# Business Continuity Guide 2017

Government of Alberta ■
*Alberta Emergency Management Agency*

June 2017

## Acknowledgements

The Business Continuity Guide is the primary resource document for the Government of Alberta's departments in the development of a business continuity plan as defined by the Alberta Emergency Plan. The Alberta Emergency Management Agency has prepared this guide in order to provide a frame of reference for Business Continuity Officers to develop, maintain, and improve their departmental Business Continuity Programs. Consideration has been given to the development of three components: the legislated requirements, business continuity plan components (ability to activate and implement the plan), and business continuity management program components (ability to improve department's business continuity resilience) for continuous improvement.

The guide emphasizes departments' responsibility to resume essential services for Albertans in the face of business continuity disruptions. In managing business continuity disruptions, a successful outcome is judged by both the technical response and the perceived competence of the management.

We hope you find this guide a valuable addition to your business continuity planning resources. If you have any questions, comments, or recommendations for amendments, please contact:

**Plans Manager**

**Alberta Emergency Management Agency**
**14515 122 Ave NW**
**Edmonton, Alberta T5L 2W4**

**Phone: 780-422-9000**

**Website: http://www.aema.alberta.ca**

3rd Edition
ISBN 978-0-7785-5982-5

## Record of Amendments

The Business Continuity Guide may require updates and amendments based on various factors. In order to ensure that the most accurate copy of the Guide is maintained, it is recommended that a business continuity team member be assigned the responsibility of maintaining current copies of the Guide.

List of all amendments made to the Guide since inception.

| Amendment Number | Effective Date | Amended By (Please print) | Initials |
|---|---|---|---|
| 2007-01 | April 2007 | | |
| 2014-02 | 15 August 2014 | Shem Bundi | SB |
| 2017-03 | 1 June 2017 | Alan Younghusband<br>Dan Howlader | AY<br>DH |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Table of Contents

# Business Continuity Management

## 1.1 Executive Summary

When a significant event causes disruption to the provision of essential services to Albertans, the Government of Alberta (GOA) will execute the GOA Business Continuity Plan (BCP) in order to recover the disrupted services. The GOA BCP outlines the framework by which the government manages the continuity of its essential services during business disruptions. Under the coordination of Alberta Emergency Management Agency (AEMA), individual departments will implement their individual BCPs (as required) to ensure the continuation of critical and vital services that are essential for the health and safety of all Albertans. Under current legislation and in conjunction with industry best practices, AEMA and GOA departments maintain comprehensive Business Continuity Management programs to address the known and unknown risks that may adversely affect Albertans.

This guide will assist Business Continuity Officers (BCOs) and their teams through the process of business continuity planning and management. This guide is intended as an overview of current best practices targeted at GOA departments, and while extensive, may not cover all unique requirements for each department. Users are encouraged to seek additional information as needed of this guide to meet the demands of their departments. Similarly, while many of the lessons and components in this guide may transfer to municipal management, outside users should ensure fit and applicability for their specific requirements. Additional information and assistance for GOA departmental Business Continuity Teams (BCTs) is available from AEMA.

## 1.2 GOA Business Continuity Management (BCM)

When a disruptive incident occurs, and the initial emergency response has been resolved, departments need to begin the task of restoring and maintaining essential services to Albertans. Through a comprehensive Business Continuity Program, with a documented BCP, departments will be able to assess potential risks, understand their impacts, and know how to resume essential services efficiently and effectively, regardless of the mechanism of disruption.

A comprehensive Business Continuity program will:

- Ensure provision of essential services to all Albertans.
- Ensure and maintain confidence in government.
- Minimize potential revenue loss.
- Reduce the impact related to service disruption.

## 1.3 Authority and Legislation

The current legislative framework for business continuity planning in the GOA is derived from the *Emergency Management Act* (EMA) and the *Government Emergency Management Regulation* (GEMR). These documents assigned roles, responsibilities and authorities for business continuity planning in the GOA.

The GEMR assigns AEMA the responsibility for developing, implementing and maintaining the Alberta Emergency Plan (AEP) and the GOA BCP. The GEMR also assigns AEMA the responsibility for requiring each department, in consultation with AEMA, to prepare, implement, and maintain a BCP. The deputy heads of departments (typically deputy ministers) retain the accountability for business continuity planning within each department.

## 1.4 Guiding Principles

This guide provides a frame of reference for BCOs to develop, maintain, and improve their departmental BCM program. This guide is meant to highlight current industry best practices and provide suggestions or an alternative perspective that will enhance existing BCPs. The Guide is not a prescriptive instruction manual that must be followed to meet GOA BCP requirements. While not focusing on templates, it is understood that content specific to the department be more important than standardization of the plan.

## 1.5 Business Continuity Standards and Best Practices

Business continuity continues to gain momentum and recognition within both the national and the global emergency management framework. Currently, the GOA recognizes that in the international business continuity community, ISO 22301:2012 provides leadership and comprehensive standards for business continuity professionals to benchmark against in developing and enhancing their BC programs. AEMA uses CSA Z1600 to create measureable goals within a national context. Both of these standards are used as benchmarks in developing this Guide and will be used on an ongoing basis to inform best practice for the GOA.

## 1.6 Acronyms

| Acronym | Full Spelling |
|---|---|
| AEMA | Alberta Emergency Management Agency |
| AEP | Alberta Emergency Plan |
| BC | Business Continuity |
| BCG | Business Continuity Guide |
| BCM | Business Continuity Management |
| BCO | Business Continuity Officer |
| BCP | Business Continuity Plan |
| BCT | Business Continuity Team |
| BIA | Business Impact Analysis |
| CSA | Canadian Standards Association |
| DM | Deputy Minister |
| EMA | Emergency Management Act |
| EOC | Emergency Operations Centre |
| FERP | Facility Emergency Response Plan |
| GEMR | Government Emergency Management Regulation |
| GOA | Government of Alberta |
| GOA BCP | Government of Alberta Business Continuity Plan |
| IAP | Incident Action Plan |
| IT | Information Technology |
| MTPD | Maximum Tolerable Period of Disruption |
| RTO(s) | Recovery Time Objective(s) |

## 1.7 Terms and Definitions

**Business continuity management** – A holistic process that identifies potential threats / risks to the organization and the impacts those threats / risks may pose to continuity of essential services. This is a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders and organizational reputation.

**Business continuity plan** – A plan that prioritizes essential services, employs mitigation measures, and coordinates and implements the continuity of service strategies when a business disruption occurs.

**Business continuity program** – Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

**Business disruption** – Any event, anticipated or not, which causes an unplanned, negative deviation from the expected delivery of essential services according to GOA objectives.

**Business impact analysis** – Process of analyzing government activities and determining their criticality based on set criteria.

**Department** – A department is a cabinet minister's area of responsibility, or portfolio, and the people who work for the ministry. The Minister, who is head of the ministry, is a member of the Executive Council. For the purpose of this plan, a department will include Agencies, Boards, and Commissions (ABCs) with the understanding that their participation in the program is largely voluntary and at the discretion and direction of their department deputy head.

**Essential (or common) function** – An internal function or process that supports a department's essential services, there are two types of common functions:

- A business procedure that can be either automated or manually operated.
- A business unit of a department that is crucial to the continued functioning of the department's essential services.

**Essential services** – There are four categories of essential services: Critical, Vital, Necessary, and Desired. Essential services are a product or benefit delivered directly to external stakeholders by departments of the GOA. Essential services are delivered to either:

- Citizens of Alberta, including, but not limited to individuals, families, organizations or local governments; and
- Other departments of the GOA or other levels of government that support the citizens of Alberta.

**Exercise** – Process to assess, practice, and improve performance during a simulated business continuity disruption.

**Maximum Tolerable Period of Disruption (MTPD)** – This is the period it would take for adverse impacts, which might arise as a result of not providing a product / service or performing an activity, to become unacceptable.

**Recovery Point Objective** – Refers a point to which information technology (IT) used by an activity must be restored to enable the activity to operate on resumption.

**Recovery Time Objective** –The period of time following an incident within which product or service must be resumed, or activity must be resumed or resources must be recovered.

**Resources** – All assets, people, skills, information, technology, premises, and supplies that an organization has to have available to use, when needed, in order to operate and meet its objectives.

**Risk** – Something that exposes the GOA to potential disruption of essential services, and is evaluated by likelihood and impact.

**Risk assessment** – Overall process of identifying, analyzing, and evaluating risks.

**Significant Business Continuity Disruption** – An event where:

1. A single department is overwhelmed and is unable to manage / respond to the incident with internal resources
2. Multiple departments are impacted for longer than 24 hours
3. Government is not able to maintain essential services within predefined timeframes (24 hours for critical services, 72 hours for vital services and two weeks for necessary services).
4. The Provincial Operations Centre is at levels 2-4 in response to a business continuity disruption (see Section 8.5 for more details).

**Vital Records** – Vital records are those without which a public authority could not continue to operate. They may include documents, files, or records in any form or format, containing information that is essential to operations.

## Business Continuity Program Creation and Management

### 2.1 What is a Business Continuity Program?

At its core, business continuity is focused on minimizing preventable disruptions to the essential programs and services offered by a government, an industry, or a business, and when preventing service gaps is no longer an option, business continuity describes processes and practices to restore and resume business as efficiently as possible. Within the GOA, business continuity refers to both the protecting of outward services provided to Albertans as well as to the internal processes that support those services.

The central document of a business continuity program is the BCP, which prioritizes essential services, describes mitigation measures, and coordinates and implements continuity of service strategies when a business disruption occurs. The BCP should be a living document that reflects the values, objectives, and framework of its department that grows and changes in accordance with each departmental reorganization. A BCP must outline realistic and achievable strategies that help departments identify and prioritize their core services; recognize risks and how to mitigate them; and create specific, actionable solutions to continue providing service regardless of disruptive events and emergencies.

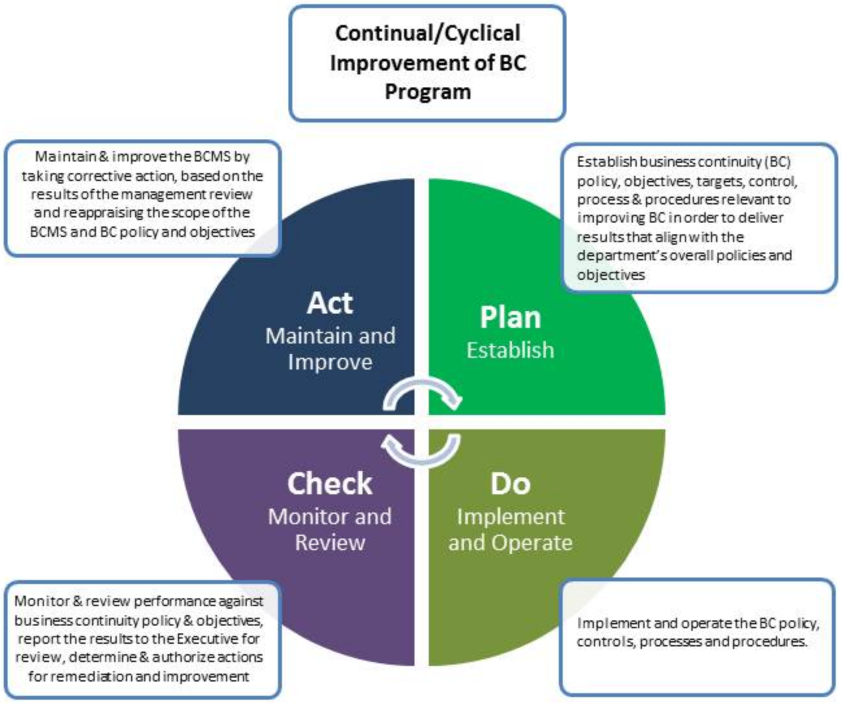
The BCM program is a cyclical program that delineates and describes all activities concerning business continuity within the department. A typical BCM Program encompasses development of a BCP with all that this entails as described in this guide; awareness and training for the department on the BCP; execution of the BCP as required; and amendments and improvements to BC matters on a regular basis.

The BCM program must be managed within an established framework and according to the principles contained in the department's BCM policy. A BCM Program must reflect the department's strategy, objectives and culture to ensure that the program is relevant, effective and meets current service delivery goals.  The cyclical /continual improvement of BC program involves a Plan, Do, Check and Act Model as illustrated in Figure 1 below.

### 2.2 BCM Program Scope

Clearly defining the scope of the BCM program allows the BCT to describe what is encompassed by the program, and limits redundancies caused by external partner plans or programs. The scope of a BCM program begins with identifying the departmental mission and objectives, and outlining what processes and services support those overarching principles. A clearly articulated scope also helps participants understand the limitations of a BCM program.

**Figure 1 – Cyclical / Continual Improvement of BC Program**



Maintain & improve the BCMS by taking corrective action, based on the results of the management review and reappraising the scope of the BCMS and BC policy and objectives

Establish business continuity (BC) policy, objectives, targets, control, process & procedures relevant to improving BC in order to deliver results that align with the department's overall policies and objectives

Monitor & review performance against business continuity policy & objectives, report the results to the Executive for review, determine & authorize actions for remediation and improvement

Implement and operate the BC policy, controls, processes and procedures.

## Business Continuity Plan Development

### 3.1 Overview and Plan Development Objectives

Business continuity plans provide guidance for sustaining essential services during a disruption, and procedures for recovering those functions that are disrupted.

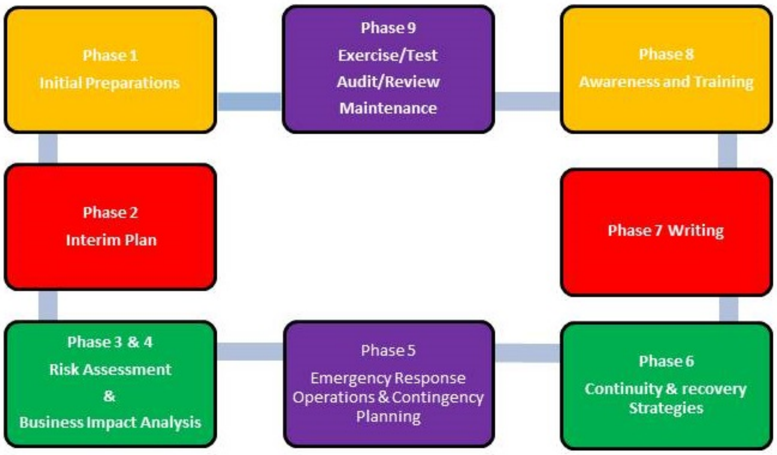
Plan development objectives are to:

- Understand the purpose and role of supporting plans (i.e. Communication Plan, Crisis Management Plan, Facility Emergency Response Plan, Disaster Recovery Plan), and development of policies and procedures.
- Identify the key people involved in implementing the BCP, and clarifying their roles and responsibilities before, during, and after a disaster.
- Understand the process, design framework, structure, and contents of the BCP.

### 3.2 Planning Steps / Development Process

Developing a plan is an extended process that will engage multiple partners across your department. It is recommended that you work through a progressive development process that will enable to you to build your BCP through collaborative and objective analysis.  The successive planning steps / development process described below are intended as a suggested method that will facilitate GOA departments in producing an effective BCP.  In order to develop a relevant and tailored BCP, each departmental BCO must determine the level of detail required for each step to address their specific departmental needs.

**Figure 2 – Planning Steps Flowchart – Phases of BCP Development**



#### 3.2.1 Initial Preparation

As in any major policy or program development, there are initial key steps that must be satisfied before creating a BCP. Below are common considerations which will need to be addressed prior to Plan development. This is not an exhaustive list; individual departments may have unique considerations in their initial preparation.

- Engage Management

  - Identify the right level of management to sponsor the Business Continuity Program.
  - Ensure management understands what the BCP will encompass, when it would be used and what are its intended outcomes.
  - Be open about the resources necessary to complete a BCP and confirm that these resources will be available throughout the development of the plan.
- Establish BCMS requirements, considering the organization’s mission, goals, internal and external obligations, and legal and regulatory responsibilities.
- Secure team member participation and commitment.
- Define the scope of your BCP.

### 3.2.2 Interim Plan

BCP development takes time, and disasters can happen at any time prior to completion of a thorough plan. If a BCP is being developed for the first time (as opposed to updating or modernizing an existing plan), departments may want to consider adopting an interim plan. An interim plan offers limited protection against disruptions and should be prepared when the department doesn’t have an existing BCP or the current BCP is significantly out of date. The interim plan should be solely focused on critical services which are regarded as particularly at risk or vulnerable. In order to ensure timeliness of an interim plan, the plan should be developed independently by the BCT; the formal BCP development will engage all stakeholders.

Key things to consider when devising an interim plan are:

- Notify management about the Interim Plan Structure and Roles
- Appointment of a Business Continuity Team (BCT) to develop the Interim Plan
- Establish a procedure for convening the BCT
- Identify basic recovery requirements and practical recovery strategies
- Ensure that all members of the BCT have a copy of the Interim Plan and that they are fully briefed on its contents

### 3.2.3 Risk Assessment

Risk Assessment (RA) consists of identifying and assessing risks that can potentially disrupt business operations. Upon completion of a risk assessment, BCOs should know the most likely and most dangerous threats to departmental operations. The RA then will inform possible actions for risk mitigation. Risk mitigation consists of those actions that can be taken to reduce the likelihood of the occurrence of a specific risk, or reducing the impact should the risk occur.

### 3.2.4 Business Impact Analysis

Business impact analysis (BIA) begins with identifying the specific business units within the department, and the specific resources required to execute the responsibilities of those units. These resources include (but are not limited to) specific locations, staffing levels, IT requirements, training requirements etc. From here, the Business Continuity Team will then assess the effect on the department should one of the Business Units be unable to execute their duties. This enables the Business Continuity Team to prioritize the services and resources necessary to maintain (or restore) the essential Business Units in the event of a disruption.

### 3.2.5 Emergency Response and Contingency Procedures

This phase consists of reviewing existing emergency response procedures and assessing their connection to the BCP. Emergency response plans often focus on contingency activities for specific types of disruption, plan activations, and coordination that will need to be generalized to meet with the all-hazard approach of a BC Program.

### 3.2.6 Disaster Recovery and Continuity Strategies

Disaster recovery strategies are specifically concerned with recovering the technology and information (IT) systems that support the department. Continuity Strategies are those strategies designed to resume departmental operations other than IT systems – for example manual workarounds or staffing reallocation.

### 3.2.7 Writing

This phase identifies the key people who will draft, review, and produce the actual BCP. This team establishes the structure of the BCP, identifies necessary sections of the plan, and evaluates the information that will be included in the plan.

### 3.2.8 Awareness and Training

This section outlines the specific training requirements necessary for executing specific response and recovery activities, and details the mechanisms by which the department will be made aware of Business Continuity as a whole. A comprehensive Awareness and Training program ensures that all members of the department will be able to work together effectively.

### 3.2.9 Review, Test, Exercise, Audit, and Maintenance

Once complete, the BCP must be tested (preferably through an exercise) to validate the plan and identify any areas that require clarification/improvement. If possible, upon completion of initial validation through an exercise program, the BCP should be audited by an outside agency to ensure clarity and thoroughness by someone who is not intimately familiar with the department. Finally, once the BCP has been validated and reviewed for effectiveness, the BCP will require regular review and maintenance to ensure that it remains relevant to the organizational structure and responsibilities until the next formal revision.

## 3.3 Structure and Content of the Business Continuity Plan

A BCP shall include sufficient information to enable individuals not intimately familiar with the internal workings of the department to clearly understand how the department will maintain its essential services in the event of a disruption. There is no set template for a BCP; all departments must determine what best addresses their needs.

### 3.3.1 Cover Page, Contents and Layout

The cover page must clearly display the effective date, confidentiality restrictions (if any), and any legal disclaimers. An executive foreword by the senior member of the Business Continuity Team is also required to signify Executive approval and support of the plan. The executive forward may also be written or endorsed by the department’s deputy head.

### 3.3.2 Business Continuity Program

#### Introduction

The introduction outlines the Business Continuity Management program of the department, the structure, and purpose of the BCP, conditions for activation of the plan, and who is specifically affected by the plan.

#### Department Business Continuity Management (BCM) Program Policy

This section describes the departmental policy underlying the BCM Program. At a minimum, it will include:

- Applicable legislation and regulation or governance framework.
- The department's specific policy statement regarding Business Continuity.
- The specific objective, scope, and assumptions underlying the BCM Program.
- Specific program limitations (if any).

#### Departmental Organizational Structure

This section outlines the overarching structure of the department. It lists the business units of the department, and briefly describes the function of each of the departments. This enables a clear understanding of the interdependence of the business units, and the services they provide both within the department and externally to the GOA and Albertans.

#### Departmental Business Continuity Organizational Structure

This section identifies those personnel specifically assigned tasks in the departmental BC program. This section describes the roles and responsibilities of each member of the BCT and identifies essential and non-essential personnel in the event of a disruption of any type. The departmental business continuity organizational structure includes (but is not limited to) the executive team, the designated BCO(s), and representatives from each business unit.

### 3.3.3 Plan Activation, Coordination and Communication

#### Activation and Escalation Procedures

This section explains the criteria by which the BCP is activated and the procedures for its implementation. It includes notification procedures, recall of essential personnel procedures, and instructions on activation of Emergency Operations Centre (EOCs) or alternate sites.

#### Communications and Coordination

This section outlines the procedures by which all communications, both internally to affected staff and externally to the GOA and Albertans, as a whole will be executed. At a minimum this section will include specific identification by position as to who is authorized to speak for the department, and the means by which this communication will be executed. This section also outlines coordination processes in both routine operations and in the event of a disruption.

#### Essential Services List

This section lists all essential services provided by the department and identifies the maximum tolerable duration they can be disrupted. This enables prioritization of resources and recovery efforts. This list will include those sections resources that are necessary for supporting the essential service.

#### Contact Information

This section includes current contact information for those personnel identified as essential within the BCP. At a minimum, it must include an e-mail addresses and telephone number for a departmental contact for both working hours and after-working hours.

### 3.3.4 Business Impact Analysis and Risk Assessment

While not a specific element of the BCP, the business impact analysis  and risk assessment  should be included so that the broader context of the BCP is better understood.

### 3.3.5 Business Unit(s) Continuity Procedures

For smaller departments in the GOA that operate from a single location, a single BCP may be sufficient. For larger departments, or departments that operate from multiple locations, it may be necessary for individual business units or geographic regions to prepare a separate BCP. In this case, individual Business Units or location-based Continuity Plans will be included in the departmental BCP as separate documents or annexes. The departmental BCP will describe how the department as a whole will recover from a disruption that affects the department generally; the Business Unit Continuity Plans will describe how each specific Business unit will recover from a disruption that affects a business unit individually.

### 3.3.6 Review, Maintenance, Training, and Exercises

This section describes the means by which the BCP is maintained, trained, tested, and updated. At a minimum it will include identification of who is responsible for review, maintenance and exercise design (usually the BCO) and the frequency for each of the listed activities.

### 3.3.7 Supporting Documents

This section includes any supporting plans or documents that help inform, but are not essential to the departmental BCP. These documents are usually in the form of annexes, appendices, and attachments depending upon how critical they are to the understanding of the departmental BCP.

## 3.4 Approval and Distribution

Once the BCP is finalized, the BCO will schedule a briefing to the executive members of the departmental BCT. At this time the BCO will review the plan in detail and seek formal approval of the plan. In the GOA context, approval authority is generally held at the level of Deputy Minister.

### 3.5 Summary

Business continuity plans are living documents that require a great deal of time and effort to prepare properly. They must be reviewed, and revised if necessary, every time the circumstances from which they were prepared materially change.

Executive Team buy-in is paramount to the success of any BCP. Without top-level involvement in the development and implementation of the Business Continuity Program, the program risks stagnation or under-prioritization. This will lead to the GOA being ineffective when Albertans need them most.

## Plan Activation and Incident Management

### 4.1 Overview

This section describes the identification and communication processes following a business disruption, including the initial impact assessment, and how a decision to activate the BCP is made and by whom. This section also describes the establishment of emergency operations and notification process for recovery teams. Specific procedures are required for:

- Incident management.
- Incident detection and reporting.
- Alerting and notification.
- BCP activation and deactivation.
- EOC activation.
- Impact and damage assessment (coordinated with emergency response plan) and situation analysis.
- Development and approval of an Incident Action Plan (IAP).

### 4.2 Management and Control Responsibilities

This section provides an overview on incident management span of control. It describes the roles and responsibilities of key players within the BCM program and identifies the delegation of authority and management succession in the BCM program. Within the GOA, this section can also outline departmental liaisons to the BCP.

#### 4.2.1 Executive Team

The executive team is responsible for decision-making and directing crisis communication for significant business disruptions. They retain the authority to activate the BCP, and may, where appropriate, delegate that authority to the BCT in accordance with the department’s BCP.

#### 4.2.2 Management Team

The management team reports directly to the executive team, and has the responsibility to oversee business recovery and continuity processes being executed by the BCT and the operational staff. They are responsible for communicating recovery status to the executive team and making the necessary management decisions to support the recovery efforts, in addition to implementing executive decisions. They oversee the business disruption from the initial response to the point at which normal business operations are resumed based upon continuity strategies. Their responsibilities include:

- Assessing preliminary impacts with support from the BCT.
- Provision of regular reports to the executive team on the status of the incident (when activated) or status of the program (regular business cycle).
- Developing action plans during an event for executive approval.
- Execution and supervision of the BCP with executive team direction.
- Organization and provision of administrative support to the recovery effort.

#### 4.2.3 Operational / Response Team

The operational / response team is responsible for executing specific recovery processes necessary for continuity or recovery actions of critical business functions at the primary or alternate locations. Response teams may be broken into sub-teams, each with their own leader to facilitate the recovery effort, their responsibilities include:

- Execution of the recovery procedures for their business area.
- Communication of the status of recovery, including issue identification, to the management team as needed.
- Identification of resources needed for recovery operations.

### 4.3 Emergency Operations Centre Location

Emergency response efforts following a disruption are coordinated from a departmental EOC. When developing an EOC plan, consideration should be given to communication systems, facility security, and equipment needed during the BCP activation. A primary and secondary location for the departmental EOC should be included on the plan.

### 4.4 Emergency Procedures

A Facility Emergency Response Plan (FERP) responds to a specific facility/building emergency event. It focuses on ensuring the health and safety of the building’s occupants, identifies hazards specific to the facility, and outlines the processes for evacuating the facility. FERPs are not a part of BCPs, but they are interlinked.

### 4.5 Activation Procedures and Operations

Differing levels of impact will require differing levels of response. Determination in advance of level of impact/response will ease decision-making with respect to a business continuity disruption. Level of impact is determined based upon the effect on essential services. Below are a number of aspects that a BCP should cover, including:

Notification processes:

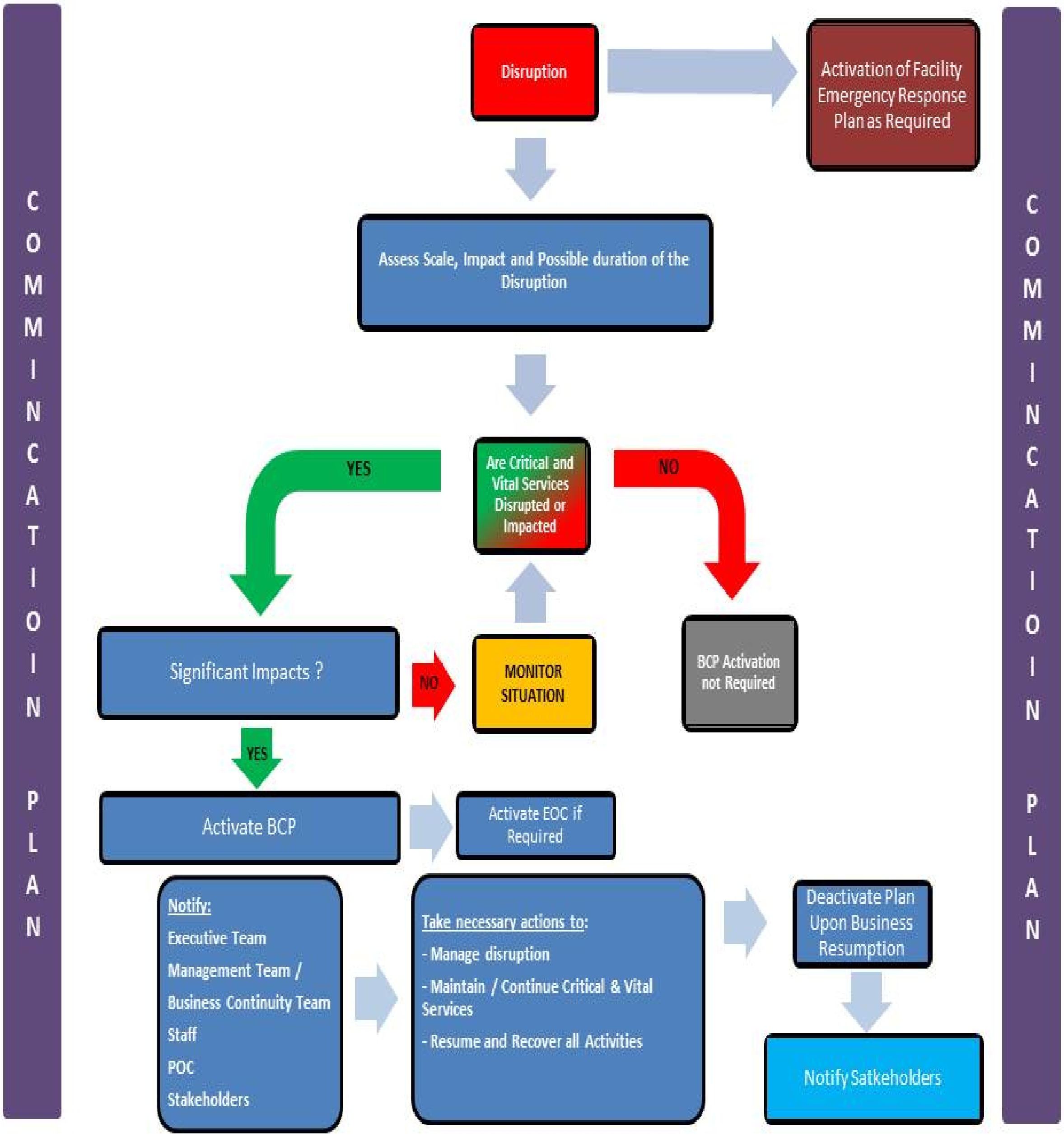
- Notification of a potential or actual disruption with impacts to essential services to BCT members and management.
- EOC activation and the methods by which the BCT will be convened.
- External Partner notification procedures.
- Staff notification procedures.
- BCP implementing instructions (roles and responsibilities, locations etc.).
- Impact assessment criteria, including triggers for escalation
- Triggers by which response activities can be reduced.
- The process to deactivate the BCP.
- Procedures for demobilization and resumption of normal operations.

### 4.6 Communication Plan

The communication plan must clearly describe:

- Management of internal / external communications.
- Lines of responsibility for communications between Executive Team, Management Team, and Operational Response Teams.
- Draft key messages for external partners who may be affected by the disruption.

**Figure 3 – Plan Activation Process Flowchart**


COMMINCATIOIN PLAN
Disruption
Activation of Facility Emergency Response Plan as Required
Assess Scale, Impact and Possible duration of the Disruption
YES
Are Critical and Vital Services Disrupted or Impacted
NO
Significant Impacts ?
NO
MONITOR SITUATION
BCP Activation not Required
YES
Activate BCP
Activate EOC if Required
Notify:
Executive Team
Management Team /
Business Continuity Team
Staff
POC
Stakeholders
Take necessary actions to:
- Manage disruption
- Maintain / Continue Critical & Vital Services
- Resume and Recover all Activities
Deactivate Plan Upon Business Resumption
Notify Satkeholders
COMMINCATIOIN PLAN

# Risk Assessment

## 5.1 Background

A situation that leads to a disruption in a department’s ability to deliver essential services is a risk in the context of the Government of Alberta’s BC program. Risk assessments are completed with two factors in mind: probability of occurrence, and the impact of occurrence. In addition to preventing disruptions and ensuring service continuity, a completed RA will provide:

- An understanding of risks to delivery of departmental essential services.
- Comparisons between risks of different types, thereby enabling prioritization of mitigation resources.
- Assessments of vulnerability of essential services to risk.

Risk assessment standards that may be used:

- Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management – Integrated Framework.
- ISO 31000 Risk Management Principles and Guidelines.

## 5.2 Risk Assessment Processes

### 5.2.1 Risk Assessment Considerations

Key considerations for a successful risk assessment:

- Departmental essential services are the forefront of any risk assessment process, and they must be identified prior to the commencement of the assessment.
- Participants must fully understand the chosen risk assessment method so that they can participate in the process.
- The combined knowledge of the risk assessment group may identify unforeseen risks, and they must be accounted for in the final assessment.
- Risks, once identified, may be mitigated, accepted, or ignored by the risk owner.
- The departmental executive team must approve the written report of the risk assessment.
- Risk assessments will be reviewed annually at a minimum, and will be fully conducted whenever there is a significant change in the department.

### 5.2.2 Risk Assessment Walkthrough

A sample walkthrough of a risk assessment using ISO 31000 risk management principles and guidelines follows below. The key steps are:

- Setting the risk context – Identify the departmental essential services and describe both the internal and external requirements in their delivery.
- Risk identification – Identify the specific risks that could potentially disrupt the department’s delivery of its essential services.
- Risk analysis – Determine and describe each risk in terms of its likelihood and impact.

- Risk evaluation – Compare the results of the risk analysis against risk criteria in order to determine whether a specific risk will be accepted, mitigated, or ignored.
- Risk treatment – Identification of specific actions that will be taken to lessen the likelihood of a risk occurring, the impact that the risk would have, or both.

### 5.2.3 Setting the Context

Risk cannot be assessed in a vacuum. A risk that may be critical to one department may only be incidental to another. Setting the context requires (but is not limited) to the following inputs and will deliver the following outputs:

Setting the Context - Inputs

- Essential Services - Identify departmental services and categorize as critical, vital, necessary, and desired.
- Scope – Define the scope for the risk assessment. Will it cover every business unit or will it be limited to a specific business unit?
- Information Gathering – Gather all necessary information including legislation, regulation, policies, and historical data.
- SWOT analysis tool - Evaluate the current strengths, weakness, opportunities and threats for your department.

Setting the Context - Outputs

The required output from context setting is an understanding of the broad themes of risk that your department faces. These themes include risk caused by loss of staff, loss of IT, loss of communications, etc.

### 5.2.4 Risk Identification

Specific risks are named and described under the identification process. Methods for risk identification include surveys and questionnaires, interviews, focus groups, workshops, previously approved policy documents, legislation, and historical data.

Risk Identification – Inputs

- Risk context developed in the previous step of the process.
- Essential services list.

Risk Identification – Output

- Named list of risks for your department
- Existing mitigation strategies

### 5.2.5 Risk Analysis

The objective of risk analysis is to understand risk in terms of its likelihood of the named risks occurring, and its impact on essential services.

There are many ways by which the likelihood of a risk occurring and its impact are determined, but the two most commonly used methods of analysis are quantitative analyses and qualitative analyses.

Quantitative analysis consists of comparing specific statistical values for risks. In general, this method is most used for comparing the impact of a disruption rather than likelihood, as it is possible to determine quantities from a disruption (dollars lost, Albertans not served at a data centre, facilities unavailable) whereas it is impossible to place a numeric value on the likelihood of a risk (how many floods will happen? How many pandemics will happen?).

Qualitative analysis consists of comparison based upon informed judgment of likelihood or an impact. The key requirement for qualitative analysis is that the judgment is informed; guesswork or generalities do not represent qualitative analysis.

Both qualitative and quantitative techniques are useful in determining the likelihood and impact of a risk, but neither method is superior. Quantitative analysis is more specific, but requires detailed, accurate, and consistent information for a comparison to be useful. Qualitative analysis, while less specific than the former method, is better able to describe potentialities.

Likelihood in the context of Risk Analysis is a statement that describes the chance that a specific event will happen in a specific area. It generally is expressed as a function of time, i.e. there is a 30% chance that this area will flood in the next two years. Two quantitative measures for calculating likelihood include:

Frequency – The number of times a named event occurs over a chosen timeframe in a particular location. An example would be that a building has flooded three times over the past seven years.

Probability – An expression of how expected an event can be in the future. Probability is usually expressed as a percentage. Probabilities are based upon previously recorded frequencies. For example, a 100-year flood has a 1/100 chance of occurring in any given year, or expressed as a probability of 1% or 0.01. An event that is expected to occur 3 times of the next 2 years would have a 1.5 probability each year, or a 150% chance of occurrence.

Qualitative representation of likelihood expresses the chance of occurrence through descriptive words. Each word, or phrase, will have a designated range of possibilities attached to it. A caveat to qualitative representation is that the descriptive word or phrase must be explained in the risk analysis.

Impact means the effect on the department should the risk occur. Much as with likelihood, impact can be can be expressed through qualitative expression or quantitative measurement.

One common measure of impact is to determine the damages that may be caused by the occurrence of the risk in terms of dollar amount of the likely loss. This may be estimated through historical data. This dollar value can include second- and third-order effects if known.

Not every potential impact can be quantified, and quantitative measurements may not adequately express the scope of a risk occurrence. To better express the effect of risk occurrence on Albertans, qualitative representation of impact should be incorporated into risk analysis. A loss may cost a great deal of money, but be mostly invisible to daily life; conversely, a relatively minor cost in dollars could have a great impact, such as complete loss of access to electronic records due to a power outage. As with likelihood, qualitative impact descriptors must be described to ensure consistency during the analysis.

An example of a qualitative measurement system for fatalities and injuries could be:

Impact Major Impact – Significant and lasting disruption of service to a large number of Albertans over a large area

Moderate Impact – Significant disruption of service for a short period to a moderate number of Albertans in a limited area

Minor Impact – Minor disruption of service for a short period to a limited number of Albertans in a small area

Negligible Impact – No disruption of service to Albertans, but a condition that must be remedied before normal daily operations can resume

Key considerations in analyzing risk include:

- Risk frequency.
- Predictability of risk.
- Speed of effect of risk (i.e. fire has a high speed of effect, while pandemics have a low speed).
- Duration of period between warning of risk and effect of risk occurrence.
- Duration of disruption likely to be caused by the particular risk.
- Degree of permanence of the disruption caused by the particular risk (i.e. a facility destroyed by fire has a high degree of permanence, while staff outages caused by a pandemic has a low degree of permanence).
- Existing mitigation strategies.

### 5.2.6 Risk Evaluation

Risk evaluation is the process of comparing risk levels with established criteria to determine whether a risk is acceptable or tolerable, and it assists in determining the vulnerability of an organization to the risk events

A sample categorization method for risk evaluation below:

DETERMINE RISK LEVEL FOR EACH TRHEAT

| | Vulnerability to Threat | | | |
|---|---|---|---|---|
| **Impact of Loss** | Low | Moderate | High | Very High |
| Major | 🟨 | 🟥 | 🟥 | 🟥 |
| Moderate | 🟩 | 🟨 | 🟥 | 🟥 |
| Minor | 🟩 | 🟨 | 🟨 | 🟥 |
| Negligible | 🟩 | 🟩 | 🟨 | 🟨 |

| | Risk Rating Interpretation | |
|---|---|---|
| DETERMINE ACCEPTABILITY OF RISK | 🟥 | These risks are very high. Countermeasures recommended to mitigate these risks should be implemented as soon as possible. |
| | 🟨 | These risks are moderate. Countermeasure implementation should be planned in the near future. |
| | 🟩 | These risks are low. Countermeasure implementation will enhance organization's preparedness. They are of less urgency than the above risks. |

### 5.2.7 Risk Mitigation

Risk mitigation strategies include increasing redundancy of critical systems, identifying personnel for staff augmentation / replacement, identification of alternate facilities, etc. One of the key aspects of risk mitigation are the associated costs, and in a resource-constrained environment it may not be possible to mitigate against every potential risk. The final decision to accept risks rests with the departmental executive team.

There are four primary risk management strategies: acceptance, reducing / controlling / containing the risk, transferring or sharing the risk, and avoiding the risk.

Acceptance – Risk may be accepted if the any or all of the following conditions exist:

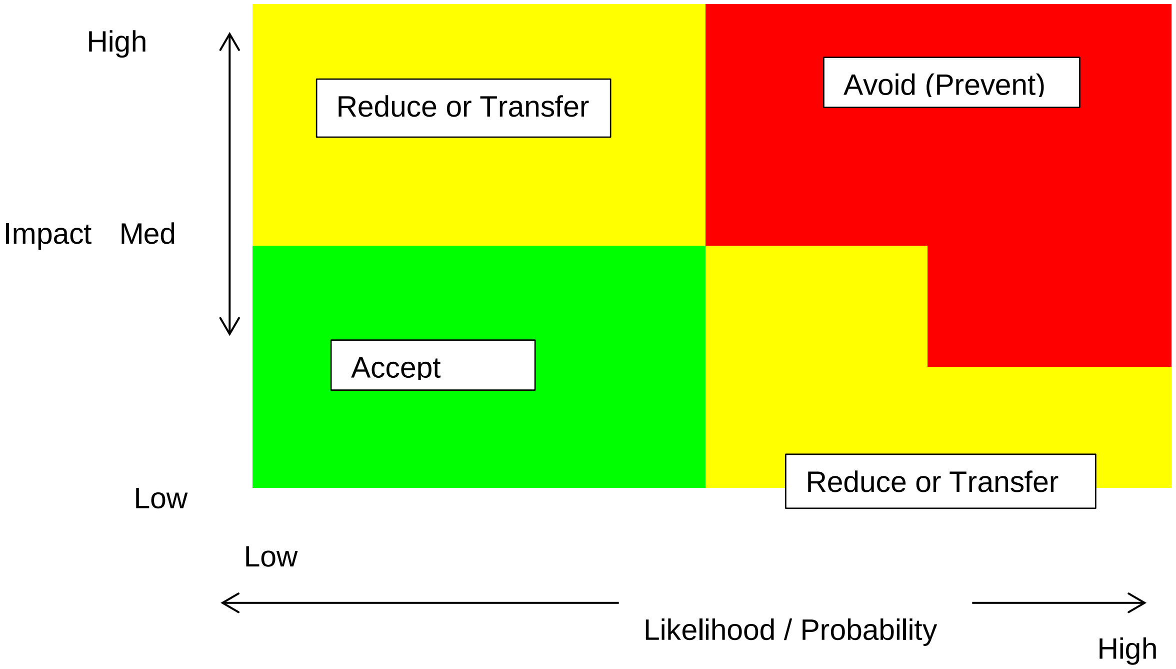
- The potential impact is minimal.
- No cost effective mitigation is possible.
- The risk is unlikely.

Reduction / controlling / containing – High probability, but low impact risks tend to fall under this strategy.

Transfer or share – For departments in the GOA, a risk may exist within the department that would be inappropriate for the department to address individually. IT service outages are an example of cross-government risk, as the GOA uses a common backbone for IT, it is necessary that there is a common response to ensure the continued ability of the GOA to communicate in a widespread event. In this example, while a specific department may face a high impact risk due to an IT outage, this risk is either transferred to the outsourced service provider or shared with other departmental IT teams.

Avoid – Risks identified as high probability and high impact must be avoided. This risk mitigation strategy is the least common, as it is the most resource-intensive. Very few risks require this type of mitigation, as the risk must be completely eliminated through redundancy.

**Figure 4 - Risk Response Matrix**



### 5.3 Summary

For a risk assessment to be useful, the assessment must be objective, detailed, and accurately reflect the impact of an event on a department. BCOs must understand that while they may be the ones preparing the assessment, the executive team and risk owners retain the authority to mitigate risks.

## Business Impact Analysis

### 6.1 Overview

A comprehensive business impact analysis is core competence in BC planning. For the GOA, a BIA is the process of analysing activities and understanding the effects that a business disruption might have upon continued provision of service, both in terms of external service provision and internal processes/functions that facilitate that service. A BIA also:

- Confirms the order in which essential services are resumed and resources required to facilitate their continuity and / or resumption.
- Predicts the consequences of function disruption and processes information needed to develop recovery strategies.
- Identifies critical job functions, business processes / functions, potential risks, and threats to continuity of business operations.
- Assists in the determination of which services can be temporarily shut down in order to focus resources on critical and vital business processes or functions.

The following basic information is necessary to complete an effective and viable BIA:

- Obtain a commitment by senior management to support the BIA and instruct all departments/divisions to assist the BCO.
- Clearly define purpose, objectives, and scope of the BIA.
- Clear, concrete language describing the BIA and business processes / functions
- Identification of business process / function owners using a current organization chart.
- Identification of dependencies and interdependencies between public facing services and internal processes and policies that support them. A critical outward facing service cannot be maintained if the software required to support it is allowed to fail.

### 6.2 Business Impact Analysis Importance

Business continuity best practices (such as ISO 23301 and the CSA Z1600) require that a BIA must be conducted to justify business continuity strategies, associated resource requirements, and interdependencies. Within the GOA, a BIA helps departments:

- Have a clear understanding on the duration of a disruption each process / service can tolerate.
- Identify the most critical functions and target time frames in which these functions must be restored or made operational.
- Identify costs and long term impacts associated with disruption to critical services. These often include financial costs, but can also include danger to health and safety, loss of infrastructure and loss of confidence in the GOA.
- Map dependencies and relationships between business processes and supporting systems

A BIA separates and delineates time critical business functions / services by differentiating those functions / services that are absolutely critical and / or vital within a short time frame following a significant business continuity disruption from those that are desired or necessary. Departments must ensure minimum standards of service are maintained throughout the disruption and appropriately prioritize functions that must be restored immediately.

This information can assist the BCO in developing recovery plans that will accurately ensure continuity of services.

## 6.3 Conducting a Business Impact Analysis

BIAs consists of:

- Project planning
- Data gathering
- Data analysis
- Documentation of findings
- Management review and approval

Fundamentally, for a BIA to be undertaken successfully, senior management must support the BIA within the wider goals and objectives of the BCM program. In communicating the goals and objectives of a BIA, BCT members should contextualize the purpose and goals for cross-departmental stakeholders who may be less familiar with emergency management and business continuity. The final BIA report should clearly present the tangible and intangible impacts of a business continuity disruption and identify critical functions which must not be allowed to lapse or that must be prioritized for restoration. Regardless of the complexity and the size of an organization, the following are the key steps to complete a comprehensive BIA for part or whole of the organization.

The required steps for a comprehensive BIA are below:

### 6.3.1 Define the Scope

The following points must be considered when defining the scope of a BIA:

- Decide if the BIA intended is for all or part of the organization. A number of factors will influence the decision, for example, size, and complexity of the organization, and / or the resources available to complete the BIA.
- Before asking business units about what is critical in the event of a business disruption, ensure there is clarity regarding BIA definitions, scope, and departmental policy.
- Define and establish benchmark criteria for criticality measurements and communicate it to business unit owners to ensure it is well understood. This ensures a consistent approach across the entire organization.
- Senior management or business unit managers are the audience at which the proposed scope and purpose of a BIA are presented. Executive participation ensures that the BIA is consistent with the organizational business plan.

### 6.3.2 Preparing the Business Impact Analysis

In preparing a BIA, the method of data collection / interviews should be chosen with organization's size, complexity, and culture in mind.

- Managers should not prioritize their business functions. Instead, questionnaires should be designed to provide the BCO the required information to prioritize business functions in comparison to the organization as a whole.
- Questionnaires should be specifically designed for each level of staff (employees, management, directors).

BIAs should focus on the key areas of the organization, sometimes referred as 5Ps.

- People – Health and safety of all persons; skills needed to perform critical functions.
- Premises – Locations of the department's key functions; means of protection of vital physical and intellectual assets owned by the organization and those assets (properties, facilities and infrastructures) owned by the other organizations upon which it is dependent.
- Processes – Those activities that generate the critical business function or service.
- Providers – Stakeholders; Communication both internal and external.
- Profile – Impacts should be assessed against people, reputation / credibility, premises, processes, environment, economic and financial, regulatory and contractual obligations and providers.

A BIA questionnaire can be quantitative, qualitative or a mixture of both: The table below shows examples for quantitative and qualitative BIA elements:

| Quantitative | Qualitative |
|---|---|
| Property loss | Human resources |
| Revenue loss | Morale |
| Fines | Confidence |
| Legal liability | Social responsibility |
| Overtime | Image |
| Additional expenses | Reputation |
| Accounts receivable | Loyalty |
| Accounts payable | Brand |

### 6.3.3 Data Collection: Scope and Methods

It is important to define the data collection scope for each business unit. The BCO must clearly identify:

- Who will be canvassed for information.
- Where the desired information is likely located.
- How reliable the information is likely to be.
- How current the information is likely to be.

There are a number of ways in which data can be collected and verified, and chosen methods must produce desired results and offer flexibility to meet your departmental needs. Appropriate methods should be matched to the information requirements and organizational capacity of each business unit. Common BIA data collection methods are:

- Questionnaires – This is a simple, cost effective written format where questions can be distributed electronically or in a paper format for manual completion. Interviewees complete questionnaires independently and with minimum support from the developer.
- Workshops / round table discussions – This method provides an opportunity to share different views and seek a common ground or consensus from interviewees. Smaller groups tend to provide more detailed and informed feedback, but can significantly increase the cost in both time and resources.
- Personal interviews – These are one to one, detailed interviews enabling extended interaction between the interviewer and the participant. The interviewer

can ask additional questions or explore other leads that may be raised by the interviewee.

- Physical inspection – Involves physically viewing the site / location being reviewed. By physically viewing the location or site or working environment, the reviewer will have an opportunity to speak directly with staff regarding their operational tasks and processes and to complete a professional assessment of environmental risks. This reduces the dependency of relying on reports generated by individuals not trained in business continuity. The risk of this method of data collection is the likelihood that the reviewer does not have intimate familiarity with the operations and processes of the business area.

### 6.3.4 Post Collection Activities

- Information obtained from a BIA interview should be recorded in a consistent way. This ensures information is acquired and tracked in a consistent manner.
- Time permitting, results should be confirmed with business unit managers.

Feedback from the interviews and questionnaires is to enable BCO / BCT to:

- Identify key business processes and functions.
- Establish requirements for business recovery.
- Determine resource interdependencies that exist both internally and externally to achieve objectives
- Determine impact on operations of a disruption.
- Develop priorities and classification of business processes and functions.
- Develop recovery time requirements.
- Determine revenue impact, operational impact, reputation / loss of confidence, legislated obligations / legal impact of disruption, life safety and infrastructure / property impact.
- Inform a management decision on Maximum Tolerable Outage (MTO) for each function

### 6.3.5 Processing Data

Integrate the data collected from all business units into a single departmental list of functions, organized by criticality. This step is required to identify those functions that must be restored quickly following a business disruption and those which can be delayed. Determining criticality can be challenging across large departments with competing priorities; use the department's core mission and business plan as the benchmark to assess criticality.

An assessment of the impact severity to Albertans if the function or service were to be stopped will determine the importance of a function or service. The GOA BCP outlines four maximum time outages thresholds for restoration of service:

- Critical – Restored within 24 hours.
- Vital – Restored within 72 hours.
- Necessary – Restored within 2 weeks.
- Desired – May be restored more than 2 weeks.

If a function or a service is dependent on other business functions, then the BCO must consider the criticality of that function in determining any downstream implications.

A thorough BIA will identify the dependencies between processes and sub-processes. This ensures that impacts of a business disruption are assessed to their logical conclusion. All dependencies are to be identified within the plan.

Resource requirements that are necessary for essential services are identified as the BIA data is reviewed. Resources are commonly separated into two categories: People and Materiel (equipment/facilities/IT requirements).

### 6.3.6 Data Control

Before preparing the final report for a BIA, it is important to conduct data moderation / control to ensure the data collected will lead to sound decisions. This can be done by:

- Assessing the validity of the operational requirements developed from the data.
- Addressing the implication of the findings by addressing the gaps between the proposed operational requirements and the department's actual recovery and continuity strategies.

The following points should be considered under a BIA data control or moderation phase:

- Comparison of the current data output with the findings of earlier BIA reviews (if available). Things to look for are substantial change to business; does the change reflect bias or opinion to arrive at the criticality. Address any major changes.
- Conduct thorough comparison across business units / divisions that perform similar processes. Major variances or inconsistencies must be addressed.
- Share the initial draft with all participating managers along with a request for their feedback or corrections.
- Comparison of BIA data with initial expectations. This may be based on prior experience in conducting BIAs.
- Resolve all possible disagreements and seek guidance from management to provide guidance if bottom up analysis fails to provide convincing results.
- Present or deliver a formal presentation of BIA report draft to peers and appropriate senior managers to discuss initial findings.

## 6.4 Final BIA Report

A BIA report is a report or statement that should present the operational requirements, structured according to the conventions used by the organization. This report is based upon the collected, analysed and moderated data. The report presents the current operational and recovery requirements of an organisation.

The BIA report shall:

- Present a brief statement on the purpose of the BIA and its context, including reference to policy, legislation and best practices.
- Describe the methods used to conduct the BIA.
- Explain the steps taken to validate and moderate the BIA data.
- Provide a clear statement of inconclusive output and how it was resolved.
- Present the essential operations / services / functions and their stoppage impacts grouped in order of criticality (MTDP).

- Highlight potential impacts that may be caused by external stakeholder failures / delays
- State the minimum resource requirements for recovery of each business unit.

### 6.5 Summary

In summary the BIA identifies the organization’s most critical business and captures the timeframe in which services and processes must be restored in the event of a business disruption. Information gathered for a BIA is designed precisely to identify the:

- Processes or functions performed by an organization.
- Resources required to support each process.
- Interdependencies between processes and/or departments.
- Impact of failing to perform a process.
- Criticality of each process.
- Maximum tolerable period of disruption (MTPD) for key products or services.

## Business Continuity Strategies

### 7.1 Overview

Business continuity strategies are professional practices within the BCM lifecycle that determine the overarching approach and methodology that will support departmental requirements in the face of a major disruption. Completed risk assessments and business impact analyses inform these strategies. BC strategies may take the following forms:

- Prevention strategies – Focused on incident prevention.
- Mitigation strategies – Focused on mitigation, limitation, or control of consequences.
- Preparedness strategies – Focused on the preparation of an effective response, and continuity & recovery management planning.
- Response strategies – Focused on the response to incidents that threaten people, property, environment, and the continuity of operations.

Continuity strategies – Focused on the continuance of critical services.

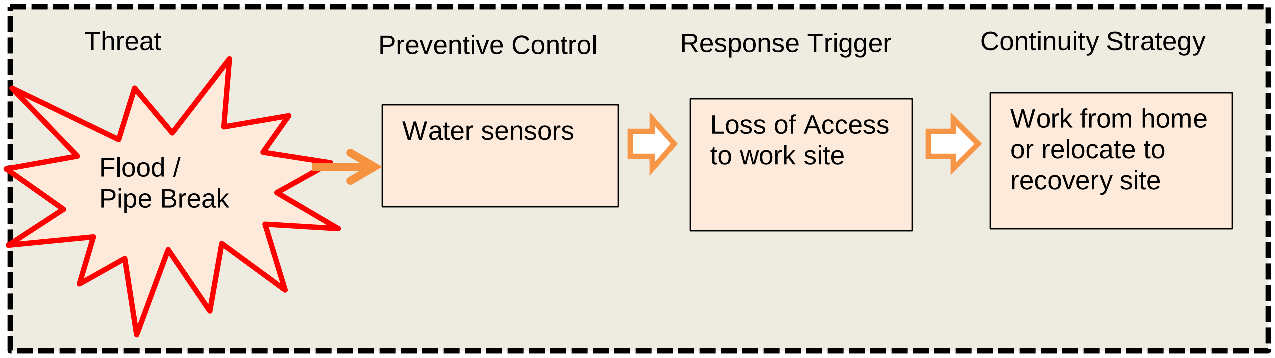
- Recovery strategies – Focus on recovering services to an acceptable level.
- Communication strategies – Focused on effective communication.
- Training and education strategies – Focused on competency-based training and education.

Effective business continuity strategies that are intended to recover each aspect of the organization's business must cover the what, where, and by whom. Factors to consider when developing strategies include:

- Capital – Balancing cost versus speed of recovery.
- Disaster recovery strategies – Recovering technology and information systems (system recovery, disaster recovery sites, work area recovery).
- Continuity strategies – Availability of resources and facilities (resource requirements) to continue critical services or activities.
- Disadvantages/advantages – To support justification for the determination and selection of the strategies for disaster recovery and business continuity.

As continuity strategy development begins, already adopted preventative measures should be identified. An example of a preventive control is water sensors in a server room ceiling that provides warning if water is detected. The table below illustrates preventive method and recovery strategy for a flood or pipe break threat.

**Figure 5 – Preventive Method and Recovery Strategy**



## 7.2 Information Gathering for Strategy Development

The methods used to gather information to design and develop BC strategies (workshops, brainstorming, meetings, surveys, emergency response plans, etc.) are the same as for those used in the development RAs or BIAs. Aspects to consider in strategy development include:

- Identify business levels or mission critical processes to ensure that participants are aware of acceptable outage times so that developed strategies will take full account of the recovery time and recovery point objectives to protect and maintain the department's services and functions.
- List all known interfaces or interdependences to avoid duplication of strategies and reduce the cost of implementing the strategies.
- Highlight the difference between disaster recovery strategies (information technology process based) and continuity strategies (basic resources and processes which enable business resumption).
- The final choice or approval of a strategy rests with senior management.

## 7.3 Approaches for Business Continuity Strategies

BCOs will identify a range of possibilities within disaster recovery and continuity. In selecting appropriate strategies (particularly with respect to alternate sites), a number of factors should be considered such as physical separation from primary site, reservation of sufficient resources, accessibility, capacity to accommodate staff, dedicated purpose for disaster recovery, availability of utilities and services.

### 7.3.1 Disaster Recovery Strategies

Disaster recovery strategies focus on recovering the technology and information systems that support services and functions within the department. The objective of disaster recovery strategies is to identify the system(s) or applications used by the department and identify methods by which the data or software will be recovered in the event of a disruption. To increase internal resilience, it is necessary to outline the systems the department uses to provide outward facing services as well as internal functions. Common disaster recovery strategies might include redundant systems, automated recovery backups, or paper files.

### 7.3.2 Business Continuity Strategies

BC strategies address all aspects of service and function recovery  less disaster recovery for IT systems. Continuity strategies include workarounds for the disrupted business process or function. Continuity strategies must be developed for each business process or function identified as critical or vital.

Common continuity strategies include:

- Identifying an alternate site or creating a reciprocal agreement with a comparable department.
- Identifying alternate suppliers for materials or service.
- Transference of staffing from non-essential functions to support essential services.
- Remote work.

- Status quo – executive team is comfortable with assumption of risk given the cost of prevention or mitigation strategies.

### 7.4 Strategy Selection Process

Similar to the decision making processes for risk and impact analyses, the executive team is the final authority for BC strategies.

Selection process for strategies must be based on:

- The contribution and opinions of all relevant levels and perspectives.
- A full understanding of the available options of each proposed strategy.
- A full understanding of the implications of each proposed strategy including cost, degree of preparedness, time for activation, etc.
- Buy-in from those who are responsible for essential services.

Strategy outcomes need to be:

- Endorsed and funded at the executive level.
- Understood and supported at the management level.
- Implemented and tested at the operational level.

### 7.5 Summary

Outlining the objectives of BC strategies is extremely important. Selected strategies must meet departmental policy and are based upon the outputs from risk and impact analyses. Follow through the selection process and involve your Executive sponsor before presenting the recommendations to the Executive to obtain approval for implementation. Once you have received final approval, prepare the continuity plans for each strategy.

## Awareness and Training

### 8.1 Overview

A successful BC program sees aware and actively engaged employees and partners that contribute to the development and implementation processes. Intra-departmental awareness increases participation and co-operation by team members when the plan is activated, they are aware that the plan exists and understand the value in compliance and engagement when the plan is activated. Awareness and staff engagement should be conducted throughout the program planning cycle.

Primary awareness and training objectives include:

- To develop and conduct BCM awareness training for all staff
- To develop and conduct crisis management team training
- To develop and conduct BC training for key appointments and business continuity team

It is recommended that the BCM team develop an annual (or even biannual) awareness and training strategy schedule to ensure regular opportunities to re-engage existing staff and meet the needs of new hires.

### 8.2 Creating Awareness

#### 8.2.1 General Staff Awareness Training

This training should be delivered to all staff and should be incorporated into an orientation for new hires. General staff training may include the following topics:

- An overview of the BCM program and why it is important to the department.
- Employee role(s) during an activation.
- Where staff can locate emergency contacts.

#### 8.2.2 Business Continuity Team Training

BCT members require more in depth training, and it should be targeted to improving member skills and increasing personal investment in the BCM process within the department. Key topics may include:

- BCM concepts, processes, policies, continuity/ recovery strategies.
- Risk and impact analysis development.
- Recovery plans documentation.
- Exercises and testing.
- Coordination with external stakeholders.

#### 8.2.3 Executive and Senior Management Training

Executive team members and senior managers require training that is tailored to providing a strategic view of how the BCM program is linked to the department’s strategic vision. Such training is also a good vehicle for getting executive level buy-in and support for the BCM program.

## Program Maintenance

### 9.1 Overview

Departments must design a cyclical maintenance program to validate effectiveness of the BCP, and ensure the plan remains relevant. As the BCT and business unit owners revise the plan, these revisions must be dated and reflected in the plan. Program maintenance and plan review should be undertaken annually, and/or under the following circumstances:

- Business objectives, processes, or risk assessments change.
- New functions, services, or technologies are introduced.
- Location(s) change.
- After an exercise, review or, audit where gaps have been identified and recommendations for improvements are made.
- After departmental re-organization.
- After changes to key supporting plans.

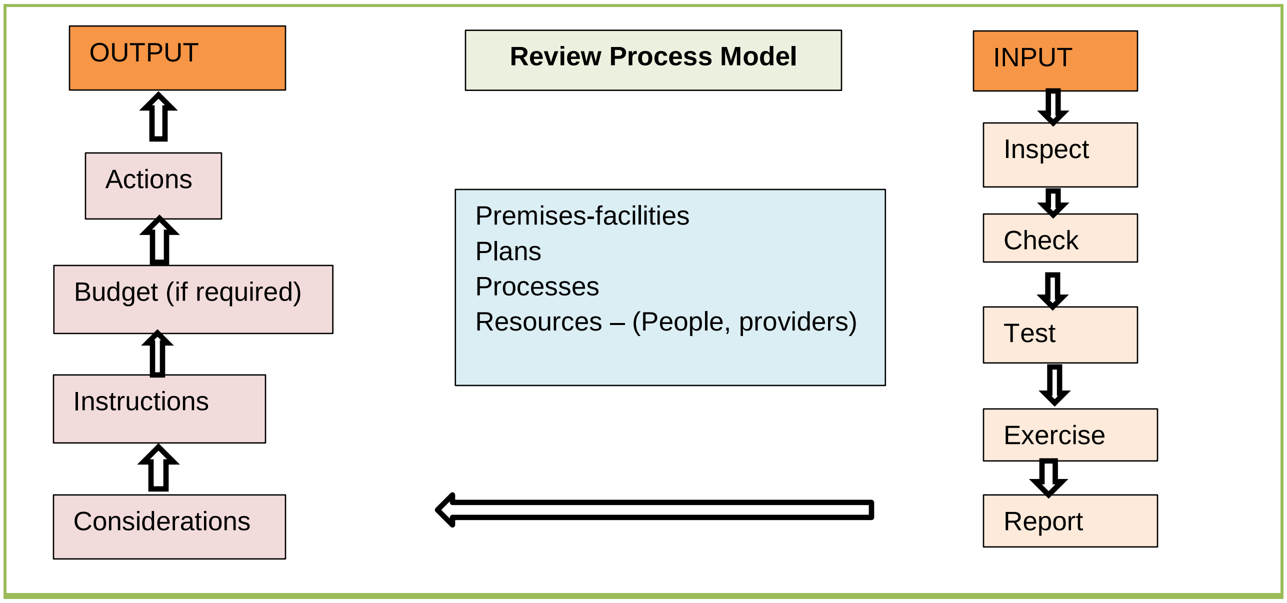
Departments should define their plan maintenance schedule at frequencies ranging from monthly to biennially, in accordance with the schedule laid down in the department's plan maintenance guidelines.

| Plan Component | Maintenance Timeframe |
|---|---|
| Departmental BCM Program | Biennial review by AEMA |
| BCM Policy | Reviewed and updated bi-annually by department |
| Business Impact Analysis and Business Continuity Strategies | Reviewed and updated annually after any significant business change |
| Risk Assessment | After a significant change within your department or the GOA |
| Business Continuity Plan | Reviewed and updated annually after any significant business change |
| Contact Lists (employees, stakeholders, BCT) | Reviewed and updated quarterly, or after a change of personnel |
| Emergency Response Operations and Contingency | Reviewed and updated annually after any significant business change |
| Awareness and Training | As required |

### 9.2 Review Process

Plan review is an internal quality control process which assesses the effectiveness of an extant plan by the judgment of those who are directly involved in business continuity planning activities. The key components of a review are people, premises, processes, providers, and plans. Internal review consists of two processes, input and output as shown in the figure below. Information is gathered by inspecting, checking, testing, and compiling a report. Output consists of implementation of any changes directed by the Executive Team after reviewing the final report generated by the input cycle. Plan review is solely concerned with the BCP; it does not cover BCM policy or budget.

**Figure 6 – The Review Process**



### 9.3 Audit Process

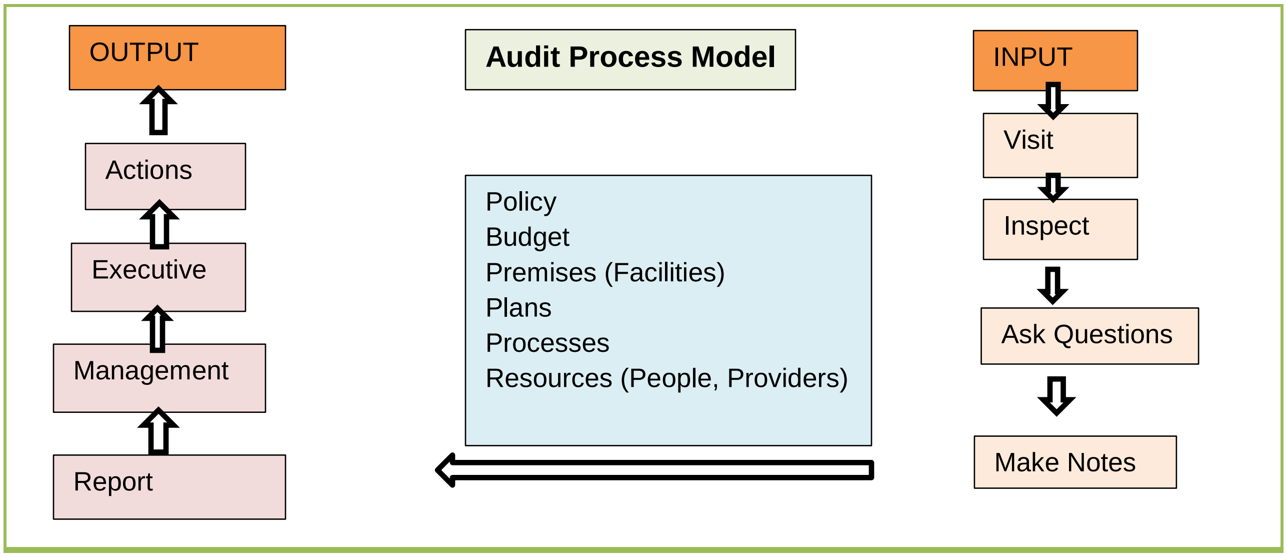
Auditing is a review process carried out by an external agency, and is designed to assess compliance with policy, legislation and regulation. An external audit is separate from the departmental BCM program, and provides an objective viewpoint. A standard audit of a BCM program will review the entire business continuity life cycle, including:

- Strategy – Holistic view of the management process, overall BC strategy, budget, policy and executive decision making.
- Analysis – Risk and impact analyses.
- Implementation.
- Test.
- Maintenance.

A BCM Audit is comprised primarily by inspection and investigation, and answers specific questions from the auditor's terms of reference. Typical audit requirements include:

- Validation of compliance to policy and legislation.
- Review department's continuity management solutions, including budget.
- Validation of departmental BCPs.
- Verification of appropriate exercise and maintenance activities.
- Highlighting deficiencies and issues.

**Figure 7 – The Audit Process**



## Exercising and Testing

### 10.1 Overview

Exercising and testing procedures are a critical element of a complete BCM, and their completion ensures that the BCP can achieve the department’s BC objectives. A test is type of activity whose aim is to obtain an expected, measurable pass / fail outcome within the structure of the planned activity. Tests are often applied to supporting plans, or focus on a specific component of the plan. Exercises, by contrast, are activities consisting of full execution of plan with a view to identifying strengths and weaknesses of the complete plan. Exercises can help:

- Validate policies, plans, procedures, training, equipment, agreements.
- Clarify and train personnel in roles and responsibilities.
- Improve intra-departmental and cross-government coordination communications.
- Identify gaps in resources.
- Improving individual performance and identifying opportunities for improvement.
- Provide a controlled opportunity to practice improvisation.

### 10.2 Exercise Types and Methods

Business Continuity Exercise (BCX) Types include:

Component – Only a single process or component of the plan is exercised. It is less formal and may be conducted more frequently. An example of this is the activation of a call out tree list.

Integrated – A number of inter-related components are exercised concurrently to validate that they can work together to complete the required objective. An example of this is a call out tree test combined with mobilisation of staff to commerce operations at the alternate site.

Full – A full exercise consists of executing all components of the business continuity plan.

Exercise methods include:

#### 10.2.1 Walkthrough Business Continuity Exercise

The primary objective of a walkthrough BCX is to ensure that critical personnel from all areas are familiar with the BCP. An example of a walkthrough BCX is a meeting of the business continuity team members to verbally go through the BCP and discuss how they would handle an incident based on the plan. This enables the BCT to identify gaps or other weaknesses.

#### 10.2.2 Table Top Business Continuity Exercise

This method involves presenting a predefined scenario to which the participants will respond with simulated actions as the BCP is applied through each step of the scenario. Such exercises are primarily targeted at the business continuity team to help foster team interaction and improve decision-making, and to validate specific response capability. Table top BCXs include the following:

- Practice and validation of specific functional response capabilities.
- Demonstration of knowledge and skills, while improving team interaction and decision-making capabilities.

- Mobilization of all or some of the business continuity team, crisis management teams or recovery teams to practice proper coordination.

### 10.2.3 Simulation Business Continuity Exercise

Business continuity teams may also execute BC activities in a simulated environment under conditions that would exist in the event of actual plan activation. This method of exercise involves complete mobilization of personnel in an attempt to establish communications and coordination as described in the BCP. It includes:

- Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning.
- Actual or simulated response to alternate locations or facilities using actual communications capabilities.
- Mobilization of personnel and resources at varied geographical sites.
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization.

## 10.3 Lessons Learned

Lessons learned reviews validate existing policies and procedures, and amend and improve gaps and oversights for the future. The review may from the experiences of key participants, supporting staff and contracted service provides who were involved in responding to the disruptive event or to the exercise. Reviews must focus on the BC system and not the individuals fulfilling the roles. Once the lessons learned are developed, they should then be tested against overarching policy, legislation, and regulation, and then disseminated into current BC practice.