Business Continuity Guide

September 2014

This Guide is primarily intended for use by
Government of Alberta Departments, Agencies,
Boards, and Commissions.

Contents

Business Continuity Management

About this section

1. Introduction
   1.1. Executive Summary
   1.2. Introduction to GOA Business Continuity Management (BCM)
   1.3. Authority and Legislation
   1.4. Guiding Principles
   1.5. Business Continuity Standards and Best Practices

1 Introduction

1.1 Executive Summary

When a significant event causes disruption to the provision of essential services to Albertans, the Government of Alberta (GOA) will activate the GOA Business Continuity Plan (BCP) in order to recover and return to normal operations. 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 impact their operations.

This guide is intended to assist Business Continuity Officers (BCOs) and their Business Continuity Teams through the process of business continuity planning and management. This guide provides an overview of current best practices targeted at GOA departments, and while extensive, may not cover unique departmental requirements. Users are encouraged to seek additional information beyond the scope of this guide to meet the demands of their departments. Similarly, while many of the lessons and components in this guide may apply to community business continuity, those users should ensure fit and applicability for their specific requirements. Additional information and assistance for GOA departmental Business Continuity Teams is available from the Business Continuity Planning Section of AEMA.

1.2 Introduction to 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 addressing business continuity; specifically, restoring and maintaining essential services. Through a comprehensive BC Program, underpinned by a comprehensive BCP, departments will be better 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 BC Program will:

- Ensure provision of essential services to all Albertans;
- Ensure and maintain confidence in government;
- Minimize potential revenue loss; and
- 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 assign 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; accountability for business continuity planning within each department is retained by the Deputy Head of the department (typically a Deputy Minister).

1.4 Guiding Principles

This guide is intended to provide a frame of reference for BCOs to develop, maintain and improve their departmental BC 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. Where templates have been provided, users are encouraged to modify them to meet their needs.

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 BC community, ISO 22301:2012 serves as the comprehensive standard for business continuity professionals to benchmark against in developing and enhancing their BC Programs. AEMA employs ISO 22301:2012 and Canada's CSA Z1600 in administering the GOA BC Program. The CSA, as a Canadian standard, is viewed by AEMA as the prime standard against which GOA programs are measured. While neither of these standards has been formally adopted by the GOA, these standards have been considered in developing this Guide and will be used on an ongoing basis to inform best practices for the GOA.

Program Creation and Management

About this Section

2. Program Creation and Management
   2.1. What is a BC Program?
   2.2. BCM Scope

2 Business Continuity Program Creation and Management

2.1 What is a Business Continuity Program?

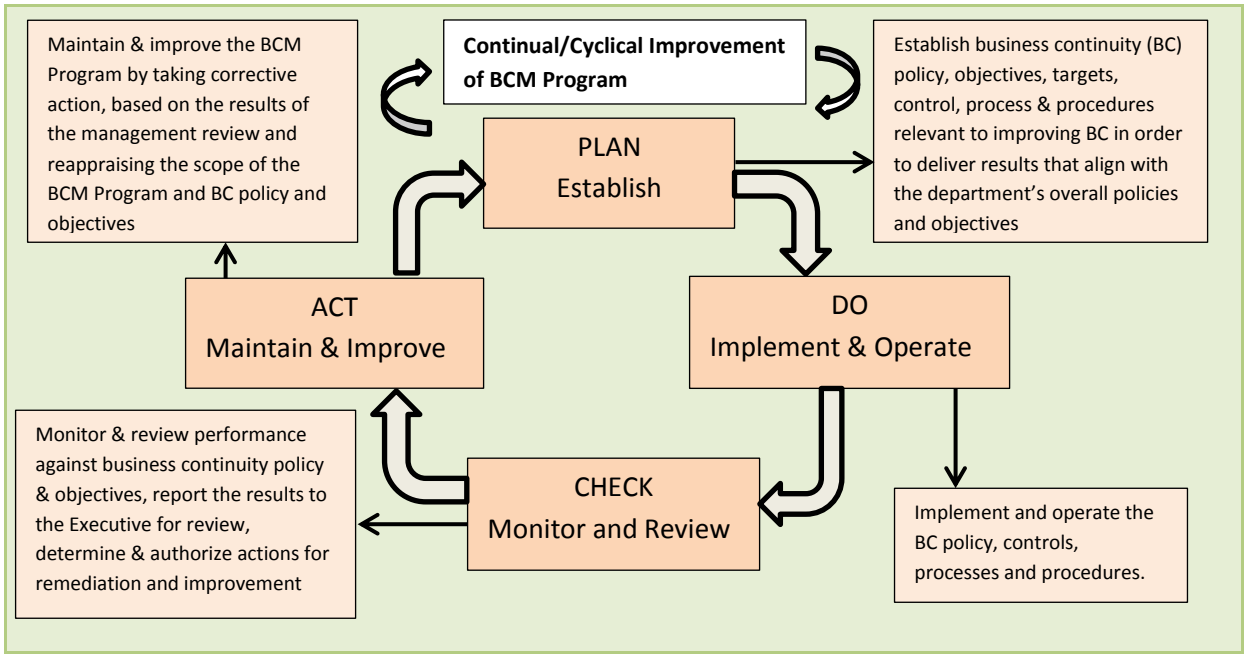
At its core, BC is focused on minimizing preventable disruptions to the essential programs and services offered by a government, an industry, or a business, and when preventing service gaps is no longer an option, business continuity describes processes and practices to restore and resume business as efficiently as possible. Within the GOA, BC refers to both the protecting of outward services provided to Albertans as well as to the internal processes that support those services. For example, it is insufficient to say that the GOA prioritizes providing 'essential service X' without also committing to maintaining the software, IT systems and staff resources (for example) required to deliver that service.

The central document of a BC Program is the BCP. The BCP is a plan that 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 parent department. Like any good plan, especially within government, it is flexible and readily adapted to each departmental reorganization. It cannot be a stagnant document that sits quietly on a shelf without regular review; the BCP must prompt regular discussion and debate around ensuring that the departmental mission, goals and objectives can be achieved regardless of external disruptions. 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 Business Continuity Management (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 (as described in this guide); awareness and training for the department on the BCP; activation and execution of the BCP as required; and amendments and improvements to BC matters on a regular basis.

An effective BCM Program will involve participation of various disciplines that need to be coordinated throughout the BCM life cycle. 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 a BCM program involves a Plan, Do, Check and Act model as illustrated in Figure 1 below.

Figure 1 – Cyclical / Continual Improvement of BCM Program



2.2 BCM Program Scope

Clearly defining the scope of the BCM Program allows the Business Continuity Team (BCT) to specifically 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 which can reduce concerns that a BCT will encroach upon or impede existing program authorities or priorities. Finally, by defining what is outside of the scope of the BCM Program, a BCT ensures that the resulting BCP will not be a document that is too large or unwieldy to be accessible to staff.

Business Continuity Plan Development

About this section

3 Business Continuity Plan Development

3.1 Overview and Plan Development Objectives

A BCP provides guidance for sustaining essential services during a disruption, and procedures for recovering those functions that are disrupted.

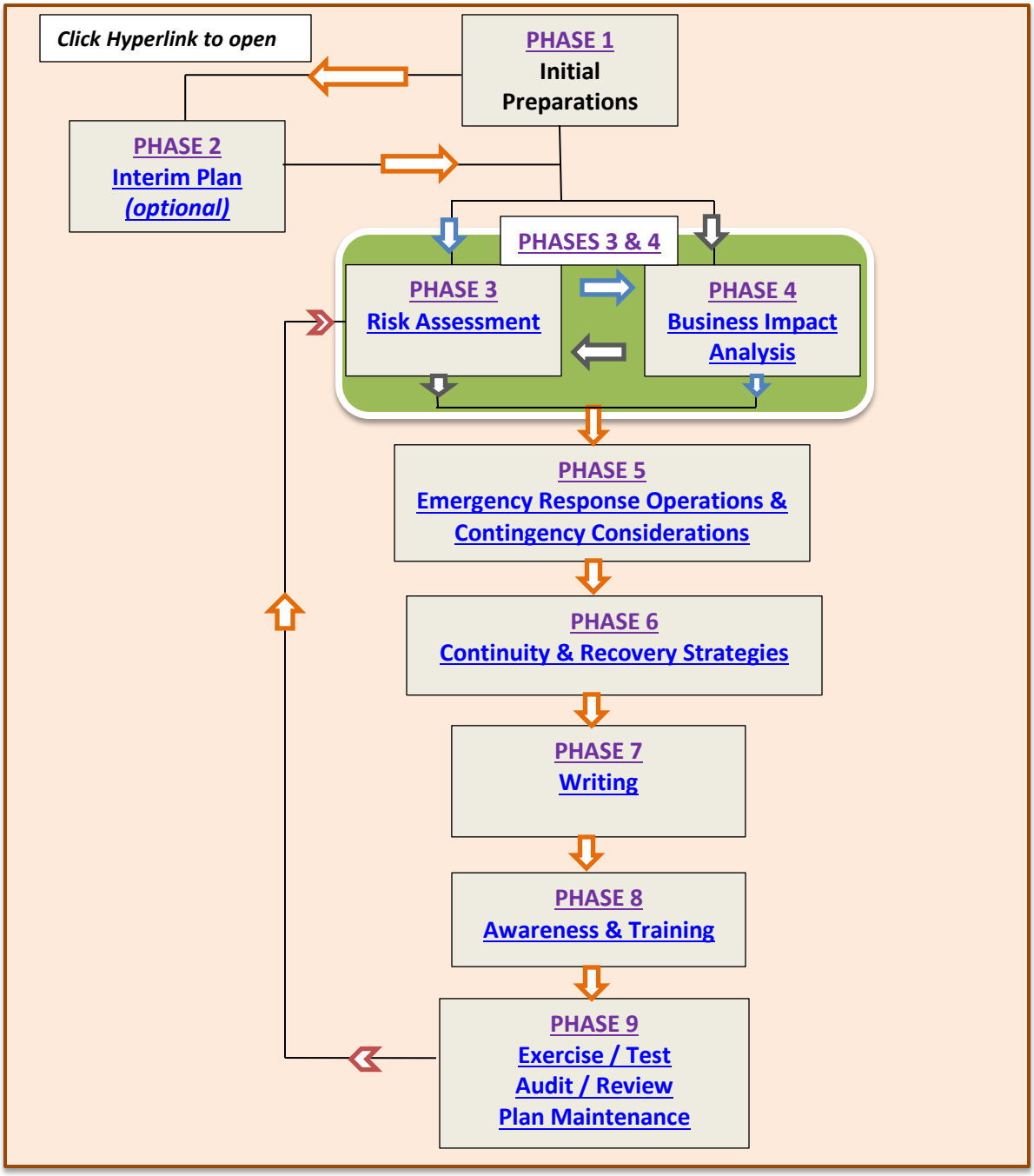
Plan Development Objectives are to:

- 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; and
- Understand the process, design framework, structure and contents of the BCP.

3.2 Planning Steps / Development Process

Developing a plan is a deliberate 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 suggested guideposts 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 – Phases of BCP Development



3.2.1 Phase 1 - Initial Preparation

As with any major policy, program, or plan development sequence, there are a number of key considerations which must be addressed before commencing a deliberate process to create a BCP. The following list of common considerations is not exhaustive; individual departments may have unique considerations to address as part of their initial preparation:

- Management Engagement
  - Identify the right level of management to sponsor the BC Program. In the GOA this decision is the responsibility of each department deputy head;
  - Ensure management understands what the BCP will encompass, when it would be used, and what are its intended outcomes; and
  - Be open about the resources necessary to support the program and complete the BCP, and confirm that these resources will be available throughout the development of the plan.
- Research and consider legislation, industry regulations, and any other directives or policies that guide or impact the department;
- Secure team member participation and commitment; and
- Define the scope of your BCP.

Involve Executive Management in the following:

- Assignment of a project sponsor to take ownership for the BCP project. He or she is responsible for ensuring that:
  - Support for the planning project from all senior managers is obtained and maintained;
  - Planning activity is completed on schedule; and
  - Department wide awareness of the BCP project and the completed BCP.
- Objectives and scope for the project are approved
- A BCO is formally appointed to:
  - Organize and supervise project planning, development and review;
  - Organize and supervise the planning process, the creation of the BCP and its testing, training and ongoing maintenance; and
  - Provide regular progress reports to the project sponsor

3.2.2 Phase 2 - Interim Plan *(optional)*

To develop a comprehensive BCP takes time. Disasters can happen at any time prior to completion of a thorough BCP. 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 that are regarded as particularly at risk or vulnerable. An Interim Plan will normally be developed independently by the members of the BCT, whereas the development of the full BCP will require wide stakeholder engagement.

Key Things to Consider when Devising an Interim Plan are:

- Notify management about the Interim Plan Structure and Roles;
- Appointment of a BCT (if not already done) to develop the Interim Plan;
- Establish a procedure for convening the BCT;
- Identify basic recovery requirements and practical recovery strategies; and
- Ensure that the Executive Team is fully aware of, and approves the Interim Plan once completed.

Phase 3 and 4 – Risk Assessment and Business Impact Analysis

There is no clear industry consensus on whether you should conduct your Business Impact Analysis (BIA) or your Risk Assessment first. Each BCO must weigh the needs and vulnerabilities of the department to determine in which order to complete the BIA and the Risk Assessment; they can also be completed concurrently.

3.2.3 Phase 3 - Risk Assessment

Risk Assessment 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 Risk Assessment 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.

For detailed information on *Risk Assessment*, click the hyperlink

3.2.4 Phase 4 - Business Impact Analysis

The 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 BCT will then assess the effect on the department should one of the business units be unable to execute their duties.

This enables the BCT to prioritize the services and resources necessary to maintain (or restore) the essential business units in the event of a disruption.

For detailed Information on *Business Impact Analysis Section*, click the hyperlink.

3.2.5 Phase 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 (ERPs) 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.

For detailed information on *Emergency Procedures Section*, click the hyperlink.

3.2.6 Phase 6 - Disaster Recovery and Continuity Strategies

Disaster Recovery Strategies are specifically concerned with recovering the information and technology (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.

For detailed information on *Business Continuity Strategies*, click the hyperlink.

3.2.7 Phase 7 - Writing

This phase identifies the key people who will draft, review, and produce the actual BCP. This team determines the structure and contents for the BCP.

REMEMBER *- The people who will execute the plan should participate in the development of the plan. This is to ensure that inputs to the plans are provided by the appropriate subject matter experts and that you do not end up with an impractical plan.*

3.2.8 Phase 8 - Awareness and Training

This section details the mechanisms by which the department will be made aware of the BC Program, the BCP, and their roles in supporting departmental BC. It also serves to outline the specific training requirements necessary for executing specific response and recovery activities. A comprehensive Awareness and Training program ensures that all members of the department will be able to work together effectively.

For detailed information on *Awareness and Training* click the hyperlink.

3.2.9 Phase 9 – Plan Review, Test, Exercise, Audit and Maintenance

BCPs are not static; they must evolve as the department changes. Thus, whenever there is a significant change in a department (new staffing levels, new technology, change in organization or organizational responsibilities), the current BCP should be reviewed by the BCT to ensure its relevance and effectiveness. 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 until the next formal revision.

Auditing and review are terms that are sometimes used interchangeably. In this Guide, an audit is conducted by an individual or body that is external to the BCP development, and measures the plan against an empirical standard, typically legislation or formally adopted policies. A review is a less formal assessment which can be conducted internally or by an external partner. For example, the GOA Corporate Internal Audit Services may audit a BCP against current Alberta legislation; whereas a BCO may review their BCP after a departmental reorganization to ensure communication pathways are still relevant and intact.

For detailed information on *Exercise and Testing*; *and* *Program Maintenance* click the hyperlink.

3.3 Structure and Content of the Business Continuity Plan

A BCP must 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. However, there are some commonalities between all effective BCPs.

3.3.1 Cover Page, Contents and Layout

Cover page and Executive Foreword

The cover page must clearly display the effective date, confidentiality restrictions (if any), and any legal disclaimers. An Executive Foreword drafted by the senior member of the BCT is also required to signify Executive approval and support of the plan. This Executive Foreword will be signed by the deputy head of the department.

3.3.2 Section 1 – Business Continuity Program

Introduction

The introduction outlines the BCM 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 Program Policy

This section describes the departmental policy underlying the Business Continuity Management (BCM) Program. At a minimum, it will include:

- Applicable legislation, regulation, and governance framework;
- The department's specific policy statement regarding Business Continuity;
- The specific objective of the BCM Program;
- The scope of the department's BCM Program;
- The assumptions underlying the BCM Program; and
- 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. This enables a clear understanding of the interdependence of the business units, and the services they provide both internally to the department and the GOA, and externally to 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 Business Continuity Officer(s), and representatives from each Business Unit.

3.3.3 Section 2 – 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 Centres (EOCs) or alternate sites.

Facility Response Procedures (May be included; not specifically part of the BCP)

Many business disruptions result from damage or loss of the facility within which the business occurs due to physical damage (fire, flooding, severe weather etc). The departmental BCP ***may*** (but is not required to) describe the procedures that will be followed in the event of damage or loss of the facility while it is occupied. If these procedures are included, they should (at a minimum) include the procedures by which evacuation of the facility will be conducted, how staff will be accounted for, and how the emergency at the facility will be mitigated. This detail is required to be described in the Facility Emergency Response Plan (FERP), a separate document that connects to the BCP.

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 duration they can be disrupted. This enables prioritization of resources and recovery efforts. This list will include those resources that are necessary for performing the essential service. The Essential Services List is the cornerstone upon which the rest of the BCP is built.

Contact Information

This section includes ***current*** contact information for those personnel identified as essential within the BCP. At a minimum it must include e-mail addresses and telephone numbers for both working hours and after-working hours. Each person identified on this list must also have a designated alternate who must provide the same contact information.

3.3.4 Section 3 – Business Impact Analysis and Risk Assessment

While not a specific element of the BCP, the Business Impact Analysis (BIA) and Risk Assessment (RA) should be included. BIAs and RAs are key elements required to build a BCP that is both realistic and effective. While the background documentation from these two activities is not specifically required to be contained in the BCP itself, doing so is highly recommended as a means of aiding understanding of the complete context of the overall Plan.

3.3.5 Section 4 – 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 Section 5 – 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 Section 6 – 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. For example, a departmental-specific glossary would generally be included as an Annex, while emergency response plans from the municipality in which the department is located could be an attachment.

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. Once the Executive team (including the deputy head) has approved the plan, it is distributed across the department. Generally it is preferred that only limited numbers of hard copies are provided, as version control becomes problematic as the plan is updated.

3.5 Summary

BCPs 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.

Preparation of an effective BCP is an art form. The temptation to include every possible detail in a BCP must be resisted; a plan that attempts to provide for every possible eventuality spreads itself so thin that it prepares for none. Instead, BCOs must identify the crucial elements that make their department an effective element of the GOA and prepare plans to minimize the impact of a disruption and recover from a disruption in the shortest time possible. If the BCP provides a clear set of processes, protocols, and procedures adaptable to any disruption, regardless of the actual mechanism of disruption, it will serve its intended purpose.

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

Plan Activation and Management

About this section

4. Plan Activation and Incident Management
   - 4.1. Overview
   - 4.2. Management and Control
     - 4.2.1. Executive Team
     - 4.2.2. Management Team
     - 4.2.3. Operational/Response Team
   - 4.3. Emergency Operations Centre (EOC) Location
   - 4.4. Emergency Procedures
     - 4.4.1. Facility Emergency Response Plan (FERP) and BCP
     - 4.4.2. Building Evacuation
   - 4.5. Plan Activation Procedures and Operations
     - 4.5.1. Level of Response
     - 4.5.2. Escalation and Control
     - 4.5.3. Activation Processes
     - 4.5.4. Escalation Process
     - 4.5.5. De-escalation Processes
   - 4.6. Communication Plan
   - 4.7. Plan Activation Process Flowchart

4 Plan Activation and Incident Management

4.1 Overview

This section describes the normal process by which a business disruption is identified and communicated, how the initial impact assessment is performed, 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 and control;
- Incident detection and reporting;
- Alerting and notification;
- BCP activation and deactivation;
- Emergency Operations Centre activation;
- Impact and damage assessment (coordinated with emergency response plan) and situation analysis; and
- 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

Executive Team is responsible for decision-making and directing crisis communication for significant business disruption. 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. Executive Teams are generally comprised of Executive Directors, Assistant Deputy Ministers, and Deputy Ministers (or their equivalents).

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. The Management Team may receive delegated authority to activate the BCP. 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. Management Teams are generally comprised of Managers and Directors (or their equivalents).

Specific responsibilities of the Management team may include:

- Assessing preliminary impacts with support from the BCT;
- Provision of regular reports to the Executive Team on the current status of the incident (when activated) or status of the program (regular business cycle);
- Developing action plans during an activation for Executive approval;
- Execution and supervision of Executive Team direction;
- Supervision of the execution of the BCP; and
- 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 location or alternate locations. The Operational / Response Team reports directly to the Management Team. The Response Teams may be broken into sub-teams, each with their own leader to facilitate the recovery effort.

Specific responsibilities of the Operations / Response team include:

- Execution of the business recovery procedures for their area of responsibilities in the order of priority identified in the BCP;
- Communication of the status of recovery to the Management Team as needed;
- Identification of issues or problems that must escalated to the Management Team for resolution;
- Establishment of shifts for Recovery Team members to support the recovery effort;
- Establishment of liaison with alternate site personnel if needed; and
- Identification of resources needed for recovery operations.

4.3 Emergency Operations Centre (EOC) Location

The EOC is the centre from which overall direction and control, coordination and resource support will be provided to the Management Team to resolve a disruptive incident. EOCs can be activated in response to Consequence Management events as well as to Business Continuity disruptions. When developing an EOC plan,

consideration should be given to communication systems, facility security, and equipment needed during the BCP activation.

4.4 Emergency Procedures

4.4.1 Facility Emergency Response Plan (FERP) and BCP.

The Facility Emergency Response Plan (FERP) is a plan to respond to an emergency event that has impacted a specific facility/building. 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. To ensure facility events are reported, it is advisable to establish a relationship between the FERP and BCP. Note that this relationship does not mean that FERP is part of the BCP; it merely means that the two are connected.

4.4.2 Building Evacuation

Emergency response procedures should be detailed in the FERP. All building evacuation or shelter-in-place processes must also be detailed in the FERP.

4.5 Plan Activation Procedures and Operations

4.5.1 Level of Response

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. For example, if a disruption is considered minor, it may solely require monitoring, but if the disruption is considered major or extreme, activation of the BCP would be required. See activation process flowchart.

4.5.2 Escalation and Control

Notification

A BCP must clearly define notification processes for both:

- **Detection of Potential Disruption** – A disruption is likely or predicted to occur; and
- **Declaration of Disruption** – A disruption has occurred and is impacting essential services.

4.5.3 Escalation Process

A BCP must clearly describe:

- EOC activation and the methods by which the BCT will be convened;
- Executive and Management Team notification procedures;
- External Partner notification procedures;
- Staff notification procedures;
- BCP implementing instructions (roles and responsibilities, locations etc); and
- Impact Assessment Criteria, including triggers for escalation.

4.5.4 De-escalation Processes

A BCP must clearly describe:

- Triggers by which response activities can be reduced;
- The process to deactivate the BCP; and
- Procedures for demobilization and resumption of normal operations.

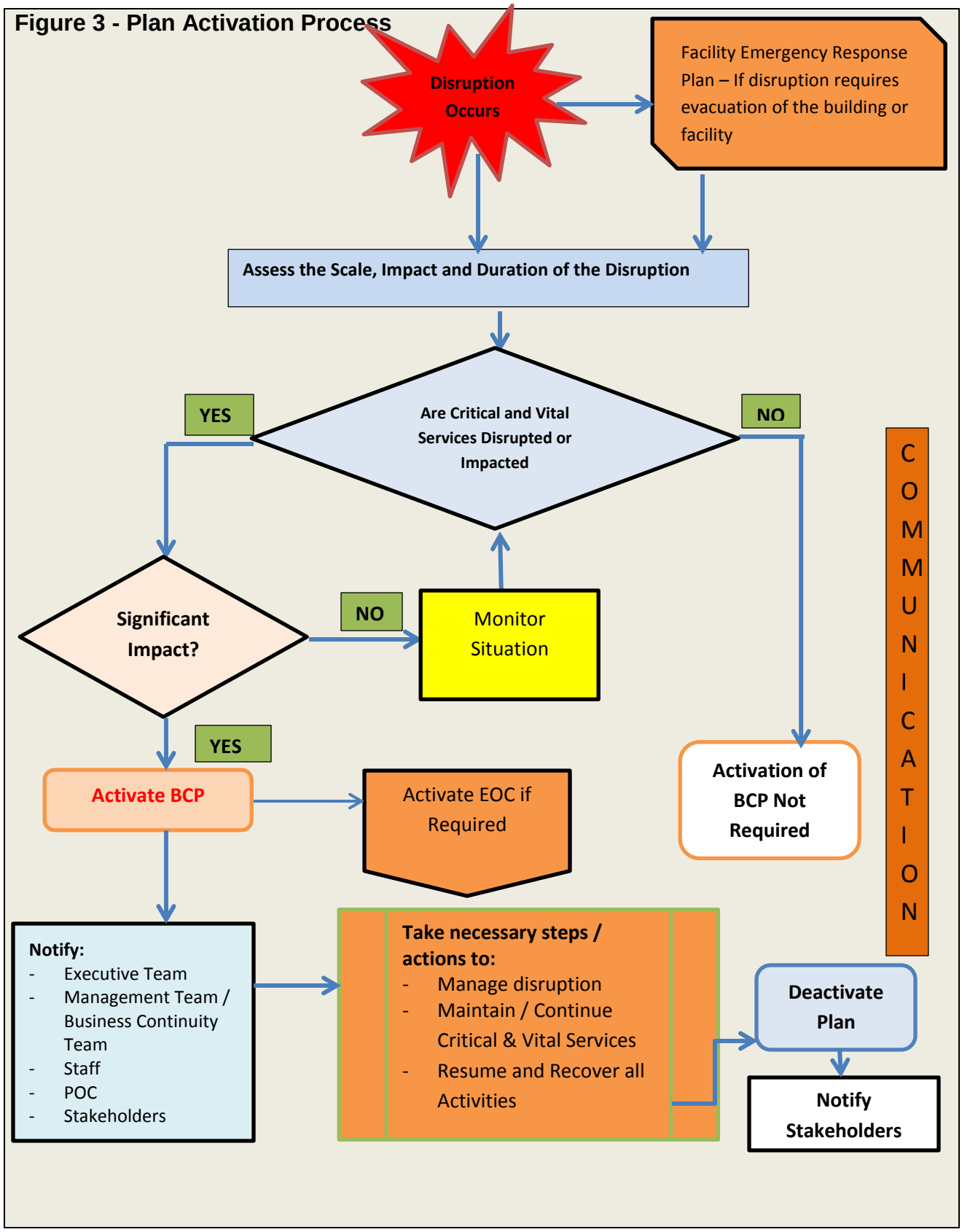
4.6 Communication Plan

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; and
- Draft key messages for external partners who may be affected by the disruption.

Figure 3 – Plan Activation Process Flowchart (Next Page)

Figure 3 - Plan Activation Process



Risk Assessment

About this section

5 Risk Assessment

Merriam-Webster defines risk as "*the possibility that something bad or unpleasant (such as an injury or a loss) will happen*". This definition should be kept in mind throughout this section.

5.1 Key Terms

Risk (in the context of BC) – effect of uncertainty on objectives with a resulting effect that is a positive or negative deviation from what is expected.

Risk Assessment – overall process of risk identification, risk analysis and risk evaluation.

Risk Owner – person or entity with the responsibility and authority to manage a risk.

Risk Identification – process of finding, recognizing and describing risks.

Risk Analysis – process to comprehend the nature of a specific risk and to determine the level of risk.

Likelihood - chance of something happening.

Asset – anything of value to the department. Assets can be tangible (such as a building) or intangible (such as reputation).

Quantitative Assessment – an assessment method through which statistical values are assigned to specific risks for comparison.

Qualitative Assessment – an assessment method that assigns non-statistical values to risks. This assessment produces narrative, descriptive or comparative information about risks.

Probability – a measure of the chance of an event or incident happening.

Frequency – the number of occurrences of an event in a defined period of time.

5.2 Risk Assessment in Business Continuity Planning - Background

Risk in the GOA BC Program may be defined as a situation that leads to a disruption in a department's ability to deliver essential services. Thus, risk is a factor that must be carefully managed to ensure that the GOA is able to sustain operations and deliver services to Albertans at all times.

In order to properly mitigate risk, it first must be thoroughly assessed against two factors: probability, or the chance that the particular risk will disrupt essential service delivery; and impact, the degree of disruption that would be caused if the risk occurred.

An example of the difference between likelihood and impact of a specific risk is that a disruption of essential services due to key staff absenteeism as a result of an influenza pandemic may be classed as ***likely*** during flu season, but that the ***impact*** of staff absenteeism due to influenza may be minor if the department is closed for holidays and would not be providing services anyway.

To prevent disruption and ensure continuity of service, the threats or risks to the essential services must be identified through a robust Risk Assessment (RA) process.

RA and Business Impact Analysis (BIA) are the foundation of effective business continuity planning, but the two processes are often confused. RA consists of identification and analysis of specific risks that may affect a department's ability to deliver essential services to Albertans. Conversely, BIA consists of identification and analysis of those business processes / activities (including required resources) that are needed to deliver those essential services, and the effect of disruption upon them.

Which Comes First? Risk Assessment or Business Impact Analysis.
Business continuity practitioners have debated whether Risk Assessment is necessary to complete an effective BIA. Some have argued that Risk Assessment is not necessary to complete a BIA, because business continuity is about minimizing the consequences of a disruption. While this may be true, limitations on resources means that not every risk can be mitigated, and thus within the context of the GOA, a Risk Assessment is necessary in order to focus effort.

5.3 Risk Assessment vs Business Impact Analysis

BIA is discussed in greater detail later in this guide. However, the table below provides some key distinctions between RA and BIA in relation to business continuity.

Key Points – RA versus BIA

What RA does

- Provides understanding of risks to delivery of departmental essential services
- Permits comparison between risks of different types, thereby enabling prioritization of mitigation resources
- Enables assessment of vulnerability of essential services to risk

What BIA does

- Provides understanding of business processes / activities
- Ranks services based upon their criticality to resumption of normal operations
- Provides understanding of the impact of disruption, which enables assignment of recovery objectives and prioritization

5.4 Objectives of Risk Assessment

- Identify the various threats to departmental delivery of essential services;
- Assess departmental vulnerability to each threat and the potential exposure should the risk occur; and
- Review controls presently in place to mitigate or reduce risks, and ensure that business unit owners understand those risks and decide to accept, prevent or manage them.

The Disaster Recovery Institute and British Continuity Institute have identified the basic competencies needed to successfully complete risk evaluation and control as:

- Understand the threats, loss potential, and vulnerability.
- Evaluate risk analysis tools and techniques.
- Define a risk evaluation strategy.
- Select a process to evaluate risk.
- Establish risk mitigation measures to prevent or minimize the effect.

5.5 Risk Assessment Process

5.5.1 Choosing RA Framework

There are a number of methodologies / techniques ranging from simple to complex (CSA Z1600- 2008) that BCOs can employ to complete their departmental RA.

> Some commonly used tools for Enterprise Risk Management (ERM) are:
> - ISO 31000 Risk Management Principles and Guidelines.
> - Committee of Sponsoring Organizations (COSO) ERM – Integrated Framework.
> - Australia/New Zealand Standard (ASS/NZS 4360:2004) Risk Management.

Each BCO must complete their RA with whichever tool is most appropriate for their department, and with which they feel comfortable. While there is no GOA-specifically mandated RA tool, the GOA does require every department to have an ERM process, and has recommended ISO 31000:2009[1] as a framework for enterprise wide risk management.

> When choosing the framework for your RA, it is appropriate to consider the framework that has been adopted by your ERM unit or branch.

5.5.2 Risk Assessment Considerations

The following are some of the key considerations for a successful RA, regardless of the chosen methodology:

- An effective RA process is dependent upon having the right people participating in the process;
- RA must be conducted with the department's essential services at the forefront;
- Participants must fully understand the chosen RA method so that they can participate in the process;
- Unforeseen risks may be identified as a result of the combined knowledge of the RA group. These new risks must be accounted for in the final assessment;
- Risks can only be managed once they have been identified and assessed;
- Essential services must be identified prior to commencing the RA;
- Risks, once identified, may be mitigated, accepted, or ignored. This decision will come from the risk owner;
- A written report of the RA must be compiled and approved by the department Executive Team; and

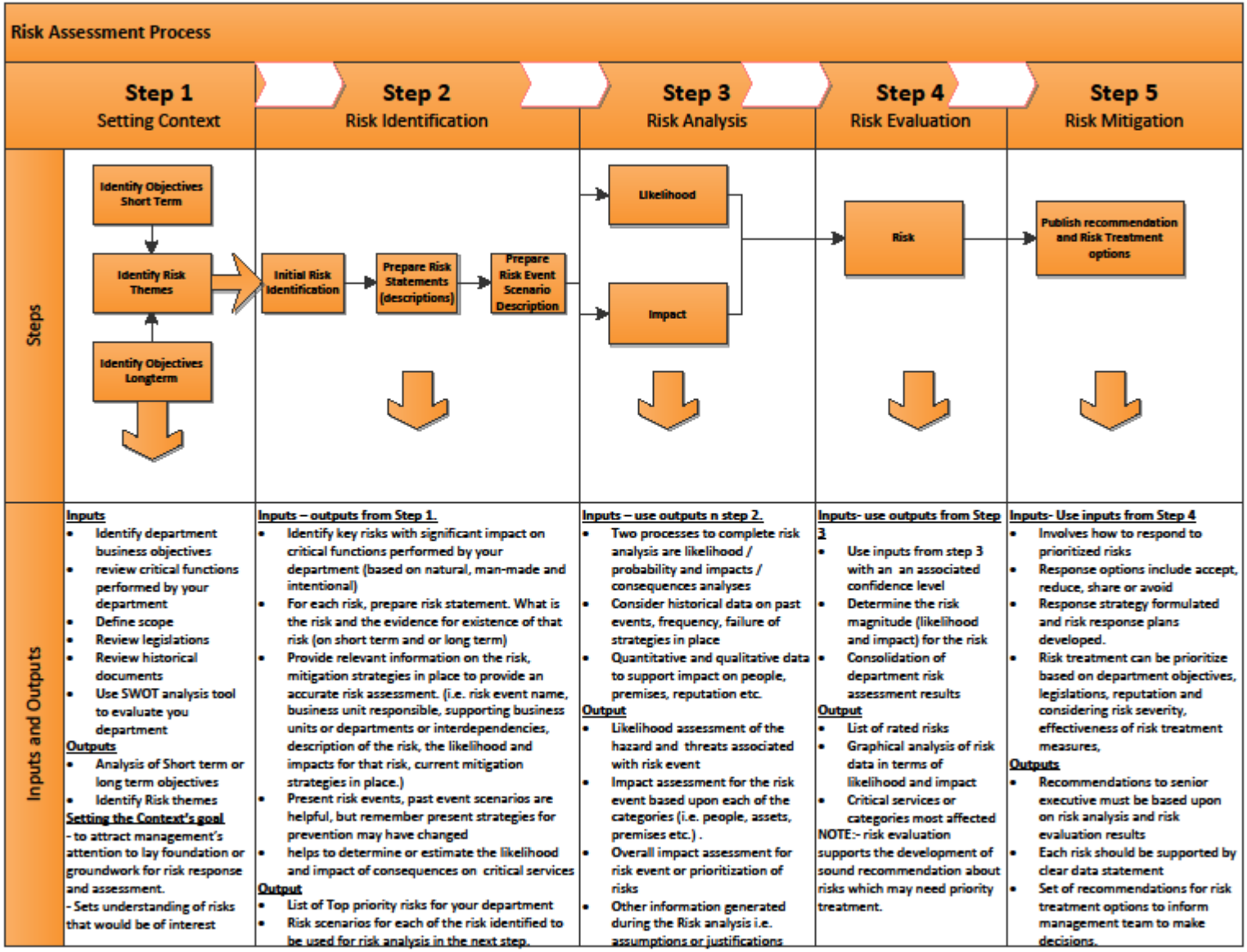
[1] GOA Enterprise Risk Management - https://ext.sp.tb.alberta.ca/Planning/Pages/ERM.aspx

- RAs will be reviewed annually at a minimum, and will be fully conducted whenever there is a significant change in the department.

5.5.3 Risk Assessment Walkthrough

A sample walkthrough of a RA 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. Note that acceptance or ignorance of a risk is a decision to be made by the risk owner, not the BCO; and
- **Risk Mitigation** – 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.


Risk Assessment Process
Step 1
Setting Context
Step 2
Risk Identification
Step 3
Risk Analysis
Step 4
Risk Evaluation
Step 5
Risk Mitigation
Steps
Identify Objectives Short Term
Identify Risk Themes
Identify Objectives Longterm
Initial Risk Identification
Prepare Risk Statements (descriptions)
Prepare Risk Event Scenario Description
Likelihood
Impact
Risk
Publish recommendation and Risk Treatment options
Inputs and Outputs
Inputs
Identify department business objectives
review critical functions performed by your department
Define scope
Review legislations
Review historical documents
Use SWOT analysis tool to evaluate you department
Outputs
Analysis of Short term or long term objectives
Identify Risk themes
Setting the Context's goal
- to attract management's attention to lay foundation or groundwork for risk response and assessment.
- Sets understanding of risks that would be of interest
Inputs – outputs from Step 1.
Identify key risks with significant impact on critical functions performed by your department (based on natural, man-made and intentional)
For each risk, prepare risk statement. What is the risk and the evidence for existence of that risk (on short term and or long term)
Provide relevant information on the risk, mitigation strategies in place to provide an accurate risk assessment. (i.e. risk event name, business unit responsible, supporting business units or departments or interdependencies, description of the risk, the likelihood and impacts for that risk, current mitigation strategies in place.)
Present risk events, past event scenarios are helpful, but remember present strategies for prevention may have changed
helps to determine or estimate the likelihood and impact of consequences on critical services
Output
List of Top priority risks for your department
Risk scenarios for each of the risk identified to be used for risk analysis in the next step.
Inputs – use outputs n step 2.
Two processes to complete risk analysis are likelihood / probability and impacts / consequences analyses
Consider historical data on past events, frequency, failure of strategies in place
Quantitative and qualitative data to support impact on people, premises, reputation etc.
Output
Likelihood assessment of the hazard and threats associated with risk event
Impact assessment for the risk event based upon each of the categories (i.e. people, assets, premises etc.) .
Overall impact assessment for risk event or prioritization of risks
Other information generated during the Risk analysis i.e. assumptions or justifications
Inputs- use outputs from Step 3
Use inputs from step 3 with an an associated confidence level
Determine the risk magnitude (likelihood and impact) for the risk
Consolidation of department risk assessment results
Output
List of rated risks
Graphical analysis of risk data in terms of likelihood and impact
Critical services or categories most affected
NOTE:- risk evaluation supports the development of sound recommendation about risks which may need priority treatment.
Inputs- Use inputs from Step 4
Involves how to respond to prioritized risks
Response options include accept, reduce, share or avoid
Response strategy formulated and risk response plans developed.
Risk treatment can be prioritize based on department objectives, legislations, reputation and considering risk severity, effectiveness of risk treatment measures,
Outputs
Recommendations to senior executive must be based upon on risk analysis and risk evaluation results
Each risk should be supported by clear data statement
Set of recommendations for risk treatment options to inform management team to make decisions.

5.5.4 Step 1 – 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. Accordingly, the first step of a RA is setting the departmental context. 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 them as Critical, Vital, Necessary and Desired. It is important to understand these services at all levels of your department;
- **Scope** – Define the scope for the RA. Will the RA cover every Business Unit or will it be limited to a specific Business Unit?;
- **Information Gathering** – Gather all necessary information including (but not limited to) legislation, regulation, policies, and historical data; and
- **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 (but are not limited to) risk caused by loss of staff, loss of IT, loss of communications etc. Not every department will face the same risk themes, and not every theme will carry the same weight in each department.

5.5.5 Step 2 – Risk Identification

Risk identification is the process by which specific risks are named and described. It must be noted that naming a risk must be done by generalization based upon the underlying nature of the risk. For example, a risk may be named and defined as a lack of sufficient trained personnel. It is immaterial in terms of BC planning (other than in mitigation strategies) as to whether this lack is caused by absenteeism due to illness or inability to physically access the work location as a result of severe weather. The underlying problem is that sufficient trained personnel are unavailable to deliver the department's essential services. Risk identification is performed by the BCT and the risk owners.

Methods to Identify Risk

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; and
- Essential Services List.

Risk Identification - Output

- Named list of risks for your department; and
- Existing mitigation strategies.

5.5.6 Step 3 – Risk Analysis

During this step of the RA process, the named list of risks for your department will be considered in the context of likelihood and impact. This is the step wherein mitigation strategies will be identified / developed, and prioritized in order to ensure resources are best employed. The objective of risk analysis is to understand risk in terms of its likelihood of the named risk occurring, and its impact on essential services. During this stage the BCO will develop more specific risks (i.e. absenteeism due to illness) from the generalized risks (absenteeism) in order to better determine the likelihood of the risk occurring.

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 and qualitative.

5.5.6.1 Quantitative analysis

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?).

5.5.6.2 Qualitative analysis

Qualitative analysis consists of comparison based upon informed judgment of a 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 quantitative, is better able to

describe potentialities. Nobody can see the future; one can only estimate the probability and impact of an event. One caveat to a quantitative assessment is the fact that as circumstances change, the value of historical data changes. For example, if a BCO was estimating the likelihood and potential impact of flooding in a specific area, all historical data would become invalid once flood mitigation measures were completed.

5.5.6.3 What is likelihood in the context of Risk Analysis?

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.

Quantitative measures for calculating Likelihood:

- **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. The table below displays some common Probability and Frequency descriptors.

Sample Probability and Frequency Descriptors

P Descriptor	Probability (P) definition	F Descriptor	Frequency (F) definition
Certain	>99% chance of occurring in a given year (one or more occurrences per year.)	Frequent	Up to once in 2 years or more
Likely	50 - 99% chance of occurring in a given year (one occurrence every one to two years.)	Likely	Once in 2 years up to once in 25 years
Possible	5-49% chance of occurring in a given year (one occurrence every 2 to 20 years.)	Possible	Once in 25 years up to once in 50 years
Unlikely	2-5% chance of occurring in a given year (one occurrence every twenty to fifty years.)	Unlikely	Once in 50 years up to once in 100 years
Rare	1 - 2% chance of occurring in a given year (one occurrence every fifty to one hundred years.)	rare	Once in 100 years
Extremely rare	<1% chance of occurring in a given year (one occurrence every one hundred or more years.)		

Once this process has been completed for all named risks, the risks can then be ranked from Most Likely to Least Likely.

5.5.6.4 What is Impact in the context of Risk Analysis?

Impact or consequence are used interchangeably; for the purpose of this guide, impact will be used. 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.

Quantitative representation of impact:

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.

> **Note:** - Human life cannot be quantified.

Qualitative representation of Impact:

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.

> AEMA has identified a range of conditions to measure impact and these include manageability of the event, staff health and safety, essential services and records, infrastructure, interdependence, financial costs, and public visibility[2].

Below is an example of a qualitative measurement system for fatalities and injuries. You can repeat the same with the rest of measurement criteria you have chosen (such as financial costs, public visibility etc.).

[2] GOA BCP 2013:- Cross Government Risk Assessment Annex M, Figure M1

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

5.5.6.5 Key considerations in analyzing risk include (but are not limited to):

- Determination of the frequency of the particular risk;
- Degree of predictability of the particular risk;
- Speed of effect of the mechanism 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 (ie 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; and
- Obligations (external and internal).

Risk Analysis Output

List of particular risks expressing both the likelihood and impact of each risk.

5.5.7 Step 4 – Risk Evaluation

In a perfect world, each department would have unlimited resources to mitigate each identified risk. Unfortunately, however, the GOA operates in a resource-constrained environment and must decide which risks must be mitigated and which risks must be accepted. In order to do this, each particular risk identified in the Risk Analysis must be evaluated against each other in order to enable prioritization.

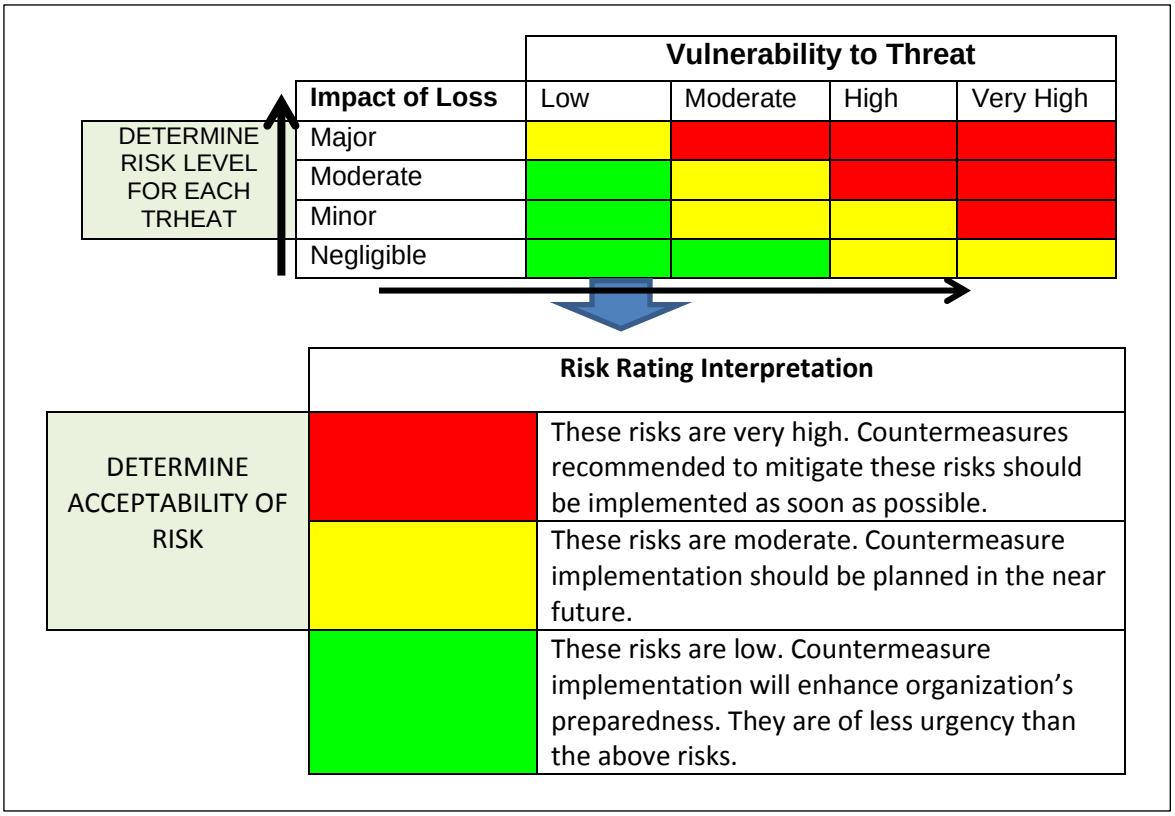
Risk evaluation assists in determining the vulnerability of an organization to the risk events. Risk evaluation is the process of comparing risk levels with established criteria to determine whether a risk is acceptable or tolerable.

This process is done after completing risk analysis; it requires estimation of both impact and likelihood for an entire department through careful and objective consideration.

The risk that is considered to have high impact / likelihood might actually turn out to have low or medium impact after considering the organization's preparedness, adaptability and mitigation measures already in place. Alternatively, without mitigation, a medium impact risk could actually represent a high impact in the event of risk occurrence.

Therefore, vulnerability refers to the susceptibility of an organization to a risk. When calculating vulnerability to the threat consider **success** (*how likely the threat is to succeed*); **extent** (*how much damage there is likely to be*) and **rating** (s*ummary of both aspects, value from the chosen range for vulnerability*).

A sample categorization method for risk evaluation is displayed below:



An example of a prioritized list of risks for a Risk Evaluation is displayed below:

Subject: Staff / People **Date: dd/m/yr**

If there are more threats per asset, use extra lines

Asset	Cost /impact	Threat	Likelihood	Rating of Likelihood	Vulnerability			Threat Summary	Overall Assessment
					Success	Extent	Rating		
Staff	Priceless High	Pandemic	Once in 20 years	Low	Moderate	Very High	High	High	
		Succession / Skill Loss	Once in 1 year	High	High	High	Very High	High	

Subject	Type of resource or asset being assessed i.e. staff
Date	Date the Risk Assessment is conducted
Asset	Description of the asset to be assessed
Cost / Impact	Total value of the asset, considering how much it would to replace or how important or value it is to the organization.
Threat	Brief description of the threat
Likelihood	How often does this threat arise? See likelihood explanation
Rating of likelihood	Value chosen from the range of likelihood.
Vulnerability - success	How likely the threat is to succeed. This helps in determining risk response strategies
Vulnerability - extent	How much damage is likely to be experienced - This helps in determining risk response strategies
Vulnerability - rating	Summary of both aspects and a value from the chosen range for vulnerability
Threat Summary	Provide a summary of the risk for that specific asset or a summary of threat combination to that particular asset or resource
Risk Assessment	Provide an overall assessment of the asset taking into account of all threats.

Risk Evaluation Outcome

Prioritized list of particular risk that will be mitigated

5.5.8 Step 5 – Risk Mitigation

Risk Mitigation is the final step in RA; risk mitigation encompasses all strategies by which the identified risks will be addressed. Risk mitigation strategies include (but are not limited to) increasing redundancy of critical systems, identifying personnel for staff augmentation / replacement, identification of alternate facilities etc. Note that in a resource-constrained environment it may not be possible to mitigate against every potential risk; the final decision as to which risks will be accepted rests with the departmental Executive Team.

ISO 31000 identifies four risk management strategies or risk response strategies:
- Acceptance
- Reduce / control / contain the risk
- Transfer or Share the risk
- Avoid the risk

5.5.8.1 Acceptance

Risk can generally be accepted if the any or all of the following conditions exist:

- The potential impact is minimal;
- No cost effective mitigation is possible; and
- The risk is assessed as unlikely.

If the department decides to accept the risk, it is important to understand the implications of that decision. Choosing to accept a risk means that no steps are taken to prepare for the consequences should that risk event occur. At that point the department will simply hope for the best, and manage the consequences should the event happen.

5.5.8.2 Reduce / Control / Contain

Reduction / controlling / containing risk is all about prevention and minimization. The types of risks that are most often reduced / controlled / contained are those with low impact but high probability.

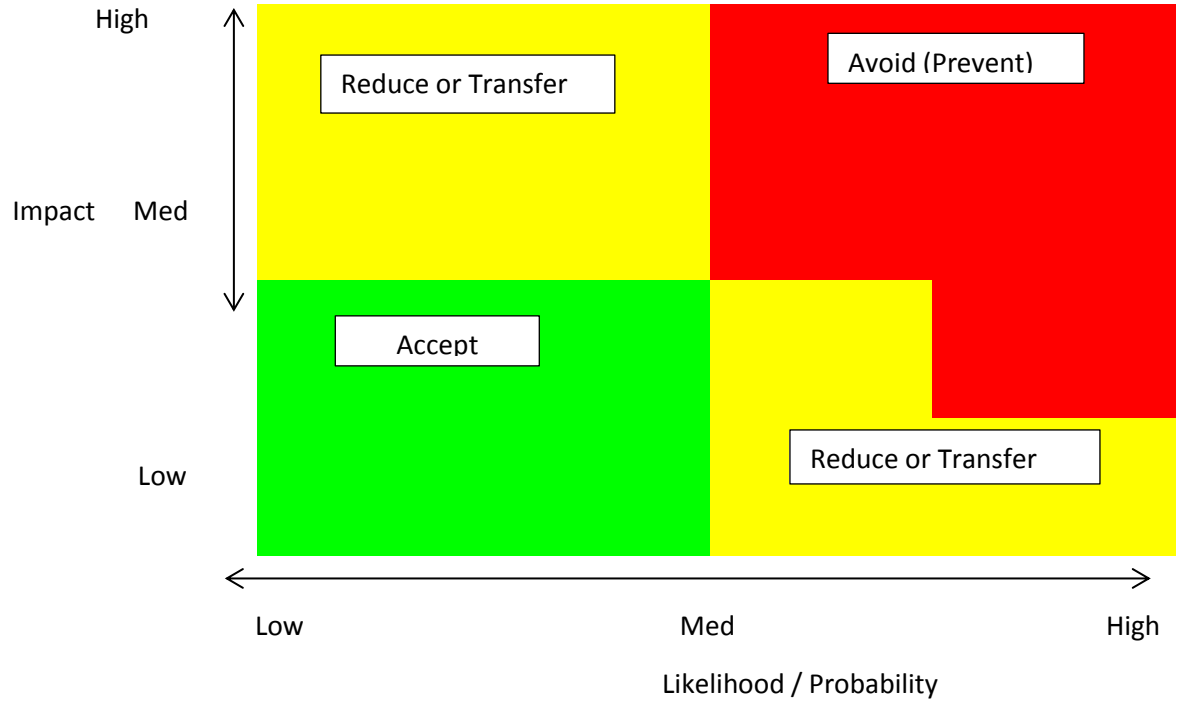
5.5.8.3 Transfer or share

For departments in the GOA, a risk may exist within the department that would be inappropriate for the department to address individually. The most common example of this type of risk would be IT service outages. Since 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 particular department may face a high impact risk due to an IT outage, this specific risk is either transferred to the outsourced service provider or shared with other departmental IT teams.

5.5.8.4 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 risk mitigation, as to avoid a risk, the risk must be completely eliminated through redundancy or an equivalent strategy.

Risk Response Matrix



5.6 Summary

RA is a crucial step in BC planning. It is impossible to prepare for every conceivable risk; however, without a thorough, objective assessment of risk it is likely that a department will either be extremely well-prepared for an event that never happens, or be completely unprepared for an event that happens often.

For a RA to be useful, the assessment must be objective, detailed, and accurately reflect the impact of an event on a department.

Finally, BCOs must fully understand that while they may be the ones preparing the RA, it is the Executive Team and risk owners who retain the authority to mitigate risk. BCOs may make recommendations; ultimately, the Executive Team will make the decisions.

Business Impact Analysis

About this section

Note: The primary sources for this material are:

Principles & Practice of Business Continuity: Tools and Techniques, Jim Burtles, Rothstein Publishing, 2007.

Supply Chain Management Guide to Business Continuity, 1st Ed, A.K. Betty, American Management Association, 2011.

The Definitive Handbook of Business Continuity Management, Andrew Hiles, Wiley Publishing, 2011.

6 Business Impact Analysis

6.1 Key Terms

The GOA BC program recognizes the value of approved national and international standards[3]. These standards allow for linguistic consistency across government. The following BIA terminologies are defined in accordance with ISO 22300-2012 (Societal security--Terminology).[4]

Business Impact Analysis (BIA) – This is the process of analysing activities and the effect that the business disruption might have upon them.

Maximum Acceptable Outage (MAO) – This is the period it would take for adverse impacts, which might arise as a result of not providing a product / service / function or performing an activity, to become unacceptable.

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.

Minimum Business Continuity Objective (MBCO) – Refers to minimum level of services and / or products that is acceptable to the organization to achieve its business objectives during a disruption

Recovery Point Objective (RPO) – Refers a 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 product or service must be resumed, or activity must be resumed or resources must be recovered.

Process – Refers to a set of interrelated or interacting activities which transforms inputs into outputs, for example:

- A ***business process*** - a group of business activities / tasks performed by a business function in pursuit of a business service / product or an organizational goal. A business process usually depends upon several business functions for support, e.g. IT, personnel, facilities, suppliers, etc.
- A ***business function*** – a business unit within an organization focused on a specific business goal or ***service***. This may be a section, a department, or a division depending on the complexity of the organization.

[3] GOA BCP 2013: Section 8.1
[4] ISO 22300 – 2012: Terminologies

6.2 Overview

A comprehensive BIA is one of the key professional practices identified by DRI International[5] ; it is considered a core competence in business continuity 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 that facilitate that service.

This section explains the value of a BIA and what a BCO must know to conduct an effective and viable BIA that:

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

The BIA not only ensures that resources are applied appropriately toward protecting an organization's most critical services, it also saves the unnecessary expense of applying an inappropriate level of resources to less critical areas. If correctly conducted, a BIA provides clear, trusted, consistent and real risk impact analysis information to senior management against which they can make quality decisions about managing risks.

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; and
- 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.

[5] DRII Professional Practices: Business Impact Analysis

6.3 Why Conduct Business Impact Analysis

Business continuity best practices (ISO 23301- 2012 and the CSA Z1600-2008[6]) require that a BIA must be conducted to justify business continuity strategies for critical business functions, associated resource requirements and interdependencies. Within the GOA, a BIA helps the business continuity officer to:

- 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; and
- Map dependencies and relationships between business processes and supporting systems[7].

A BIA separates and delineates time critical business functions / services by differentiating those functions / services that are absolutely critical and / or vital[8] 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.

6.4 How to Conduct Business Impact Analysis

Conduct of a BIA consists of:

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

[6] ISO 22301 – 2012: Section 8.2.2; and CSA Z1600-08: Section 5.1.2.1
[7] GOA BCP 2013:Section 9.4
[8] GOA BCP 2013: Section 9.2 and 9.3 (essential services as defined in the GOA BCP 2013)

Fundamentally, for a BIA to be undertaken successfully, senior management must fully support the BIA within the wider goals and objectives of the BCM[9] program. In communicating the goals and objectives of a BIA, BCOs should help 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 BC 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.

Required Steps For a Comprehensive BIA.

- Step 1 – Define the Scope
- Step 2 – Preparing the BIA
- Step 3 – Data Collection: scope and methods
- Step 4 – After the Interview
- Step 5 – BIA -Data Input
- Step 6 – Data Moderation
- Step 7 – Prepare Final Report for BIA

6.4.1 Step 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 the resources available to complete the BIA. For large organizations, it can be helpful to conduct a pilot project within an individual business unit or division. The pilot project may help to confirm that the BIA questions are accurately testing departmental policies and processes;
- 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. Currently, the GOA BCP identifies four categories of criticality defined as critical, vital, necessary, and desired or desirable[10]; and

[9] ISO 22301 – 2012: Section 5.1 & Section 5.2; CSA Z1600-2008: Section 4.1
[10] GOA BCP 2013: Section 9.3; Figure 3.

- High level senior management or business unit managers[11] 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.

6.4.2 Step 2 – Preparing the Business Impact Analysis

To prepare the BIA, the BCO must choose the method of data collection / interviews and tailor questionnaires to the organization's size, complexity and culture. Clear instructions must be provided with the questionnaires.

Once the questionnaires are prepared, the BCO will identify business owners or process owners and notify them of the BIA to ensure that relevant information is prepared.

- 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; and
- Questionnaires should be specifically designed for each level of staff (employees, management, directors).

Once the questionnaires are ready, the BCO will provide guidance to participants on their completion.

The BIA should focus on the key areas of the organization, sometimes referred as '5Ps'. The 5Ps are:

- **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 which generate the critical business function or service;
- **Providers** - Stakeholders; Communication both internal and external; and
- **Profile** - impacts should be assessed against people, reputation / credibility, premises, processes, environment, economic and financial, regulatory and contractual obligations and providers.[12]

[11] ISO 22301 – 2012: Section 3.53; NOTE 1 & 2

[12] CSA Z1600-08: Section 5.1.3; ISO 22301 – 2012: Section 8.3.2 (note ISO focuses on resources requirements as whereas the CSA focus on impacts against the 5Ps)

A BIA questionnaire can be quantitative, qualitative or a mixture of both.[13] The table below shows examples for quantitative and qualitative BIA elements:

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

6.4.3 Step 3 – Data Collection: Scope and Methods

6.4.3.1 Scope

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; and
- How current the information is likely to be.

Understanding the "Human Response"
Participants who are less well-versed in business continuity or emergency management practices may feel competing pressures when participating in a BIA. They may feel pressure to hide or minimize risk genuinely experienced by their department in order to enhance personal and organizational competency; they may also struggle to differentiate between what is an essential service to their unit versus what is essential to the department or the GOA as a whole.

[13] Principles & practice of Business Continuity: Tools and Techniques 2007 by Jim Burtles.

6.4.3.2 Methods

There are a number of ways in which data can be collected and verified. Chosen methods must produce desired results and offer flexibility to meet your departmental needs. Each of the following methods has strengths and weaknesses. In collecting data, the BCO should match the appropriate method to the information requirements and organizational capacity. Common BIA data collection methods are:

- **Questionnaires** –This is a simple, cost effective written approach where questions can be distributed electronically via email or via a SharePoint site or in a paper format for manual completion. Questionnaires are completed by interviewees independently and with minimum support from the developer;

  - Provide clear, concise instructions to ensure participants are clear about what is expected of them and how they should complete the questions.
  - Be cognizant of the time required to complete your questions and be up front about it when you write your instructions; you will have a higher response rate if the time commitment is reasonable given competing professional demands and is clearly communicated.
  - Ensure your distribution methods are consistent and reach the appropriate audience.
  - Be prepared to offer support and guidance to interviewees during completion of the questionnaires.
  - Set a clear deadline for response to be submitted.

- **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 which may be raised by the interviewee. Interviews can be conducted either in person or remotely, via such means as telephone or video conferencing; and

- **Physical inspection** – Involves physically viewing the site / location being reviewed. By physically viewing the location or site or working environment, the BCO 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 RA. The risk of this method of data collection is the likelihood that the BCO does not have intimate familiarity with the operations and processes being viewed.

6.4.4 Step 4 – After the Interview

- Information obtained from a BIA interview must be recorded in a consistent way. This ensures information is acquired and tracked in a consistent manner; and
- Time permitting, result should be confirmed with departmental leads or unit owners before compiling final analysis. Departmental leads will be the most reliable source to flag inconsistencies or potential inaccuracies.

The ultimate Goal of the feedback from the interviewees is to enable the BCO 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.

6.4.5 Step 5 – Input of the Data (BIA)

6.4.5.1 Criticality Order

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.

Individuals who are less familiar with creating essential services lists or conducting BIA's might feel that this process devalues or minimizes the work that they do. As BCO, you will need to ensure consistent and clear communication to all staff that this process is to identify key vital services that must be maintained for support to the GOA and to Albertans and is not intended as a value or budgetary ranking.

To determine how important critical function / service is, consider the following factors:

Assess the impact severity to Albertans if the function or service were to be stopped The GOA BCP outlines four maximum time outages thresholds for restoration of service:

- Critical – services that must be restored within 24 hours.
- Vital - services that must be restored within 72 hours.
- Necessary - services that must be restored within 2 weeks.
- Desired - services that 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.

6.4.5.2 Dependencies

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.

6.4.5.3 Resource requirements

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).

6.4.5.4 Time requirement

One of the end results of a BIA is identification of the amount of time required to perform the process or activity in order to deliver the product or service to its key stakeholders.

- **Maximum Tolerable Period of Disruption (MTPD)** - is the maximum amount of time that the department's key services can disrupted before the disruption becomes intolerable to the GOA or Albertans in general. This is the crucial parameter in selecting recovery strategies.

The GOA has identified four MTPD categories; services that are:

- Critical - must be restored within 24 hours
- Vital - must be restored within 72 hours
- Necessary - must be restored 2 weeks, and
- Desired - more than 2 weeks.

6.4.6 Step 6 – BIA 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; and
- 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 disagreement and seek guidance from management to provide guidance if bottom up analysis fails to provide convincing results; and
- Present or deliver a formal presentation of BIA report draft to peers and appropriate senior managers to discuss initial findings.

6.5 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 should:

- 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; and
- State the minimum resource requirements for recovery of each business unit.

6.6 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; and
- **MTPD** for key products or services.

6.7 Checklist

BIA Checklist	Completed Yes / No
1. What are the key / major processes or functions carried out by the unit	
2. For each identified key / major Risk Assessment a. Does it depend on the availability of a product or service from outside the unit - If yes, what is the effect if the product or service is unavailable - Does the unit have any control over the availability of the product or service? - How long can the operation continue without the product or service? b. Who depends on the products / services of this operation? - How are they affected if the product / service is unavailable? c. Are there any legal, regulatory, contractual, statutory, social, political. environmental obligations to carry out the operation? - If yes, what are they? - What are the implications if a process fails? - How long can the operation outage last before it becomes unacceptable?	
3. Are there any anticipated changes (such as re-organization, software upgrades etc.) which will have implications on the operation? If yes, what are they?	
4. What are the minimum resource requirements to enable the unit to recover from an operation outage, for example: a. number of staff b. number of desks, chairs, telephones, computers c. any special equipment d. time required to move to alternate sites	
5. Have you consulted key personnel (for example business continuity team and stakeholders)	
6. Have you evaluated the impacts of a loss of each major / key operation or critical process from the perspective of the entity's objectives? Consider: - Health and Safety - Legislation / Regulatory - Financial; - Reputation - Environmental - Political - Legal / contractual - Social - Interdependences and third party relations	
7. What are the vital records and are they identified?	
8. Have you identified alternative / manual process techniques that can be adopted during the recovery phase as needed.	
9. Other issues to be on your checklist: - Determine the maximum tolerable period of disruption (MTPD) for each critical process - Obtain executive support and endorsement of the BIA.	

6.8 BIA Worksheets

1. List key functions in priority order

Department:	Date BIA Completed:
Business Unit:	BIA Point of Contact:
Key Functions – List all applicable functions:-	
1.	
2.	
3.	
4	

2. The sample worksheets below can be used as a guideline for a BIA.

This chart is adapted from the ISO Risk Management Guide framework.

PEOPLE	PREMISES	PROCESSES	PROVIDERS	PROFILE / IMPACT
Key Staff What staff required carrying out key functions?	**Buildings** From which locations do a department's key functions operate? (Primary site, alternative premises)	**IT** What IT is essential to carry out key functions?	**Reciprocal Arrangements** Are there any reciprocal agreements with other organisations?	**Reputation** Who are key stakeholders?
Skills / Expertise / Training What skills / level of expertise are required to undertake key functions?	**Facilities** What facilities are essential to carry out key functions?	**Documentations** What documentation / records are essential to carry out key functions, and how are these stored?	**Contractors / external providers** Do you tender key services out to another organisation? If so - to whom and for what?	**Legal considerations** What are legal, statutory and regulatory requirements?
Minimum Staffing Levels What is the minimum staffing level with which could provide some sort of service?	**Equipment / Resources** What equipment / resources are required to carry out key functions?	**Systems & Communications** What systems and means of communication are required to carry out key functions?	**Suppliers** Who are your priority suppliers and whom do you depend on to undertake your key functions?	**Vulnerable Groups / Social** Which vulnerable groups might be affected if your organisation fails to carry out key functions?
				Do the same for: - Financial - Political - Environmental - Health and Safety

PEOPLE	PREMISES	PROCESSES	PROVIDERS	PROFILE- IMPACT
Key Staff Can staff be contacted out of hours? Could extra capacity be built into your staffing to assist you in coping during an incident?	**Buildings** Could you operate from more than one premise? Could you relocate operations in the event of a premise being lost or if access to the premise was denied?	**IT** Is data backed-up and are back-ups kept off site? Are there any disaster recovery arrangements in place?	**Reciprocal Arrangements** Do you have agreements with other organisations regarding staffing, use of facilities in the event of an incident?	**Reputation** How could reputational damage to your organisation be reduced? How could you provide information to staff and stakeholders in an emergency (e.g. press release)?
Skills / Expertise / Training Could staff be trained in other roles? Could other members of staff undertake other non-specialist roles, in the event of an incident?	**Facilities** Are any of your facilities multi-purpose? Are alternative facilities available in the event of an incident?	**Documentations** Is essential documentation stored securely (e.g. fire proof safe, backed-up)? Do you keep copies of essential documentation elsewhere? (i.e. off-site storage)	**Contractors / external providers** Do you know of alternative contractors or are you reliant on a single contractor? Do your contractors have contingency plans in place? Could contractors be contacted in the event of an incident?	**Legal considerations** Do you have systems to log decisions; actions; and costs, in the event of an incident?
Minimum Staffing Levels What is the minimal staffing level required to continue to deliver your key functions at an acceptable level? What measures could be taken to minimise impacts of staff shortfalls?	**Equipment / Resources** Could alternative equipment / resources be acquired in the event of an incident / disruption? Could key equipment be replicated or do manual procedures exist?	**Systems & Communications** Are your systems flexible? Do you have alternative systems in place (manual processes)? What alternative means of communication exist?	**Suppliers** Do you know of suitable alternative suppliers? Could key suppliers be contacted in an emergency?	**Vulnerable Groups / Social** How could vulnerable groups be contacted / accommodated in the event of an incident?

Interview worksheet Example:

Business Process Identification Definitions

Key Word	Explanation - information which be entered in each column of the Worksheet:
Operation	Name or brief description of the operation / process / function.
Input	Name or brief description of critical input needed for the operation to be carried out or a piece of information and/or the completion of a task/process needed in order to commence or complete a business process.
Input Source	From where the critical input comes or the point of origin (within the organization) of the input for a business process.
Outage Time	How long the operation can continue without the critical input.
Control	How much control over the input there is, for example none, poor, total, contractual.
Output	Name or brief description of the product or service resulting from the operation or an outcome, product or service resulting from the completion of a business process.
Recipient	Who needs the output (to be followed up with recipient) or the name of the client, customer or business process the output is sent to.
Obligation	Details of any legal, contractual, statutory, social or political obligations to carry out the operation.
Impact	Brief description of the impact of an operation stoppage, severity and who will be affected.
Criticality	How quickly the operation must be resumed after a disaster has occurred, as perceived at the time of the interview. May be updated as the interviews proceed (very high, high, moderate, low and very low)
Comment	Brief comment from the interviewer and interviewee, as appropriate, to cover, for example, details of forthcoming changes which may affect the operation.

Name of Interviewee: **Department Unit**

Interviewer **Date**

Operation / Function / process	Input	Input source	Outage time	Control	Output	Recipient	Obligations	Impact	Criticality	Comment
Pay System - IMAGIS	Computer system	Computing	1 day-	Total	Bi-weekly / monthly	Staff; social welfare	Contractual / social	No payments	High	Very important end of second week and end of the month

Impact Worksheet Example

Impact Definitions

Key Word	Explanation
Impact – name or brief description	Brief description of the impact of an operation stoppage.
Source of impact	Operation or business unit causing the impact (may be external).
Subject of impact	Operation or business unit subject to the impact.
MTPD - to subject	Highlight the shortest time if there is more than one.
Effect – fuller description	Fuller description of the impact of the operation stoppage.
Consequence – if uncorrected, obligation	What will happen if the impact is not corrected? Will any obligations to other business units be affected?
Assessed severity	Assessment of how severe the impact of the operation stoppage would be, using the agreed classification categories and ranges.

Prepared By: **Date:**

Impact – name or brief description	Source of impact	Subject of impact	MTPD - to subject	Effect – fuller description	Consequence – if uncorrected, obligation	Assessed severity
Failure of computer system	Technical failure	Pay – IMAGIS	1 day	System not available	Unable to make payment	High

Business Continuity Strategies

About this section

7 Business Continuity Strategies

7.1 Key Terms

Business Continuity – The capability of the organization to continue delivery of products or services at an acceptable pre-defined levels following disruptive incident.

Continuity Plan – A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level.

Incident – A situation that might be, or could lead to, a disruption, loss, emergency or crisis.

Infrastructure – A system of facilities, equipment, and services needed for the operations of an organization.

Outsource – To make an arrangement where external organization performs part of an organization's function or process.

Policy – The intention and direction of an organization as formally expressed by the Executive Team.

Recovery – The restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organizations, including efforts to reduce risk factors.

7.2 Overview of Business Continuity Strategies

Business Continuity Strategies is a professional practice within BCM lifecycle that determines the overarching approach and methodology that will support departmental requirements in the face of a major disruption. In accordance with the national standard, the CSA Z1600-14, an organization shall develop strategies based on the information obtained from the hazard identification, RA, and impact analysis.

CSA Z1600-2014 lists BCM program strategies that can fall into the following categories:[1]

- Prevention strategies – strategies that focus on incident prevention
- Mitigation strategies – strategies that focus to mitigate, limit or control the consequences
- Preparedness strategies – strategies that focus to prepare effective response, continuity & recovery management planning
- Response strategies – strategies that focus on response to incidents that threaten people, property, environment and continuity of operations
- Continuity strategies – strategies that focus to continue critical services
- Recovery strategies – strategies that focus to recover to an acceptable level
- Communication strategies – strategies that focus on effective communication throughout the organization
- Training and education strategies – focusing on competency - based training and education.

[1] CSA Z1600-2014: Section 5.5 Strategies

Selected strategies should be directly based on the outputs from BIA and RA.[14] Once risk and impact analyses are clearly outlined, continuity and recovery strategies can be developed and adopted to mitigate disruptions.

In developing BC strategies, it is crucial to involve the BCT as well as individuals from the department or business unit in question. They have intimate familiarity with hands-on factors that affect their unit, and have most likely experienced real world disruptions in the past from which they can draw to create practical resumption strategies. The combination of the professional oversight by the BCO with the hands-on experience of individuals engaged in their day to day activities can help develop realistic and achievable strategies that will work both within the unit and meet the overarching goals of the department.

[14] ISO 22301 – 2012: Section 8.3.1 Determination and Selection (Business Continuity Strategies)

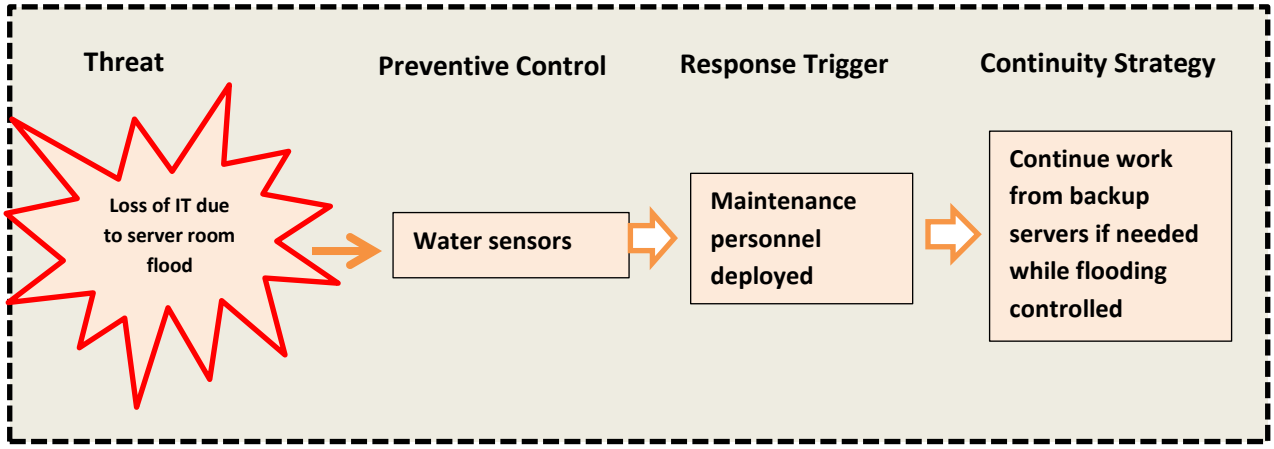
Effective BC strategies intended to recover each aspect of the organization's business must cover the ***what, where, and by whom***. Factors to consider when developing strategies include:

- **Capital** – Recovery costs balanced against speed of recovery;
- **Disaster recovery requirements** - Recovering technology and information systems (system recovery, disaster recovery sites, work area recovery);
- **Resource requirements** - Availability of resources and facilities to continue critical services or activities; and
- **Disadvantages/advantages** – Each strategy will provide advantages and disadvantages for recovery. These must be carefully considered to support the final recommended strategy.

Before starting development of continuity strategies, the BCO should investigate the preventive controls the department has already adopted. The BCO should determine if preventive measures are in place to reduce the potential impact of a disaster, or if treatment options proposed after risk and impact analysis can or will be implemented. Strategies solely designed to recover business functions or systems after a disruption, may not provide the capability to ensure continuity of services if the disruption is severe.

An example of a preventive control is water sensors in the ceiling and floor of a server room which provides warning if water is detected. This enables facility maintenance personnel to respond to the presence of water before catastrophic flooding occurs.

Figure 4 – Preventive Method and Recovery Strategy



7.3 Methods / Sources of Information to Develop Strategies

The methods used to gather information to design and develop BC strategies (workshops, brainstorming, meetings or other techniques etc) are the same as for those used in the RA or BIA.

7.3.1 What BCOs Need to Know When Gathering Information to Develop Continuity Strategies

When gathering information BCOs must:

- Consider key information sources including:
  - Risk and Impact Analyses report;
  - Emergency response operations plans (ie FERPs);
  - Business unit managers; and
  - Staff who would in normal circumstance actually perform the activity to restore business who can walk the BCO through it, explaining the 'why' as well as the 'how to'.
- Identify business levels or mission critical processes to ensure that participants are aware of acceptable outage times. This is necessary to ensure developed strategies consider recovery time and recovery point objectives designed to protect and maintain the department's critical functions;
- List all known interfaces or interdependences to avoid duplication of strategies and reduce implementation costs;
- Highlight the difference between disaster recovery strategies (recovering the technology and information systems that support the business) and continuity strategies (those strategies for basic resources and processes which enable the normal business operations) to the team; don't assume the team knows the difference; and
- Remember that the final choice or approval of a strategy rests with senior management.

> Resource requirements include people (skills and knowledge), infrastructure (buildings and facilities), resources, information technology, telecommunications, non-electronic information and supplies.

7.4 Approaches for Business Continuity Strategies

BCOs will identify a range of possible disaster recovery and continuity strategies to choose from. In selecting appropriate strategies (particularly with respect to alternate

sites), a number of factors should be considered such as physical separation from the primary site, reservation of sufficient resources, accessibility, capacity to accommodate staff, dedicated purpose for disaster recovery, availability of utilities and services.

Examples of Alternate Site Strategies

- Hot Site - a data centre facility or office facility with sufficient hardware, communications interface and workspace capable of providing almost immediate backup data processing support
- Warm Site - a data centre or office which is partially equipped with hardware, communications interfaces, electricity and environmental conditioning capable of providing backup operating support with minimal start-up time.
- Cold Site - one or more data centre or office space facilities equipped with sufficient pre-qualified environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations.

7.4.1 Disaster Recovery Strategies

Disaster Recovery strategies focus on recovering the technology and information systems that support services and programs 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 disruptive event. To increase internal resilience, it is necessary to clearly outline the systems the department uses to provide outward facing service as well as internal processes. Common Disaster Recovery strategies might include dual or redundant systems, automated recovery backups or manual (paper) files. Any proposed IT Disaster Recovery Strategies must be approved by departmental IT.

7.4.2 Business Continuity Strategies

BC strategies address all aspects of essential BC less Disaster Recovery for IT systems. Continuity strategies include workarounds for the disrupted business process or function. For example, if an IT system that produces payments were disrupted and could not be recovered in an acceptable time, the department must have an alternate process by which payments could be generated while the disruption was being resolved. In the case of a disruption to a payment process, strategies might include manual cheques. All continuity strategies will be derived from the risk and impact analyses. Continuity strategies must be developed for each business process or function identified as critical or vital.

Commonly applied 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; and
- Working from remote locations.

It should be noted that it is also possible to have a “Do Nothing” (*Accept the Risk*) strategy where the Executive Team is comfortable with assumption of risk given the cost of preventive or mitigative strategies.

7.5 Strategy Selection Process

Similar to the decision making processes for risk and impact analyses, the final authority for BC Strategies is held by the Executive Team.

7.5.1 Selection Process

The selection process for BC 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; and
- Buy-in from those who are responsible for Essential Services.

7.5.2 Strategy Outcomes

Strategy Outcomes need to be:

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

7.5.3 Steps for Strategy Selection Process

The strategy selection process will include some or all of the following steps as described below:

7.5.3.1 List Practicable Strategies

Use the information generated by information gathering to develop options for business continuity strategies. These options will range from complete duplication of the department (staffing, IT, facilities, etc) to completely working remotely, with a range of other options falling within that continuum. Discard the completely unrealistic options (duplication of the department, 100% remotely), and prepare the list of strategies that could potentially be implemented.

7.5.3.2 Estimate of Costs, Degree of Effort, and Speed of Recovery

After listing feasible strategies the next factor the BCO must consider is the costs or resource requirements for each strategy. It is important to estimate the cost, degree of effort required to implement the strategy, and speed of recovery provided by the strategy as a result of potentially differing perspectives on recovery needs. For example, the Executive Team might be more concerned with costs, while the operational staff might be more concerned with outage time.

7.5.3.3 Operational Considerations and Preferences

Operational staff will help to identify advantages and disadvantages on the various options. The goal is to understand the operational procedures for each proposed strategy so that operational staff needs are sufficiently addressed.

7.5.3.4 Management Considerations

Management considerations must be integrated into the final report to build a business case for the proposed strategies. It is important that management's comments are shared with the BCT.

7.5.3.5 Executive Case Summary

The purpose of the executive business case is to provide the Executive Team with a high level summary which outlines the proposed strategies and recommendations. The business case should be supported with facts and cost figures, as well as with practical considerations including recommendations from the management review.

7.5.4 Executive Input, Decision and Implementation

The Executive Team will either reject or accept the report as written, require changes, additions and / or deletions before making a final decision. Most likely, the DM may request further information before reaching a decision (perhaps in consultation with his or her Executive Team). The BCO should be prepared to support them through their deliberations so that informed final decision can be reached. Once the final decision has been made, the selected strategies will be incorporated in the departmental BCP.

7.6 Summary

Outlining the objectives of BC strategies is extremely important. The BCO is responsible for guiding the process to develop effective recovery and continuity strategies. Selected strategies must meet departmental policies, and are based upon the outputs from risk and impact analyses. The final selection process must be based upon Operational, Managerial, and Executive Team needs while still remaining both practical and cost-effective. Once the Executive Team has approved the final BC strategy (ies), the BCP will be written to clearly explain how those strategies will be implemented through processes, procedures, and protocols.

Awareness and Training

About this section

8 Awareness and Training

8.1 Awareness and Training Objectives

The objectives of an Awareness and Training Program include:

- To develop and conduct BCM awareness training for all staff;
- To develop and conduct crisis management team training; and
- To develop and conduct BC training for key appointments and the BCT.

8.2 Creating Awareness

A successful BC program is more than a binder on a shelf or a well mapped out policy on your hard drive; it is a program of which employees and partners are actively aware and engaged. 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 when the plan is activated. Awareness and staff engagement should be conducted throughout the program planning cycle; ideally, staff have been engaged in developing various elements of the BCP and value their continuing contribution to the security of business operations.

8.3 Training

Training refers to specific educational practices intended to gain skill in executing BC activities. Current best practice requires participation in a training program for those staff directly involved in implementing the BCP in the event a disruption and suggests, where possible, basic introductory training for all other staff.

8.3.1 General Staff Awareness Training

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

- An overview of what the BCM Program encompasses;
- Why BCM is important to the department;
- What is the employee's role during a BCP activation; and
- Where staff can locate emergency contacts.

8.3.2 Business Continuity Team Training

This training should be delivered to staff with specific BCM responsibilities within the BCP. It aims to improve the BCM skills of the BC team as well as increasing personal investment in the BCM process within the department. Key topics may include:

- BCM concepts, processes, policies, continuity / recovery strategies;
- How to complete/update risk / impact analyses;
- How to document recovery plans;
- How to test the plans; and
- Coordination with other departments, AEMA and other stakeholders.

8.3.3 Executive and Senior Management Training

This training is tailored to the Executive Team and Senior Managers with the aim of providing a high-level view of how the BCM program is linked to the department's strategic vision. One of the benefits of executive training is that it ensures executive level buy-in and support for the BCM program.

8.4 Awareness and Training Frequency

It is recommended that the BCM team develop (at a minimum) 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.

The GOA requires that all departments conduct collective BC training exercises on an annual basis. Awareness and training sessions prior to these exercises ensures that the exercises will strengthen departmental BC, thereby increasing the resiliency of the department.

Program Maintenance

About this section

9 Program Maintenance

9.1 Overview

A maintenance program ensures that the BCP remains current and relevant, ready to handle any business disruption. The BCO must design the maintenance program in such a manner as to validate effectiveness of the BCP. In order to maintain and update the BCP, it is necessary to assign responsibilities to the BCT or business unit owners according to their specific responsibilities as described in the plan. When revisions are made, they must be documented, dated and reflected in the plan. The BCP should be reviewed and updated at least on an annual basis. Program maintenance and plan review will need to be undertaken:

- After changes to business objectives or processes;
- After changes to Risk Assessments;
- After changes caused by new functions, services and technology;
- After change to the department's location;
- After the department has performed an exercise;
- After review or audit where gaps have been identified and recommendations for improvements are made;
- After departmental re-organization;
- In accordance with the department's BC maintenance program; and
- After changes to key supporting plans such as FERP etc.

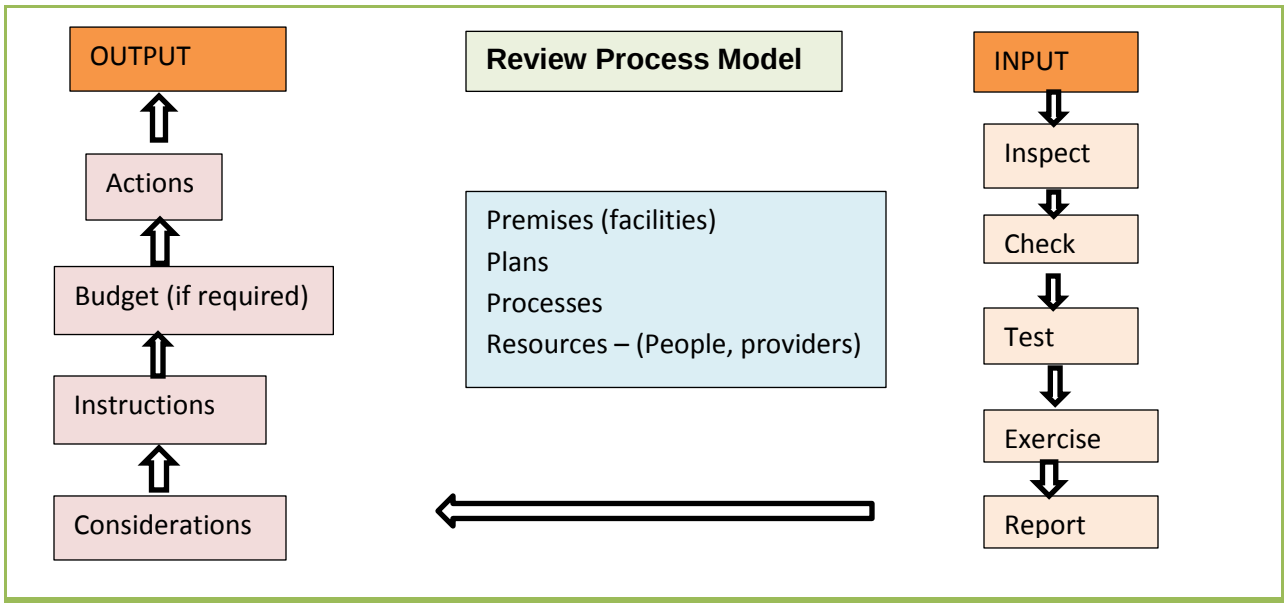
Departments should define their plan maintenance schedule at frequencies ranging from monthly to biennially, in accordance with the schedule laid down in the department's plan maintenance guidelines. For example:

Maintenance Component	Maintenance Timeframe
Departmental BCM Program	Biennial review by AEMA - Per the GOA BCP and legislation requirements
BCM Policy	Reviewed and updated bi-annually
Business Impact Analysis and Business Continuity Strategies	Reviewed and updated once a year or after any significant changes to the business
Risk Assessment	If it is no longer valid or if there has been a significant change within your department and GOA in overall.
Business Continuity Plan	Reviewed and updated once a year, and after any significant changes to the business
Contact Lists (employees, stakeholders, BCT)	Reviewed and updated every 3 months, or after a change of personnel
Emergency Response Operations	As required based upon recommendations from Lessons Learned from a real emergency or exercise
Awareness and Training	When new ideas emerge for creating awareness or training
Plan Distribution	After updates

9.2 Review Process

Plan review is an internal quality control process which assess the effectiveness of an extant plan by the judgment of those who are directly involved in BC 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 5 – The Review Process



9.3 Audit Process

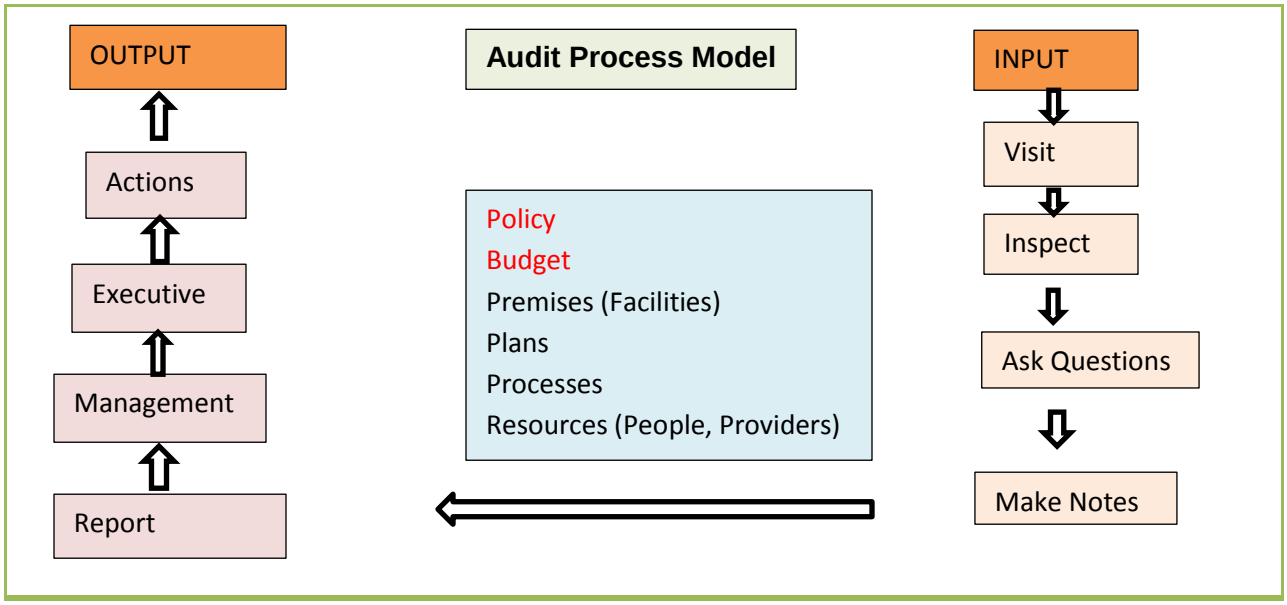
Auditing is a review process carried out by an external agency, and is designed to assess compliance with policy, legislation and regulation. An external audit is separate from the departmental BCM program, and provides an objective viewpoint. A standard audit of a BCM program will review the entire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

- Strategy – holistic view of the management process, overall BC strategy, budget, policy and executive decision making;
- Analysis – Risk and impact analyses;
- Implementation;
- Test; and
- 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; and
- Highlighting deficiencies and issues.

Figure 6 – The Audit Process



Exercise and Testing

About this section

10 Exercising and Testing

10.1 Overview

The main goal of exercising and testing BCPs is to ensure that the BCP can achieve the department's BC objectives. Exercising and testing procedures are a critical element of a complete BCM. Executive Team support is essential to an effective Exercise and Test Program, as their influence is often required to ensure participation even by those with key roles in business continuity.

There is a difference between a test and an exercise. A test is type of activity whose aim is to obtain an expected, measurable pass / fail outcome within the structure of the planned activity. Testing is often applied to supporting plans, or focused on a specific component of the plan. Exercises, by contrast, are activities consisting of full execution of BCPs with a view to identifying strengths and weaknesses of the complete plan in order to improve the 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; and
- Provide a controlled opportunity to practice improvisation.

Exercises and Tests can be conducted as:

Component (Usually a Test)

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

Integrated (Usually an Exercise)

A number of inter-related components are exercised concurrently to validate that they can work together to complete the required objective. These exercises require more extensive planning and coordination. An example of an integrated exercises is a call out tree test combined with mobilisation of staff to commerce operations at the alternate site.

Full (Exercise)

A full exercise consists of executing all components of the BCP. Such an exercise will require extensive planning, coordination, and cooperation within the department and cross-governmentally if other departments are involved. It is advisable that a full exercise should only be attempted after extensive component and integrated exercises.

10.2 Exercises Types or Methods

There are a number of methods that can be applied to exercise or test the BCP depending on the intent of the exercise or test and what resources are available to support the exercise. Some of these include:

10.2.1 Walkthrough or Orientation Business Continuity Exercise (BCX)

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 BCT 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 that need to be fixed.

10.2.2 Table Top BCX

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 BCT to help foster team interaction and improve decision-making, and to validate specific response capability. Table top BCXs address 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; and
- Reinforce the content and logic of the plan.

10.2.3 Simulation BCX

BCTs 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; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization.

Lessons Learned Section

About this section

11 Lessons Learned

11.1 Purpose

The purpose of this section is to provide information on how to complete the Lessons Learned process after a disruption or an exercise. The *Government Emergency Management Regulation (GEMR),* section 2 (1)f-B, requires departments, in consultation with AEMA to review the effectiveness of the plans based on the **lessons learned** evaluation criteria established for a real emergency.

The objective of a Lessons Learned review is to validate existing policies and procedures and to amend and improve gaps and oversights on a go-forward basis. Lessons Learned reviews can draw 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. It is imperative that the review focuses on the BC system and not at individuals who are fulfilling roles within it. Lessons Learned should then be tested against overarching policy, legislation and regulations and then disseminated into current BC practice.

NB: **Lessons Learned** often describes a procedure or process (also known as a post incident review process or an after action review) and **lessons learned** describes the findings that emerge from the process that can be then put into a BCP or into policy.

11.2 Lesson Learned Activities

11.2.1 Conducting Lessons Learned Session

A Lesson Learned session provides a forum to discuss and acknowledge the successes and gaps that were experienced by participants during an event or an exercise, and it offers an opportunity to brainstorm improvements and modifications for the future. Lessons Learned reviews can be conducted in person; either one on one with individual participants or in a group setting; they can be completed via remote conferencing abilities; and they can be completed remotely and submitted to the Lessons Learned coordinator for compilation. The ideal methodology will depend on geography and availability of past participants and the scope of the review a department is undertaking.

Ideally, a Lessons Learned session should be completed a few days after conducting an exercise and as soon as feasible after a disaster or disruption. This will encourage participants to provide as clear and detailed feedback as possible.

11.2.2 Documenting Lessons Learned Activities

Lessons Learned are captured and documented in the After Action Report or Post Incident Action Report, and shared with AEMA to improve cross-GOA resiliency.

11.3 Implementation

Moving suggestions from a Lessons Learned review or Post Action Report into the actual BCP is one of the most crucial pieces to keeping a BCP energized and current, but also one of the most challenging. BCOs must assess and prioritize the suggestions that are most relevant and achievable for the department.