Guideline

Information Management Service Continuity Plan

Governance

Authority:	Office of the Chief Information Officer
Audience:	Information Management professionals and other resources responsible for the implementation and operation of a records and information management system (also referred to as an Information Management Program) within a department or other public body, as defined in the Management of Information Act.
Compliance Level:	Recommended
Issuing Public Body:	Office of the Chief Information Officer Application and Information Management Services Information Management Services
Original Issue Date:	2023-02-20
Date Last Reviewed:	2023-02-20
OCIO Reference:	DOC00656/2023
Version Number:	1.0

Notice:

The Office of the Chief Information Officer (OCIO) is mindful of creating and delivering accessible materials, in line with the Government of Newfoundland and Labrador's Accessible Communications Policy. New materials created by OCIO align with policy requirements and modifications to existing materials will occur as part of the standard review cycle.

This document is available in alternate format. Please contact OCIO@gov.nl.ca.

Forward questions and/or comments related to this document to IM@gov.nl.ca.

Table of Contents

1.0 Overview 4
2.0 Purpose 5
3.0 Definitions and Acronyms 6
4.0 Recommended Approach 8
4.1 Understanding IM Service Continuity 9
4.1.1 Service Interruptions 9
4.1.2 Business Impact Analysis 10
4.2 Identify Key Information Governance Stakeholders 10
4.3 IM Services Delivered By the IM Program 11
4.4 IM Requirements of a Department or other Public Body 12
4.5 Integrate Business Continuity and/or Disaster Recovery Plans 13
4.6 Communicate Strategy 14
4.7 Monitor and Verify 15
5.0 Roles and Responsibilities 16
6.0 Supporting Materials and Version History 17
Appendices 18

1.0 Overview

Service continuity focuses on planning for incident prevention, prediction, and management in the event that a department or other public body's programs or services are disrupted. The goal is maintaining programs and services at the highest possible levels when a long-term disruption of normal service provision is anticipated.

The main purpose of an Information Management (IM) Service Continuity Plan is to support the overall department or other public body's business continuity planning process by making sure that sound IM advice is available to assist in the recovery of information assets.

Guidelines are recommended actions, general approaches and operational behaviors. Generally, Guidelines are a description that clarifies what should be done and how to achieve the objectives set out in policies, directives and standards.

Guidelines issued by OCIO provide a recommended approach, which takes into consideration the varying nature of information management programs.

2.0 Purpose

The Guideline – IM Service Continuity Plan provides a recommended approach that will serve to drive the design, development, implementation and management of an effective IM Program. This Guideline is part of a broader GuideBook that supports the requirement set forth in the Management of Information Act (MOIA) for permanent heads of departments and other public bodies to implement a records and information management system.

The GuideBook, also known as the Guide to IM for Public Bodies, includes the following guidelines.

Graphic: 1 - GuideBook Contents

Expected Deliverable(s)

1. The development and implementation of an IM Service Continuity Plan to support the organization's business continuity planning.

3.0 Definitions and Acronyms

A complete listing of terms are located on the OCIO website - Information Management and Protection (IM&P) Glossary of Terms.

Business Continuity Plan (BCP) – guides the actions and decisions to ensure effective continuation or recovery of all essential services. A BCP outlines the governance structure and procedures to be used to allocate resources and to coordinate the continuity activities. It may be implemented in whole or in part as the disruption requires.

Information Management – the field of management responsible for establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of an organization's records and information. (Source: ARMA)

IM Program – for the purposes of compliance with the MOIA, the OCIO defines a records and information management system (also referred to as an IM Program) as a four-part system that includes Management Framework, Core IM Capability, Enablers, and Monitoring and Verifying IM. See the Quick Reference – Records and Information Management System document on the OCIO website for additional details.

IM Service Continuity Plan – supports the overall department or public body's business continuity planning process by ensuring that sound IM advice and support is available to assist in the recovery and protection of information assets.

Information Governance Stakeholder – a business unit or a functional area that is involved with or affected by an organization's information assets. In addition to records management, information governance stakeholders include, but are not necessarily limited to, information technology, information security, risk management, legal affairs, compliance, and the individual departments or other organizational units that have recorded information in their custody or under their supervisory control. (Source: ISO)

Vital Records – records that are fundamental to the functioning of an organization. Certain vital records contain information critical to the continued operation or survival of an organization during or immediately following a crisis. Such records are necessary to continue operations without delay under abnormal conditions. They contain information necessary to recreate an organization's legal and financial status and to preserve the rights and obligations of stakeholders, including employees, customers, investors and citizens.

Some vital records may be unique and not easily reproducible, or the cost of reproduction or replacement may be considerable. They may be required in their original form to meet or fulfill evidential requirements. The term vital records also includes documentation subject to a vital records program such as pertinent IT systems, help manuals, or emergency contact lists. For the purposes of this Guideline, the use of this term does not mean solely those birth and death records referred to as "vital records" in the vital statistics or health industry. (Source: ARMA International, Emergency Management for Records and Information Management Programs)

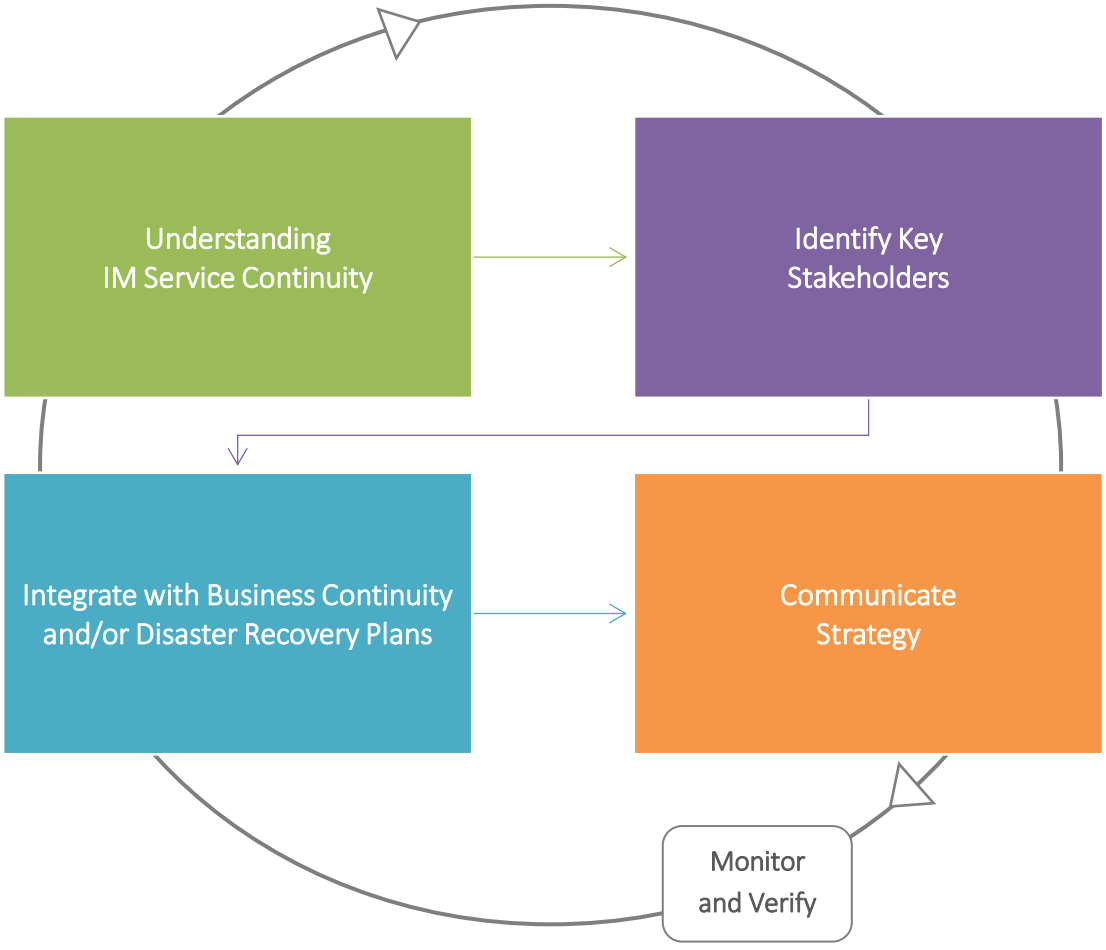
The table below includes common abbreviations used by OCIO as well as acronyms found within this document.

Abbreviation	Description
BCP	Business Continuity Plan
IM	Information Management
IM&P	Information Management and Protection
MOIA	Management of Information Act
OCIO	Office of the Chief Information Officer
PDCA	Plan, Do, Check, Act

4.0 Recommended Approach

The intent of this Guideline is to provide recommended actions, general approaches and operational behaviors that when implemented will serve to drive the design, development, implementation and management of an effective IM Program through the development of an IM Service Continuity Plan.

After reading this document, a department or other public body should be able to apply the knowledge and have an understanding of an organization's IM service continuity requirements.



Graphic: 1 - Recommended Approach

4.1 Understanding IM Service Continuity

IM Service Continuity is the concept of identifying risks and protecting information to avoid disruption in programs or services. There will always be risks that may affect your organization's information, which is why it is important to have a comprehensive plan to mitigate the risks to programs services.

Developing and implementing an IM Service Continuity Plan contributes to:

- Improved organizational functions like service delivery and decision making.
- Alignment with overall Business Continuity Plan (BCP) of the organization.
- Better collaboration and coordination between clients and stakeholders.
- Annual reviews of plan to remain in line with changing business needs.

4.1.1 Service Interruptions

An IM Service Continuity Plan ensures there is a strategy for the safety of personnel and confidential information and continuation of services during an interruption. Disruptions cannot always be stopped, but what organizations can do is embrace them, and more importantly plan for it. Many factors can cause disruptive events, such as a pandemic, adverse weather, or a cyber-security breach. For example, during a pandemic, there may be no physical risk to infrastructure or information, but much of the infrastructure or information may not be accessible because employees become ill or are out of the office to take care of sick family members. Throughout an adverse weather event employees may have to work remotely which can alter the general workflow of what information or applications they have available. This may directly affect how programs and services are delivered to the people of the province. The impact of a cyber-security breach can result in the theft of valuable and sensitive information, or disrupt system applications making them unavailable.

An IM Service Continuity Plan will ensure a continual delivery of information and services is provided effectively. It is important to initiate a plan where employees can work without being vulnerable to threats or further service disruption.

In the event of a disaster or service interruption, vital information should be restored first to the minimum service levels necessary to provide delivery of programs. Often departments or other public bodies rely on their IT Division to assist in bringing systems back online, in the event restoration of systems take time, measures should be taken to continue services (i.e., manually if necessary). Departments or other public bodies should refer to the organization's records inventory in order to identify records classified as vital.

4.1.2 Business Impact Analysis

Business Impact Analysis ensures that during a service interruption the plan for what vital information should be restored first aligns fully with the overall organizational objectives.

An IM Service Continuity Plan should identify business processes based on the urgency of continued delivery of mission-critical programs and services for the department or other public body. Recovery time of getting information systems up and running may vary due to several factors such as available IT assets, human resources, etc.

In the event of an interruption, a list of essential programs and services must be considered first to be restored in order for the department or other public body to remain operational throughout the event.

Programs and Services in departments and other public bodies are typically restored in terms of its time criticality such as:

- Critical Services – are those that must be provided immediately or the loss of life, infrastructure destruction, loss of confidence in the government and/or significant loss of revenue will result. These normally require continuity or restoration in less than one day following an interruption;
- Vital Services – are those that must be provided in less than one week or loss of life, infrastructure destruction, loss of confidence in the government and/or significant loss of revenue or disproportionate recovery costs will result;
- Necessary Services - are those that must be recovered in less than one month or considerable loss, further destruction or disproportionate recovery costs will result;
- Desired Services – are those that could be delayed for one month or longer but are required in order to return to normal operating conditions and alleviate further disruption or disturbance to normal conditions. There are no Business Continuity Plans for this category of service.

4.2 Identify Key Information Governance Stakeholders

When developing an IM Service Continuity Plan, it is important to identify key information governance stakeholders and the role they play in the organization. For example, Executive, IM Division staff, and those responsible for the department or other public body's Business Continuity Plan (BCP) are primary stakeholders who must be consulted when developing an IM Service Continuity Plan.

Attaining approval from key information governance stakeholders is one of the most important steps when developing an IM Service Continuity Plan. It ensures that there is interest in the plan, so others will support your efforts, and that employees will assist and accept the plan once implemented.

4.3 IM Services Delivered By the IM Program

When developing an IM Service Continuity Plan, an organization's IM Program Plan can be extremely useful. An IM Program Plan provides details on how IM services are created, delivered and managed.

Put simply, the IM Program Plan describes:

- What IM services, projects, activities and events are provided to whom, when and why;
- How the IM services are provided or delivered, and by whom;
- How the IM services are planned and managed to ensure end user and management satisfaction; and
- What resources are required, and where and by whom do you get them (i.e., Laptops, forms, backups).

These are critical questions that must be known in the event of a service disruption. It is important to identify IM services that are available both internally and externally. Understanding what IM services you provide will determine what advice you deliver in your plan to restore services during a disruption.

Internal IM Services

Internal IM services refer to those services delivered within the organization, including those supplied directly by IM or those that arise because of other business functions within the organization.

A department or other public body's IM Program Plan should provide the following information on internal services:

- Records and Information Management Systems
- Records Storage (e.g., records center, offsite, etc.)
- Disposition Authorities (RRDS, CRIMS and Transitory processes)

External IM Services

External IM services fall into two categories: services provided by the OCIO and services provided by third party vendors. In many cases, the contract for these external IM services are managed by central agencies (such as OCIO or the Public Procurement Agency (PPA)) through Standing Offer Agreements. Some of the external IM services provided by the OCIO are:

- IM Advisory Services
- Capacity Development
- Education and Awareness

Third party vendor services may include:

- Offsite Storage
- Physical Destruction (Shredding)

4.4 IM Requirements of a Department or other Public Body

Sound IM practices are crucial to successful IM Service Continuity. IM helps a department or other public body operate efficiently. An organization's memory resides in its records. Aside from facilitating the effective operation of an organization during its day-to-day business functions, in the event of service disruption, the information and knowledge embedded in an organization's records is critical for the continued existence of the organization.

In any organization, information is one of the core elements since it helps to make the aforementioned decisions. As a result, it is important to ensure the continuous flow of information so everybody can avail of the necessary information. By this continuous flow of information, IM Service Continuity can be achieved.

4.5 Integrate Business Continuity and/or Disaster Recovery Plans

Departments and other public bodies are increasingly subject to service disruptions. It is almost impossible to predict their nature, time and extent. Therefore, they need a proactive approach to protect themselves against the outcomes of a service interruption.

Traditionally, Business Continuity Planning and Disaster Recovery Planning were carried out separately. Business Continuity Planning typically aims to develop appropriate plans prior to a service interruption, emergency or disaster in order to resume operations to a minimum acceptable predefined level. Whereas, Disaster Recovery plan picks up after the immediate crisis has been dealt with, and refers to issues such as restoring data, recovering interrupted applications, and getting back to normal operations.

Although the goals of each of these areas are different, it is not until you combine the two that you are ready for an effective response to a service interruption. An integrated plan to combine both should include the following elements:

Identify	Protect	Test	Train
• Indenifying possible disasters, or service interuptions is vital to developing a recovery plan to mitigate them.	• Protecting information by providing limited access.	• Testing the business continuity plan and/or disaster recovery plan will provide possible outcomes that will assist with more accurate preparation.	• Training employees is essential to help prevent disasters or service interuptions and/or, to initiate recovery plans.

4.6 Communicate Strategy

When developing an IM Service Continuity Plan a department or other public body can use the Plan, Do, Check, Act (PDCA) Method to assist in this process.

PDCA Method	IM Service Continuity Plan Actions (Consecutively)	
Plan	Develop a IM Service Continuity Plan	Define services that are critical to your organization, for example health, safety, security or economic well-being of the people of the province or to the effective functioning of government, based on an analysis of the potential impacts of disruption.
	Determine the IM Service Continuity Plan strategies	Organize recovery teams, decide any relocation plans, document manual workarounds.
	Determine the economic assessment of IM Service Continuity Plan	Assess whether more resources (i.e., people, IT infrastructure) are required mitigate risk to avoid/restore a service disruption. Cost to loss of services, i.e., oil and gas revenue.
	Assess impact of disrupted service	Assess risk to data, ranging from information about individual citizens, or national security.
Do	Implement the IM Service Continuity Plan	Develop testing exercises, conduct education and awareness training.
	Practice simulated service interruption scenarios	
Check	Evaluate the simulated outcomes	Update plan to incorporate any lessons learned or shortcomings from testing and exercises.
Act	Develop the current plan based on best performance	Communicate the plan or any updates across the organization at all necessary levels.

During a service interruption, communicating information to relevant parties is a key emergency management priority. Effective communication can help stabilize a situation and lessen the adverse effect.

4.7 Monitor and Verify

A review and validation of an organization's IM Service Continuity Plan and processes are the mechanisms for monitoring and verifying IM success. The IM Service Continuity Plan needs to be lifecycle managed to ensure it provides accurate and relevant information in an often evolving environment.

5.0 Roles and Responsibilities

Departments and other Public Bodies

- Support the department or other public body's compliance with MOIA as well as OCIO-issued policies, directives, standards and guidelines, and ensure that proper protocols are in place to properly develop and manage a records and information management system, often referred to as an IM Program.
- Support the inclusion of IM Service Continuity in the organization's IM Program.

Directors responsible for IM

- Align organization-issued materials with the guidance provided by the OCIO in the development and implementation of an IM Service Continuity Plan.
- Apply a continual improvement approach to the management of the organization's IM Program to ensure the review and implementation of an IM Service Continuity Plan.

Office of the Chief Information Officer

As part of OCIO's administration of the Management of Information Act, the OCIO

- Recommends to Treasury Board policies for adoption.
- Develops, manages, monitors, and communicates IM&P policy instruments and supporting materials to departments and other public bodies.
- Provides direction on IM&P best practices, resource requirements, organizational structure, recordkeeping systems and IM Programs to departments and other public bodies.
- Assists departments and other public bodies to improve their IM&P capacity.
- Provides IM&P advisory, training and awareness services and support to departments and other public bodies.
- Supports IM forums, committees, and other professional practice communities, consisting of IM representatives from departments and other public bodies.

6.0 Supporting Materials and Version History

Supporting Materials

Below is a listing of supporting materials hyperlinked to the published location.

Management of Information Act
http://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Information Management and Protection Policy
https://www.gov.nl.ca/exec/ocio/im/im-ip-policy/

Information Management and Protection (IM&P) Glossary of Terms
http://www.ocio.gov.nl.ca/ocio/im/glossary.html

OCIO Website
https://www.gov.nl.ca/exec/ocio/

Version History

The following table highlights the version history of this document including date issued and version number.

Date (yyyy-mm-dd)	Version
2023-02-20	1.0

Appendices

Appendices listed below directly relate to the Guideline – Planning for IM Service Continuity are published independent of this Guideline on the OCIO website, https://www.gov.nl.ca/exec/ocio/im/policy-instruments/guidebook/.

Appendix	Title
A	Checklist – Information Management Service Continuity
B	Quick Reference – Records and Information Management System
C	FYI – Planning for Information Management Service Continuity