature will have its own specific risk profile and it may be that the *loss of premises plan* is much more urgent than, say, the *loss of IT plan*, or vice versa. But it's likely that some version of both of those plans will be required.

It's also important to note – which is why it's being reiterated here – that a business continuity plan is only good at its time of writing so plans need to be tested and updated as the legislature changes. Successful business continuity management is not a one-off but rather an on-going discipline that will help the legislature improve the robustness of its service over time.

Chapter 4: Assessing a Business Continuity Plan

Business continuity plans (BCP) are not static documents as organisations and priorities will continue to evolve. The focus of this chapter is on self-assessment to measure progress and make improvements. Self-assessment is not intended to be a one-off exercise, but repeated over time as circumstances change. Monitoring and reporting is a best practice.

Self-Assessment Survey:

1

BUSINESS CONTINUITY MANAGEMENT POLICY

Does the organisation have a BCM policy that appropriately guides the preparation, review and updating of the BCP?
Was the policy approved by the governance committee?
When was the BCM policy last reviewed and updated?
Is the policy sufficiently comprehensive and clear?
Is the policy well communicated and understood by plan users?

Perceived Risk

Low	Medium	High

Required Action

Insert text

2

PLAN GOVERNANCE

Is there an overall sponsor/champion for the BCM programme?
Is there an appropriate governance body in place to oversee the development, updating, execution and testing of the BCP?
Does the governance body include the right players in terms of representing the varied interests and responsibilities of the legislature?
Can the governance body make all the necessary decisions respecting the plan and how it is to be used?
Does the governance body meet regularly to review the plan, its adequacy and the plan tests?
Is the governance body regularly updated to reflect the changing structure and needs of the organisation?
Has the governance policy set out clear objectives and expectations for the BCP and how it is to be used?
Is there a clear and defined role for the governance body at the time of a significant business interruption?

Perceived Risk Low | Medium | High

Required Action

Insert text

3

PLAN ROLES AND RESPONSABILITIES

Does the BCP clearly identify who is responsible for what in developing, monitoring, maintaining and executing the plan?
Has the plan identified the right people to carry out the actions required?
Are the assignments at the right level to achieve the desired result?
Are the assignments regularly updated to reflect changing responsibilities and personnel changes?
Do the responsibilities outlined in the plan correspond to the individual/organisation assigned those accountabilities?

Perceived Risk

Low	Medium	High

Required Action

Insert text

4

SCOPE OF THE PLAN

Does the plan address the major risks to critical service of the legislature that are vital to its recovery in the event of a systemic failure or other emergent event?
Were the critical service risks identified through an appropriate impact on service analysis?
Is it clear what is included and what is not included in the responsibilities/required actions?
Is the scope of the plan appropriately updated based on changes within the organisation?
Does the plan avoid becoming too detailed such that the planned actions are at the right level and clear for implementation?
Has the plan considered various realistic scenarios that may affect the key services to be delivered?

Perceived Risk

Low | Medium | High

Required Action

Insert text

5

LINK TO IDENTIFIED RISKS

Are the key risks clearly stated in the plan?

How were the risks identified and prioritised?

Are the risks reviewed and updated from time to time?

Have the risks been reviewed and signed off by the governance body?

Are the risks well understood and communicated within the organisation?

Are the recovery actions directly related to the key risks and their impact?

Perceived Risk

Low	Medium	High

Required Action

Insert text

6

LINK TO OVERALL OBJECTIVES AND PRIORITIES

Are the overall objectives of the legislature well documented and reflected in the BCP?
Is the plan updated as organisational objectives and priorities change?
Are the overall objectives clear and well understood by those who need to develop, monitor and execute the plan?
Have the organisational objectives been approved and signed off by the governance body?
Is there a clear link between the organisational goals and objectives and the proposed activities to be carried out in the event of a business interruption or disaster?

Perceived Risk

Low | Medium | High

Required Action

Insert text

7

PLAN SPECIFIC OBJECTIVES

Are the specific objectives for the plan identified and have they been reviewed and approved by the governance body?
Are the objectives clear and well understood such that they will be met in the event of a disruption?
Are the specific objectives reasonable/achievable, e.g. the expected number of days to recover a specific legislature responsibility?
Does the plan have a clear objective hierarchy in terms of what should be done first, second, etc.?
Are the objectives reassessed from time to time as overall priorities and organisational structure change?

Perceived Risk

Low | Medium | High

Required Action

Insert text

8

REQUIRED RESOURCES

Are the required resources and staff in place to implement and maintain the BCP?
Are the limited resources allocated based on the highest risk and operational impact on the legislature?
Is resourcing reviewed as part of the annual budgeting cycle?
Are specific assets and arrangements, e.g. key contracts, kept up to date?
Are resources distributed to the right level in the organisation, i.e. those who will need to act and use them?

Perceived Risk

Low	Medium	High

Required Action

Insert text

9

PLAN DOCUMENTATION / ACCESS

Is there a clear and approved BCP document?

Do those charged with the execution of the plan agree with the plan and understand what they are to do?

Has the plan been appropriately distributed to those who need to act on it?

Can the plan be accessed if plan participants are not at their worksite?

Are there clear, regular time periods for updating of the plan?

Perceived Risk

Low	Medium	High

Required Action

Insert text

10

DOCUMENTING / TESTING EXTERNAL DEPENDENCIES

Have external critical supplier/outside organisation dependencies been identified in the BCP?
Is there a strategy to address the dependency risk?
Is the strategy realistic and has it been tested?
What are the options in the event of a key supplier failure?
Are the identified dependencies updated as suppliers change?
Are the critical dependencies and their recovery reflected in contractual terms?

Perceived Risk

Low | Medium | High

Required Action

Insert text

11

DOCUMENTING / TESTING INTERNAL DEPENDENCIES

Have the internal supplier/organisational unit dependencies been identified as part of critical service delivery?
Is there a strategy to address the dependency risk?
Is the strategy realistic and has it been tested?
What are the options in the event of a key internal supplier failure?
Are the internal dependencies updated as the organisation changes?

Perceived Risk **Low** **Medium** **High**

Required Action

Insert text

12

UPDATING OF THE BUSINESS CONTINUITY PLAN

Is the current plan up to date?
Is there a defined schedule for updating the plan?
How often is the plan reviewed by the governance body?
Is the plan reviewed and updated following a test of the plan?
Is the plan reviewed and updated after a disruptive event?
Is there a person/organisation identified as being responsible for the updating?

Perceived Risk

Low | Medium | High

Required Action

Insert text

13

ORGANISATIONAL TRAINING

Is there a training plan for those involved in the development, updating and execution of the BCP?
How often is the training delivered and updated?
Do staff believe the training they receive to have been sufficient to carry out their responsibilities?
How does the training plan deal with the turnover of staff in key positions affecting the plan?
How is training delivered as part of any induction/onboarding package to new staff?

Perceived Risk

Low	Medium	High

Required Action

Insert text

14

COMMUNICATIONS

Is there a communications component/plan as part of the BCP?
Is it clear in the plan who is responsible for communication and at what levels in the event of a business interruption?
Does the governance body agree with certain key messages, e.g. updates sent to the Members, the public and other clients?
Is there a lead communications person who is responsible for the required communications?
Is there appropriate co-ordination of communications built into the plan?

Perceived Risk

Low | Medium | High

Required Action

Insert text

15

ISSUES MANAGEMENT

Is there a defined process for identifying and reporting on issues?

Is it clear who has the authority and responsibility for addressing the issues?

Is there a reporting of the issues to the governance body?

How is progress on issues management monitored and reported?

Perceived Risk

Low	Medium	High

Required Action

Insert text

16

OPTIONS IDENTIFICATION

Was an appropriate assessment of the options made relative to cost, timeliness and impact on clients?

Was the chosen alternative service delivery appropriately tested?

Are the options identified reasonable and practical?

Are the major options periodically reviewed?

Perceived Risk

Low	Medium	High

Required Action

Insert text

17

TESTING OF THE PLAN

Has the plan been tested?
Is there a schedule for the testing of the plan?
What is the nature and extent of the testing, e.g. table-top versus live exercise?
How are the results of the testing exercise documented and acted upon?
How are the results reported and to whom, e.g. governance body?

Perceived Risk

Low | Medium | High

Required Action

Insert text

18

LEARNING FROM THE PLAN TEST RESULTS

Is there a defined process for updating the plan based on the tests conducted?
Is there a person responsible for this process?
Is there a defined role for the governance body in overseeing the test results and in updating of the plan?
Are plan test updates done on a timely basis?
Are test results appropriately considered for other areas of the plan not tested?

Perceived Risk

Low | Medium | High

Required Action

Insert text

19

AUDITING OF THE PLAN

Is there provision for a periodic external review of the BCP?
How are these results communicated to the governance body?
How are the recommendations used in updating the plan?
Is there reporting of the external assessment to stakeholders?
When was the last external review completed, and were the recommendations acted upon?

Perceived Risk

Low | Medium | High

Required Action

Insert text

The Plan in Practice

To be effective, the BCP must be an evolving document. From experience, there may be a natural tendency to develop a BCP and not look at it again until an unexpected event happens. The risk is that in the intervening period things have changed, e.g. responsibilities, priorities, key personnel, such that the plan is no longer effective. In this case people end up doing the best they can but that may not be enough.

It is far better to assign the time and resources necessary to ensure the plan is up to date and that it will assist the legislature in the recovery when an event occurs. The plan must be part of the ongoing management of the organisation as would be the case for the many other executive functions. This does not mean that it needs to be a daily event, but rather a well understood process that is given sufficient priority and attention commensurate with the risks to the organisation and when the plan was last reviewed, tested and updated. It is also better to do a proper self-assessment than to be facing an external or internal audit of a plan that is clearly out of date and potentially ineffective.

Self-Assessment Checklist

Based on the key self-assessment areas and questions identified above, a summary self-assessment checklist of areas to explore in the planned BCP review is provided below. The intent is a review of each BCP topic area and an initial assessment of the degree to which it actually exists. Based on the initial assessment, a rating is given on the area's compliance by rating it as low, medium or high. Following this for each area, it is decided which areas should be reviewed in further detail and what specific review actions are required. In this way, self-assessments are tailored to where they are believed to have the greatest risk/reward.

As noted earlier, the self-assessment process should be repeated from time to time so that the entire BCP is up to date and reflects current best practice.

Sample Business Continuity Self-Assessment Checklist and Review Plan

No.	Self Assessment Area	Description	Perceived Risk (Low/ Med/High)	Review (Yes/No)	Required Action
1	BCM Policy	A clear and up-to-date BCM policy is in place.			
2	BCM Governance	An active BCM governance body is in place.			
3	Clear BCP Roles and Responsi-bilities	Individuals are aware of their roles and responsibilities.			
4	BCP Scope	The scope of the BCP covers the required areas.			
5	BCP External Dependencies	The plan has identified and tested the critical external dependencies, e.g. outside suppliers for recovery.			
6	BCP Internal Dependencies	The plan has identified and tested the critical internal dependencies, e.g. internal suppliers for recovery.			
7	Updating of BCP	The BCP is regularly reviewed and updated.			
8	BCP Training	There is a regular training program for staff on their BCP roles and expectations.			

9	BCP Communications	Clear lines of reporting are outlined in the BCP for internal and external communications.			
10	BCP Issues Management	A clear process exists for raising and addressing issues management in the BCP.			
11	BCP Options Identification	The BCP identifies clear workable options for the delivery of service in the event of a disruption.			
12	BCP Testing	BCP test plans have been developed ranging from table-top tests to full interruption tests.			
13	Learning from the BCP tests	A follow up process exists to take the information from the BCP tests and to update the BCP.			
14	BCP Auditing	The BCP document and process are periodically reviewed by internal or external audit, or an outside expert.			
15	Link to Identified Risks	The plan has a clear and direct link to the risks of the organisation.			

16	Link to Objectives and Priorities	The identified BCP activities and priorities link to the overall objectives and priorities of the organisation.			
17	BCP-Specific Objectives	The BCP contains specific (SMART) objectives.			
18	Required Resources	The BCP has the resources it needs to maintain and update the plan and to implement the required mitigation actions.			
19	BCP Documentation	The BCP document is clear, well understood and signed off.			

Chapter 5: Experiences and Learning

This chapter contains situations experienced by some legislatures represented on the LABCoN, which provide concrete examples of the importance of having a BCM programme in a parliamentary setting.

Political Engagement

Legislatures benefit from high-level political engagement in advance on most potentially novel and/or contentious issues and there are few issues more contentious, and reputationally damaging for a legislature, than not being able to function properly and appearing to have little or no resilience in a crisis.

Whilst senior political stakeholders should not be expected to know the detail of business continuity plans, they do need to have assurance that parliamentary business can be maintained or restored in a way that meets their expectations. They need to have confidence that resilience is being actively thought about, with plans being put in place, and that the capability of individuals and teams is being nurtured.

One way to address this is to prepare a short paper for discussion with principal political stakeholders to agree on common expectations. This can be achieved by drawing up a small number of well-defined principles that form the foundation for all business continuity plans. For example, one legislature set out principles that established how quickly the chamber could be established after an incident impacting the parliamentary building (2 days); committees (2 weeks) and a new normal operating model (from 4 weeks).

It's also possible to consider and agree in advance on other key principles, such as which services will be prioritised and which specific services will be moth-balled; the primary geographical locations for any relocation plans (and where it's never suitable); means of communication with Members and staff in an emergency; and nominated spokespeople.

Discussing and agreeing on some common principles enables officials to develop plans based on realistic expectations discussed and challenged in normal circumstances rather than under the pressure of a crisis. For example, one legislature that had to relocate because of an incident was within minutes of signing a lease on an alternative venue that was deemed by politicians to be politically unsuitable.

Besides engaging senior politicians who have a role in managing the institution, it can also be beneficial to share high-level plans in due course with whips/party business managers and with government officials (given that government cabinets spend time on parliamentary estates).

IT Network Outage

Thursday is the busiest day of the week as many parliamentary committees meet in the morning and the main question time event takes place at lunchtime. This means that most Members and their employees are focussed on parliamentary business rather than handling casework or dealing with administrative tasks. Most of the legislature's administrative staff, however, would be working at their desks.

As such, it was administrative staff who noticed a gradual slowdown when using any piece of software on their PCs. This included websites being slow to respond or unavailable, documents not printing and the inability to access corporate systems. As lunchtime approached the problems worsened and it became apparent that there was a significant issue with the main IT network for the parliament. Systems that support the operation of the chamber are on a physically separate network so they were working normally. The phones are also separate so they worked fine too.

The IT staff were now focussed on finding and fixing the issue and in using phone calls and face-to-face engagement to advise Members on what they needed to do to prepare for business that afternoon. As the fault-finding continued, it became apparent that the network would have to be shut down to properly identify where the issue was coming from. This could take some time and the order of restoration of service had to be prioritised. Members are the main focus so the part of the network supporting their offices would be brought back up first and space would be found in the same area for the urgent work of the parliament – this was preparing material for parliamentary committee meetings the following week and any processing of amendments for upcoming chamber debates.

There was an existing policy that allowed for staff to be asked to step aside in an incident and this allowed for some of the chamber and committee staff to use space normally used by engagement and other support functions. This allowed for urgent work to resume while IT colleagues continued their fault-finding and rectification work. The faulty component was identified and quickly replaced and the rest of the network was restored section by section through the rest of the afternoon and evening.

So while chamber-specific systems were not affected and business there could continue as normal, there was wide disruption to every other area of the legislature. Being clear on the most urgent pieces of work allowed for resources to be moved around for that to take place and the ability to do that had been established through a specific business continuity staffing policy and the overall concept of focusing on essential activities.

While the technical issues were difficult to overcome, the biggest challenge for that day was to communicate with everyone when email was unavailable. Again, the IT colleagues recognised that this work should be prioritised and stopped any project and development work to allow those employees to take on a lot of the communications burden.

Responding to UK's Critical Terrorism Threat Level

In 2017, following the Manchester terrorist attack, the United Kingdom moved from *severe* to *critical* terrorism threat level, the highest level. This change of threat level status happened without warning late at night, meaning that for those organisations with buildings accessible to the public, there was the added complexity of making changes and communicating these changes out of normal working hours.

In the morning following the attack, the incident management framework was used to help manage two key priorities: the protocol response and the security response. The protocol response involves decisions around lowering of flags as a mark of respect; making books of condolence available; statements of condolence from the Speaker; letters conveying sympathy and support to the relevant authority; and preparations for a motion of condolence in the Chamber. The security response involved implementing increased searching and concentration of security staffing on the public entrance to the building. This was done through liaison with the relevant security authority to take advice, and where necessary, additional actions.

Although the threat level on the first day after the attack remained *severe*, officials took the opportunity to remind the Speaker, senior politicians and senior staff of the steps that would be taken should the threat level rise. Also, incident management teams started to plan how this would be communicated, including out of hours, and how it could be resourced and managed.

Fortunately, this planning helped when the move to *critical* came overnight. Short pre-prepared messages were pushed out to Members and their staff using an emergency messaging system to notify them of the changes to their routines when they came to the building. This was followed by a more comprehensive organisation-wide message setting out more reassurance, detail on changes, and next steps. Media received information and helped communicate to the public what to expect if visiting the legislature and cancellation of relevant events. Operational teams took agreed steps to cancel activities; relocate others; and convey consistently what was happening and why to external audiences. The incident management team (of senior staff) met twice to monitor feedback, discuss and deal with any operational issues. Based on this, the legislature made some pragmatic changes to how it was implementing the additional security checks.

The threat level was lowered after five days. In the subsequent debrief, the legislature noted that a previously agreed security stance had been hugely beneficial; internal communications had played a significant role in reassurance and implementation; and it practically considered further how it could deploy staff resources should it have to remain at a heightened threat level for a longer period.

Reputational Aspects of Crisis Management

Those who work in legislatures face particular issues when it comes to managing any kind of unforeseen incident given that most have an onsite media presence and/or are scrutinised and reported on daily. The media are people who have a job to do as well as those potentially impacted by an incident as it unfolds. In the era of social media, of course, anyone with a mobile device, which is most Members, staff and visitors can also report on a situation in real time.

There are certain aspects of reputation management that may be useful for legislatures to consider, in addition to the best practice advice set out in crisis communications manuals and guidance.

Many legislatures have a commitment to broadcast some or all of their proceedings. A broadcast policy should be considered to deal with any interruptions or disruptions to parliamentary business in plenary or committee, and having an agreement on these with politicians and broadcasters.

It's worth bearing in mind that Speaker statements from the Chair during plenary will define how an incident is perceived and shapes the early analysis of how the legislature is responding – by those in the room as well as external observers. As part of planning, consideration should be given to what can be scripted and available for the Speaker in a range of anticipated scenarios. Some legislatures are also trialling instant messaging between staff in key offices such as chamber desk services, broadcasting and media relations so that Speakers can be advised more immediately, on political reaction, social media sentiment, and media coverage, as a situation unfolds.

In a crisis, individual Members are likely to engage online and will be pursued by the media to give interviews. Experience shows that it's important to keep Members and staff informed regularly, even if the updates are only confirming that nothing has changed, to help manage the information vacuum that can exist in an incident and which can be filled by speculation.

If possible, it's useful to have identified key senior politicians and officials as spokespeople and to provide regular crisis communications training. This is a form of media training that can help prepare spokespeople for interviews when faced with uncertain and stressful situations. This is done once a session with the incoming Speaker and the small body of parliamentarians who are responsible for governing the legislature.

Incident Welfare Team

Parliament had recognised that it needs specialist teams to respond to business continuity incidents that might occur. This included ensuring that it had a team that would handle effective communication with stakeholders, a team that could source any necessary alternative accommodation, and a team that would restore the critical IT systems if they had been affected by an incident. Once everyone became comfortable about the roles and responsibilities for these teams, it became apparent that there was one rather significant gap in the setup – that was how people would be looked after if an incident took place at the legislature. It was clear that that need had to be addressed, but what would that responsibility look like and how could it be fulfilled?

In discussions with the business continuity board it was agreed that some research and training should be undertaken to determine what good practice might look like and what had to be done to put in an approach that would be aligned with that. To this end two members of staff attended a 'Human Aspects of Business Continuity' course to see what issues might need to be addressed. This was highly useful and allowed a considered approach to be developed that would cover three areas over three periods of time:

a. Short term: A trained team would be put in place to handle the immediate needs of regular building occupants getting home after an incident. So, as well as ensuring that the incident welfare team (IWT) members had the ability to book train tickets/pay for buses and taxis to get people home, emotional first aid to help them understand how people – including themselves – might respond to a disruptive incident was also provided.
b. Medium term: After any immediate transportation and welfare needs had been taken care of, the IWT would look to ensure that those running the incident teams properly considered the need and time necessary for staff to rest and take time away from the stressful work of managing and recovering from an incident. This could be as simple as booking a nearby hotel room for staff to rest and get cleaned up.
c. Longer term: After a significant and traumatic event it may be necessary to manage the longer-term needs of those involved and affected by the event. In this case the IWT would work with human resources colleagues to ensure any counselling was in place and would also ensure that any anniversaries of an event were appropriately marked.

While instinctively the responsibilities of the IWT might have been seen as only needing the involvement of human resources, volunteers were deliberately sought from across the legislature to be part of the team. Taking this approach has ensured that a motivated group of people have been brought together and, coupling that with regular refresher training and assessing how external incidents might have impacted the legislature, has ensured that confidence is high that the IWT will work well if called upon.

Glossary

Alternate Site	A facility to be occupied in the event that the primary site is inaccessible.
Assets	Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
Availability	The state of being accessible and usable in a timely and reliable manner.
Awareness and Training Programs	The programmes to create and maintain corporate awareness and enhance the skills required to implement the BCM programme.
Business Continuity Lifecycle	The stages of activity that an organisation moves through and repeats with the overall aim of improving organisational resilience.
Business Continuity Management (BCM)	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 of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.
Business Continuity Management (BCM) Programme	The ongoing management and governance process supported by top management and appropriately resourced to implement and maintain BCM.
Business Continuity Management (BCM) Strategy Development	The selection of possible business operating strategies for continuation of business within the minimum acceptable service delivery and minimum acceptable downtime limits.
Business Continuity Plan (BCP)	The documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Business Continuity Policy	The key document that sets out the scope and governance of the BCM programme and reflects the reasons why it is being implemented.

Business Impact Analysis (BIA)	The process of analysing activities and the effect that a business disruption might have on them.
Business Resilience	The capability to anticipate key events from emerging trends, constantly adapt to change and to bounce back from disruptive and damaging incidents.
Crisis	A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action.
Crisis Communications	The planned and exercised methods to communicate with internal key contacts (management, employees) and with external stakeholders (public, vendors, suppliers) and the media (radio, television, Internet) during a time of disruption.
Critical Service	A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of the organisation.
Design	The practice within the BCM lifecycle that identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved.
Disruption/Incident	A situation that might be, or could lead to, a disruption, loss/denial, emergency or crisis. **Short-term disruption:** A period of ten days or less. **Medium-term disruption:** A period of ten days to one month. **Long-term disruption:** A period of one month or longer.
Emergency Response and Operations	The procedures for response during/following an incident, e.g. safe rooms/ common clustering points, evacuation plans, lock-downs.
Exercise	A process to train for, assess, practice and improve performance in an organisation. *(Note: Exercises can be used for validating policies, plans, procedures, training, equipment, and inter-organisational coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement, and controlled opportunity to practice improvisation).*

Exercise Programme	A series of exercise events designed to meet an overall objective.
Formal Debrief	A discussion held within weeks of the incident or exercise, addressing the wider organisational issues that identify learning opportunities.
Hot Debrief/ Hotwash	A discussion about the issues and concerns held immediately following an incident or exercise.
Implementation	The practice within the BCM lifecycle that executes the agreed strategies and tactics through the process of developing the BCP.
Invocation	The act of declaring that an organisation's business continuity arrangements need to be put into effect to continue delivery of key products and services.
Level 1 Incident	An emergency that disrupts one directorate only, whereby the rest of the organisation is unaffected (e.g. office fire, small flood; loss/denial of personnel, office space, and information).
Level 2 Incident	An emergency that disrupts all or a large portion of the organisation (e.g. loss/denial of a building due to fire, terrorism, earthquake, bombing).
Level 3 Incident	A disastrous emergency that curtails the whole infrastructure such as a biological, chemical or explosive event, or a major natural or anthropogenic (man-made) event.
Maximum Tolerable Period of Disruption (MTPD)	The time it would take for adverse impacts, which might arise because of not providing a product/service or performing an activity, to become unacceptable.
Minimum Business Continuity Objective (MBCO)	A minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption.
Post-Incident Acquisition	A continuity and recovery strategy where resources are provided following an incident at short notice.

Recovery Point Objective (RPO)	The point to which information used by an activity must be restored to enable the activity to operate on resumption.
Recovery Time Objective (RTO)	The period of time following an incident within which a product or an activity must be resumed, or resources must be recovered.
Replication	A continuity and recovery strategy where resources are copied to a dormant site, only being brought into live operations after an incident.
Resilience	The adaptive capacity of an organisation in a complex changing environment.
Risk	The effect of uncertainty on objectives.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Evaluation and Control	The determination of events that can impact the organisation and its resources. Identification of the controls needed to prevent or minimise the effects of potential loss/denial.
Risk Management	The coordinated activities to direct and control an organisation regarding risk.
Safe Separation Distance	An adequate geographical spread between the original and duplicate resources, the various suppliers, the replica operations of the base site and its alternate site.
Single Point of Failure	The element or part of a system for which no backup (redundancy) exists and the failure of which will disable the entire system.
Test	A unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.
threat	A potential cause of an unwanted incident, which can result in harm to individuals, a system or organisation.
threat Analysis	The process of evaluating threats to identify unacceptable concentrations of risk to activities and single points of failure.

This glossary has been compiled from a variety of sources including, but not limited to, the *BCI Good Practice Guidelines* and ISO standards.

Reference and Contact Details

Reference Material Sources

Additional general reference material sources on business continuity planning may include:

- Your Auditor General and Internal Audit reports
- The Institute of Internal Auditors
- UK Emergency Planning College
- Business Continuity Institute
- Disaster Recovery Institute
- International Organisation for Standards (IS0 22301)
- Public Safety Canada Guide to Business Continuity Planning

How to Contact LABCoN

For more information on LABCoN, please visit the following website: http://labcon.network
If you have further questions on LABCoN, on this guide, or on implementing a BCM programme in your legislature, please contact by email any of the LABCoN representatives below:

House of Commons of Canada: labcon@parl.gc.ca
Legislative Assembly of British Columbia: labcon@leg.bc.ca
Legislative Assembly of Ontario: labcon@ola.org
New Zealand House of Representatives: labcon@parliament.govt.nz
Scottish Parliament: labcon@parliament.scot
Senate of Canada: labcon@sen.parl.gc.ca
United Kingdom Parliament: labcon@parliament.uk