



Power to Ontario.
On Demand.

**Meter Data Management and
Repository (MDM/R)**

**Business Continuity
Manual**

Issue 0.95

This document provides an overview of the responsibilities of MDM/R Service Recipients making use of the MDM/R incident management framework set out in the MDM/R Terms of Service.

MANUAL

Disclaimer

The posting of documents on this Web site is subject to the terms and conditions posted on the SMSIP Web site. Please be advised that, while the *IESO-SMSIP* attempts to have all posted documents conform to the original, changes can result from the original, including changes resulting from the programs used to format the documents for posting on the Web site as well as from the programs used by the viewer to download and read the documents. The *IESO* makes no representation or warranty, express or implied, that the documents on this Web site are exact reproductions of the original documents listed. In addition, the documents and information posted on this Web site are subject to change. The *IESO* may revise, withdraw or make final these materials at any time at its sole discretion without further notice. It is solely your responsibility to ensure that you are using up-to-date documents and information.

DRAFT

Document ID	SME_MAN_0008
Document Name	Business Continuity Manual
Issue	Issue 0.95
Reason for Issue	Revised draft reflecting stakeholder input - DOCUMENT NOT IN FORCE
Effective Date	June xx, 2011

Document Change History

Issue	Reason for Issue	Date

Related Documents

Document ID	Document Title
SME_AGR_0002	<i>MDM/R Terms of Service</i> – NOT IN FORCE
SME_AGR_0001	<i>SME-LDC Agreement</i> – NOT IN FORCE
SME_PRCs_0001	<i>MDM/R Temporary Change Control Process</i>
SME_MAN_0006	<i>MDM/R Change and Baseline Management Manual</i> – NOT IN FORCE
SME_MAN_0007	<i>MDM/R Incident Management Manual</i> – NOT IN FORCE

Document Control

DRAFT

Table of Contents

Table of Contents	i
List of Tables	iii
Table of Changes	iv
1. Introduction	1
1.1 Scope	1
1.2 Who Should Use This Document.....	2
1.3 Assumptions and Limitations	2
1.4 Conventions	2
1.5 Roles and Responsibilities.....	2
1.6 How This Document Is Organized	3
2. Business Continuity in an MDM/R Context	4
2.1 Purpose of this section	4
2.2 Formal Requirements	4
2.3 Recommended Measures.....	4
2.4 Communications Protocols in General.....	5
3. Precautions that <i>MDM/R Service Recipients</i> should take	6
3.1 Why precautionary measures are important	6
3.2 Formal, precautionary obligations.....	6
3.2.1 Maintaining your contact information with the SME	6
3.2.2 Mandatory Periodic Testing and Refinement	7
3.2.3 Data Retention and Re-Transmission Capability.....	7
3.3 Other recommended precautionary measures:	8
3.3.1 Proper configuration of your AS2 Client	8
3.3.2 Regular adherence to the MDM/R Incident Management Process.....	8
3.3.3 Have your own MDM/R Business Continuity Plan.....	8
3.3.4 Conduct your own Business Continuity Testing	9
4. MDM/R Business Interruption Events	10
4.1 Overview	10
4.2 Pre-Planning.....	10
4.3 Initial Response	11
4.4 Recovery	13
4.4.1 Identification of Recovery environment	13
4.4.2 Identification of Recovery Point.....	14

4.4.3 Production Environment Recovery 14

4.4.4 Re-establishing AS2 Connectivity 15

4.4.5 Processing File Backlog 16

4.4.6 Resumption of Production Operations 16

4.5 Restoration 17

5. Disruptions to SME Operations 18

5.1 Pre-Planning 18

5.2 Initial Response 18

5.3 Recovery 18

5.4 Restoration 18

Appendix A: MDM/R Recovery Time Objectives A-1

References 1

DRAFT

List of Tables

Table A-1 - Recovery Time Objective for MDM/R Services A-1

Table of Changes

Reference (Section and Paragraph)	Description of Change

DRAFT

1. Introduction

This manual is part of a series of documents (the *MDM/R Manuals and Procedures*) that detail the interactions required between the *Smart Metering Entity* (SME) and *MDM/R Service Recipients* in using Meter Data Management Repository (MDM/R) services.

The *MDM/R Manuals and Procedures* are enabled by contractual agreement (the “SME-LDC Agreement” or any other instrument that binds the *MDM/R Service Recipient* to the “*MDM/R Terms of Service*”) between the SME and the *MDM/R Service Recipient* – subject to those documents being put into legal force. In the interim, this manual may be further referenced by other legal instruments pertaining to the relationship between the IESO and a given *MDM/R Service Recipient* where applicable.

The procedures described in this manual satisfy the obligations described in the MDM/R Business Continuity plan requirement set out in the *MDM/R Terms of Service*.

1.1 Scope

This manual describes the detailed activities behind the business continuity plan referred to in the *MDM/R Terms of Service*. This document will outline the procedures and interactions required between *MDM/R Service Recipients* and the SME to restore normal service operation as quickly as possible and to minimize the business impact of an event involving the substantial loss of the OSP’s primary MDM/R Operations site availability that is expected to last longer than 24 hours “*MDM/R business interruption events*”.

The SME’s involvement in assisting a *MDM/R Service Recipient*, when they are recovering from a business continuity event within their internal systems, will fall under the scope of the MDM/R Incident Management Manual.

Normal service operation is defined as service operation within the established service levels as set out in Appendix ‘A’ of the *MDM/R Terms of Service*.

The main steps involved in the MDM/R Business Continuity Plan include:

- **Planning:** Including pro-active, precautionary measures taken by both the SME, *MDM/R Service Recipients* and their agents; and
- **Initial Response:** In reaction to a *business interruption event* affecting the MDM/R or the SME’s operations at its principal operations centre.
- **Recovery:** With a core objective to returning crucial MDM/R services to the service levels set out in the *MDM/R Terms of Service*; and
- **Restoration:** With the longer-term objective to returning to normal operations and activities on a robust and stable operating platform.

The MDM/R Business Continuity Plan applies to the MDM/R Production and Disaster Recovery environments only.

This procedure does not include the procedures for the resolution of incidents or problems that are determined to be within the *MDM/R Service Recipients’* systems or processes. These remain the responsibility of the service recipient to resolve.

1.2 Who Should Use This Document

This manual is intended for *MDM/R Service Recipients* who have signed the *SME-LDC Agreement* or have otherwise commenced production operations with the MDM/R under the applicable framework which gives relevance to this document.

1.3 Assumptions and Limitations

This manual pertains to *MDM/R business interruption events* involving the MDM/R production environment and the extent to which those incidents and problems are within the scope or responsibility of the MDM/R Operational Service Provider (OSP – see section 1.5 “*Roles and Responsibilities*” below.).

1.4 Conventions

For the purposes of this document, any references to “*IESO*” or the “*Smart Metering Entity*” (“*SME*”) may be construed to mean the same entity.

For the purposes of this document, any references to “*MDM/R Service Recipient*” shall be considered to include the principal party (i.e. the local distribution company), authorized Advanced Metering Infrastructure (AMI) Operators and Billing Agents of the *MDM/R Service Recipient*.

- An *incident* is defined as any event which is not part of the standard operation of an MDM/R service and which causes, or will cause, an interruption to, or a reduction in, the quality of that service.
- *MDM/R* means the Meter Data Management and Repository developed by the *SME* within which meter read data is processed to produce billing quantity data and such data is stored for future use.
- *MDM/R business interruption event* means an event involving the substantial loss of the *OSP*'s primary *MDM/R* operations site availability that is expected to last longer than 24 hours. The criteria for recognizing and declaring such an event is further elaborated upon in section 4 of this document.
- *MDM/R Service Recipient* means a party that has entered into a *smart metering agreement* with the *SME*.
- *OSP* means the operational service provider engaged by the *SME* to assist with the development and operation of the *MDM/R*.

1.5 Roles and Responsibilities

The *SME* shall be responsible for providing the overall management and administration of the MDM/R Business Continuity process. The *SME* will be the principal point of contact with *MDM/R Service Recipients* in this regard (see section 2 for further details).

The *MDM/R Service Recipient* shall be responsible for the management and administration of their business continuity plans that includes business processes and systems interfacing with the MDM/R. IESO recommends that *MDM/R Service Recipients* have processes in place to withstand business interruptions, including MDM/R business interruptions event lasting of short-duration (less than 24 hours), events of longer duration that involve restoration of services at the primary and/or disaster

recovery sites and processing / re-processing of files and back-log to return to normal service level operation.

The MDM/R Operational Service Provider (OSP) has direct responsibility, by way of a separate agreement with the SME, over the operation of the MDM/R in accordance with established service levels. References to the MDM/R OSP in this document are used to help explain the flow of events over the incident lifecycle. However, as will be explained in this document, the IESO maintains primary responsibility to manage the first tier of support in regards to the incident management process.

As with the normal MDM/R incident management process, the *MDM/R Service Recipient* shall be responsible for internal analysis of incidents prior to contacting the SME to ensure the incident is not internal to their organization. Once an MDM/R business interruption event is declared the *MDM/R Service Recipient* shall also be responsible for providing relevant additional detail and information when requested by the SME or the OSP as per this manual. In specific emergencies, the *MDM/R Service Recipient* may also be required to re-transmit certain information to the MDM/R as part of the system recovery process. *MDM/R Service Recipients* may also be called from time to time to participate in business continuity testing and emergency drills in order to assure the accuracy and completeness of this plan.

1.6 How This Document Is Organized

- **Section 2** describes the nature of this MDM/R business continuity plan.
- **Section 3** of this document outlines pro-active measures that can be taken by every *MDM/R Service Recipient* and their agents to prepare for an *MDM/R business interruption event* before one ever occurs.
- **Section 4** of this document outlines the steps which need to be undertaken in the event of an MDM/R business interruption event
- **Section 5** of this document outlines the reactive steps which need to be undertaken
- **Appendix 'A'** outlines the recovery time objectives for each MDM/R service in the event of an *MDM/R business interruption event*.

– End of Section –

2. Business Continuity in an MDM/R Context

2.1 Purpose of this section

This section summarizes the formal authority of this *MDM/R business continuity manual* (the “formal requirements”) and also points out that this manual contains recommended precautionary measures to be taken by *MDM/R Service Recipients* (“Recommended Measures”). While recommended measures are not formally imposed on *MDM/R Service Recipients* by any agreement with the SME or the MDM/R Terms of Service, they have been included in this manual for the benefit of *MDM/R Service Recipients* by pointing out additional issues areas that they should be directing their own efforts and attention to.

2.2 Formal Requirements

The IESO acting in its capacity of the Smart Metering Entity (SME) is bound by contractual agreement (the “*SME-LDC Agreement*”) with *MDM/R Service Recipients* which in turn gives authority to the *MDM/R Terms of Service*. Both the *SME-LDC Agreement* and the *MDM/R Terms of Service* set out the general scope of this *MDM/R Business Continuity Manual*. Specifically this *MDM/R Business Continuity Manual* sets out:

1. The definition of the MDM/R services whose service levels must be maintained (see also, Appendix ‘A’);
2. **Pre-planning** measures to be taken by the SME and *MDM/R Service Recipients* to protect those MDM/R services (see also, section 3). Some of these proactive measures are explicitly set out in the *SME-LDC Agreement*, while others are set out in this document as recommended guidelines for prudent planning and good business practice; and,
3. **SME Services - Response, Recovery and Restoration** Measures that need to be taken in the event of a disruption to the SME’s ability to carry out its operations from its principal operations centre (see section 5); and
4. **MDM/R Services - Response, Recovery and Restoration** Measures that need to be taken in the face of an *MDM/R business interruption event* (see also, section 4). The *MDM/R Terms of Service* defines an *MDM/R business interruption event* as follows:

“*MDM/R business interruption event* means an event involving the substantial loss of the *OSP*’s {MDM/R Operational Service Provider} primary *MDM/R* operations site availability that is expected to last longer than 24 hours”

2.3 Recommended Measures

The robustness of the Ontario Smart Metering system depends on the actions of all the parties that use it. Section 3 of this document also highlights various proactive steps that *MDM/R Service Recipients* should consider in regards to planning for the continuity of their own business operations insofar as they relate to the Ontario Smart Metering system.

Among the recommendations included in section 3, is that *MDM/R Service Recipients* have their own MDM/R business continuity plan which also encompasses the activities of any agents (AMI or billing) that are acting on their behalf.

2.4 Communications Protocols in General

The overarching communications protocol that governs this manual is meant to mirror that used by the **MDM/R Incident Management Process**. While various communications referred to in this manual may be tailored to suit the specific needs of a given *MDM/R business interruption event*, the use of normal, established communications channels is a critical feature of this process. This approach is taken in order to avoid additional confusion of changing communications paths in the midst of a *MDM/R business interruption event*. To this end, **section 3** of this manual emphasizes the importance of effectively planning and maintaining your registered list of organizational “incident and notifications” contacts with the SME on an ongoing basis.

Exceptions and variations:

The only major exception to the use of normal communications channels during a *MDM/R business interruption event*, may arise from a simultaneous disruption to the SMEs operations at its own facilities and disruption to the operation of the MDM/R. In this case however, your organization’s designated “incident and notifications” contact points will be alerted to any changes in communications paths, protocols or contact points. Again, the foundational precautionary measure that your organization needs to adhere to is the maintenance of your registered contacts as set out in **section 3**.

The process for declaring an *MDM/R business interruption event* is set out in **section 4** of this manual. This section imparts specific requirements for the content of various communications from the SME to *MDM/R Service Recipients*. The overarching protocol is to use existing incident management communications channels unless otherwise declared by the SME.

– End of Section –

3. Precautions that *MDM/R Service Recipients* should take

3.1 Why precautionary measures are important

The MDM/R is an integral component of the broader, Ontario Smart Metering System, and as such, the SME and MDM/R recipients both recognize the importance of business continuity through their mutual *SME-LDC Agreement* with one another, and its constituent documents such as the *MDM/R Terms of Service*. This arrangement is not unlike that of the Ontario wholesale electricity market and the Bulk Electricity System in which both the IESO and *market participants* are bound by the *market rules* to observe and maintain various business continuity functions.

The activities described in this section outline the measures that should be undertaken by *MDM/R Service Recipients* in order to assist the SME and the MDM/R Operational Service Provider (OSP) to mitigate and resolve a major disruption to the MDM/R and/or the SME's operations. Adherence to the guidelines in this section will improve the time required to resolve MDM/R business interruption events and reduce the overhead to all parties involved.

Precautionary, pre-planning guidelines are described below in terms of two general categories as follows:

Section 3.2 - Formal, precautionary obligations: As noted in section 2, these measures constitute formal obligations of the *MDM/R Service Recipient* and by extension, any agents acting on their behalf; and

Section 3.3 Other recommended precautionary measures: These measures are not formally stipulated in any agreement with the SME or the *MDM/R Terms of Service*, but are nonetheless brought to the attention of the *MDM/R Service Recipient* for their benefit in order to assist their own business continuity pre-planning activities.

3.2 Formal, precautionary obligations

3.2.1 Maintaining your contact information with the SME

Maintaining communications during a major emergency is key to mitigating and resolving the situation at hand. When a major emergency unfolds, it is not the timeframe for another party to discover that key contacts are no longer with your company or that a critical e-mail box is not being monitored by anyone. **Most/all of the reactive measures described in the subsequent sections of this document depend on the assumption that your organization has designated and maintained the correct organizational contact points with the SME.** The correct conduit to provide and maintain this information is via the *MDM/R Organization Contacts Form* (SME_FORM_0004) which is available on the SME's website.

One of the key contact types on the *MDM/R Organization Contacts Form* (SME_FORM_0004) is the "incident and notifications" contact type. In the event of an emergency these will be the first contact points in your organization to receive vital information bulletins from the SME.

Some important guidelines to consider:

- Your organization can designate more than one “incident and notifications” contact point, and it is highly recommended that you do so.
- Prompt notification to the SME of any changes to your “incident and notifications” contact points should be part of your organization’s formal business procedures.
- In addition to naming individual staff members, you should also designate common e-mail boxes and/or telephone numbers that are monitored by more than one person. This will help insulate your contact points from the day-to-day changes arising from staff sickness, leaves, vacations, etc.

3.2.2 Mandatory Periodic Testing and Refinement

The *MDM/R business continuity manual* is a living document and shall be periodically tested to ensure that it is functional, current and accurate.

As part of the MDM/R business continuity plan, the OSP and SME maintain a Disaster Recovery environment, which parallels the MDM/R Production environment, and this environment is reserved for use should a business interruption event make the MDM/R Production environment unavailable. The Disaster Recovery environment mirrors the Production environment in functionality and is sized to be able to support contracted service levels at production volumes.

The OSP and SME will perform a test of the MDM/R disaster recovery plan annually. The purpose of this test is to validate that the MDM/R production operations could transfer to the MDM/R Disaster Recovery environment and that the MDM/R Disaster Recover environment would be able to meet the contracted service levels. The SME may require your organization and its agents to participate in these tests. These may focus on a specific aspect of business continuity and/or involve a broader simulation of an emergency scenario, and may include *MDM/R Service Recipients* testing their connectivity to and operations with the MDM/R Disaster Recovery Environment. *MDM/R Service Recipients* (and by extension, their agents) are required to comply with such testing requirements under the *SME-LDC Agreement*. Details of drills and tests will be provided to *MDM/R Service Recipients* with sufficient notice to allow the *MDM/R Service Recipient* to prepare for these tests.

3.2.3 Data Retention and Re-Transmission Capability

Requirements for data retention and re-transmission capability for all *MDM/R Service Recipients* are set out in the *SME-LDC Agreement*. The *SME-LDC Agreement* requires that all information transmitted to the MDM/R must be retained for at least five days.¹ This requirement is critical to ensure that data can be restored if an MDM/R business interruption event occurs while data is in the midst of being transmitted from the MDM/R Production environment to the MDM/R Disaster Recovery Environment.

Some important guidelines to consider in fulfilling this requirement:

- Your organization should have clearly-established business procedures and technical capability to quickly identify and if necessary re-transmit file transfers to the MDM/R within the 5-day time frame.
- Your organization should have the technical resources and staff training in place to detect and diagnose Message Disposition Notices (MDNs) received by your Applicability Standard 2

¹ *SME-LDC Agreement*, section 2.6.4

(AS2) client so that you can pro-actively identify potential problems even before initial contact from the SME. The content and format of an MDN is defined in RFC 3798 which forms part of the AS2 specification. Please see the MDM/R manual, *MDM/R File Transfer Services and Web Services Configuration Workbook* (SME_MAN_9001) for further details. Where necessary, you should ensure active support and assistance from your AS2 client vendor is readily available and that your staff know how to access that support.

3.3 Other recommended precautionary measures:

3.3.1 Proper configuration of your AS2 Client

It is recommended that the *MDM/R Service Recipients' Applicability Standard 2 (AS2)* client be configured in accordance with the recommendations set out in the *MDM/R File Transfer Services and Web Services Configuration Workbook* (SME_MAN_9001). Among the more important considerations to make concerns the use of Domain Name System (DNS) names vs. IP Addresses to identify the MDM/R production environment.

The use of DNS names reduces the recovery actions required by the *MDM/R Service Recipient* should the MDM/R be required to transfer operation to the MDM/R Disaster Recovery environment. Use of DNS names would allow the MDM/R OSP to transfer your AS2 connection to the MDM/R Disaster Recovery Environment without the need for further action on your part. It may however, take a number of hours for the new DNS mapping to take effect once transferred by the OSP.

Use of an actual IP Address by an *MDM/R Service Recipient* to identify the MDM/R production environment would require recovery actions by the *MDM/R Service Recipient* should the MDM/R be required to transfer operation to the MDM/R Disaster Recovery environment. In this case, the *MDM/R Service Recipient* would be required to update the IP Address within their AS2 client to redirect their transmissions to the MDM/R Disaster Recovery environment. Although this requires more action on the part of the *MDM/R Service Recipient*, establishing connectivity to the MDM/R production environment may be quicker than waiting for the DNS mapping to take effect.

3.3.2 Regular adherence to the MDM/R Incident Management Process

The MDM/R manual entitled, "*MDM/R Incident Management Manual*" (SME_MAN_0007) sets out the official channels by which all incidents should be raised with the SME. Your front-line operational staff should be familiar with the contents of this manual and have ready access to the information it contains, including official SME contact points. Once a major incident is raised, the SME and OSP will be able to start diagnosing the problem and make a determination as to whether or not the incident has the potential to become an *MDM/R business interruption event*. Early detection of such incidents by *MDM/R Service Recipients* will assist in mitigating them.

3.3.3 Have your own MDM/R Business Continuity Plan

It is highly recommended that every *MDM/R Service Recipient* organization have its own MDM/R Business Continuity Plan that specifically meets the unique needs of their respective organizations, and is clearly understood by any AMI or Billing Agents acting on their behalf. In general terms, the plan should cover the key Business Continuity Phases of pre-planning, initial response, recovery and restoration, as depicted in Figure 3-1.

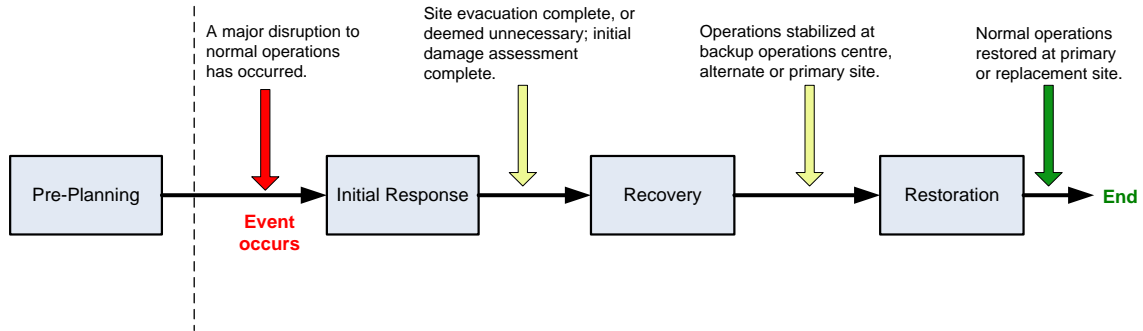


Figure 3-1: Key Business Continuity Phases

Pre-Planning: In this phase, the Business Continuity Plan is developed and maintained, periodic plan testing is conducted, improvement updates to procedures are applied, plus mitigation steps and measures are taken to minimize risk. As well, any coordination with other related business interruption plans (e.g. influenza pandemic, Disaster Recovery Plan) are made to ensure consistency and accuracy.

Initial Response: The reaction to an emergency in order to assess the level of containment and control activity required. Oversee matters of safety and evacuation. Address the policies, procedures and actions to be followed in the event of an emergency.

Recovery: Establish stabilized business operations at the alternate site, when the primary site is deemed unusable (temporarily or permanently) The recovery phase will last up to the point at which point the primary site will be re-activated, or an alternative site identified to act as the primary or backup/disaster recovery site.

Restoration: Restore or re-establish normal business operations at the primary site or a new (replacement) site.

The SME maintains a similar, internal Business Continuity Plan covering the above phases with respect to its own operations.

3.3.4 Conduct your own Business Continuity Testing

MDM/R Service Recipients are required to test connectivity to the MDM/R Disaster Recovery Environment as part of enrollment with the MDM/R. In addition to initial connectivity testing and participating in mandatory MDM/R business continuity testing as outlined in section 3.2.2, it is recommended that *MDM/R Service Recipients* conduct their own, internal business continuity testing. This may be done in conjunction with mandatory MDM/R business continuity testing that your organization will be participating in, or on your organization's timetable as an additional exercise.

- End of Section -

4. MDM/R Business Interruption Events

4.1 Overview

In parallel with the recommendations for every MDM/R Service Recipient to have their own MDM/R Business Continuity Plan, both the SME and the MDM/R OSP have their own internal plans for dealing with an MDM/R Business Interruption Event and/or a disruption to SME business operations. Sections 4 and 5 of this manual outline these activities areas insofar as *MDM/R Service Recipients* are involved in each of the 4 business continuity phases highlighted in figure 4-1.

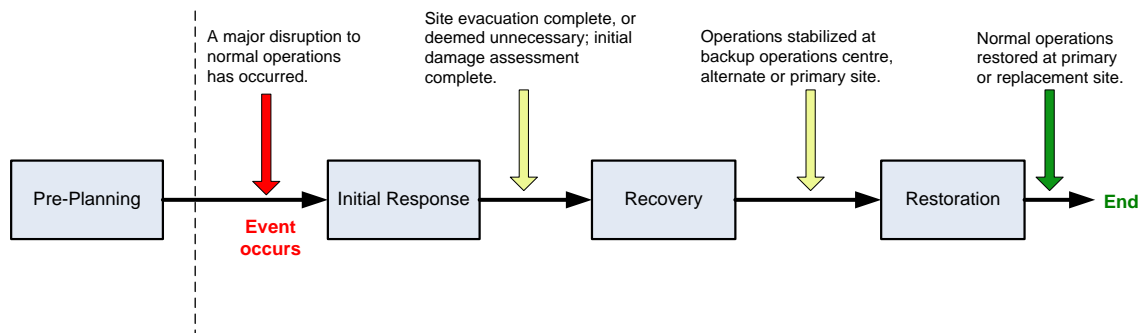


Figure 4-1: MDM/R Business Interruption Event - Business Continuity Phases

General Response and Recovery Expectations:

- The SME is accountable for recovery of the MDM/R system during a Business Interruption event.
- The SME will endeavor to ensure the MDM/R system is capable of processing three times the daily steady-state meter read volume in one business day to minimize the amount of time required to recovery from an MDM/R system outage.
- Service Recipients are expected to have their own independent business continuity plans in place with appropriate processes to respond to Yellow and Red Alert notifications issued by the SME.
- Service Recipients should be able to fail over to a secondary MDM/R production site within one business day of it being made available including submission of any back logged files created as a result of the outage.
- The SME is accountable for ensuring that the MDM/R system is restored at the primary production site within one month of a business interruption event occurring that resulted in fail over to the secondary (disaster recovery) production environment. Alternatively within one month of activation of the secondary(disaster recovery) environment:
 - an additional, second site must be identified and capable of assuming primary or back-up responsibilities (equivalent to those existing before the Business Interruption);
 - failover capabilities within the effective primary site will be available;
 - a full MSNC2 service will be made available; and
 - non-production environments will be made available.

Appendix B provides estimated timeframes for the steps described below in section 4.3 and 4.4 for selected potential business interruption event scenarios.

4.2 Pre-Planning

Pre-Planning in general: In this phase, the Business Continuity Plan is developed and maintained, periodic plan testing is conducted, improvement updates to procedures are applied, plus mitigation steps and measures are taken to minimize risk. As well, any coordination with other related business interruption plans (e.g. influenza pandemic, Disaster Recovery Plan) are made to ensure consistency and accuracy.

SME and MDM/R OSP:

The SME and MDM/R OSP maintain a joint MDM/R disaster recovery plan for the purposes of identifying, declaring, responding and recovering from an *MDM/R business interruption event*.

MDM/R Service Recipients:

MDM/R Service Recipients are expected to be taking the pro-active, precautionary measures set out in section 3 of this document, and any other applicable MDM/R manuals and procedures. As noted earlier, pre-planning activities may require mandatory participation in system wide business continuity drills and specific testing.

4.3 Initial Response

Initial Response in general terms: Initial Response encompasses the reaction to an emergency or potential emergency in order to assess the level of containment and control activity required. Oversee matters of safety and evacuation. Address the policies, procedures and actions to be followed in the event of potential or actual emergency.

4.3.1 Incident Response

The identification, recording, and initial classification for all production incidents occur as part of the Incident Management process. Once the impact of the incident has been assessed, a determination will be made as to whether an alert needs to be issued. The Business Continuity Plan is activated once an incident is deemed to be a Major Incident (i.e. the incident meets the criteria below as a Yellow or Red alert).

If it is deemed that issuing a yellow or red alert is not warranted under the current system conditions, the issue will be dealt with under the Incident Management process and it will not lead to the activation of the Business Continuity plan.

Communications Content:

All Service Recipients will be informed about the incident in accordance to the Incident Management process.

4.3.2 Declaration of Yellow Alert

MDM/R Yellow Alert – Possible Activation of Business MDM/R Disaster Recovery Plan. The SME declares an MDM/R Yellow Alert when an incident:

- Results in a significant disruption to Critical MDM/R services or poses the potential to evolve to an MDM/R *business interruption event*
- Is of medium duration (< 24 hours) with the potential for a longer duration (>= 24 hours)
- Has a clear potential to result in a major impact to *MDM/R Service Recipients*

Communications Content:

Once an SME declares a Yellow Alert, *MDM/R Service Recipients* will be notified. As with any incident, communications to your designated “incident and notification” contacts will detail any specific actions that need to be taken. Such notifications will include

1. a confirmation that an MDM/R yellow alert has been declared;
2. the nature of the situation insofar as it may be known at the time; and,
3. the anticipated time of the next communications bulletin.

Actions:

- SME and OSP alerted and/or engaged.
- Possible activation of MDM/R Disaster Recovery Plan (See Red Alert).
- Initial notification and ongoing status updates to *MDM/R Service Recipients*.

4.3.3 Declaration of Red Alert

MDM/R Red Alert - MDM/R Business Interruption Event Declared. The SME declares an MDM/R Red Alert when an incident is assessed as resulting in:

- An actual or threat of disruption of Critical MDM/R services for a period greater than 24 hours; or
- Situation overwhelms normal incident response capabilities/actions; or
- Authorities declare a disaster affecting the MDM/R’s primary operational facilities.

Communications

Once the SME and the OSP declare an MDM/R Red Alert, *MDM/R Service Recipients* will be notified. As with any incident, communications to your designated “incident and notification” contacts will detail any specific actions that need to be taken. Communication of an MDM/R Red Alert will include:

1. a confirmation that an MDM/R Red Alert has been declared and where applicable, confirmation that MDM/R operations are in the process of being failed over to the MDM/R Disaster Recovery Environment, or the anticipated time when such a failover may occur;
2. the nature of the situation insofar as it may be known at the time; and,
3. the anticipated time of the next communications bulletin and/or contact details for a joint conference call where the situation warrants such action.

Actions

- MDM/R and OSP Disaster Recovery Plans are activated.
- OSP to determine whether or not the fastest estimated path to service recovery actually involves a transfer of operations to the MDM/R Disaster Recovery Environment, or a focused restoration (or partial restoration) of the main MDM/R Production Environment. *MDM/R Service Recipients* will be notified of the intended course of action as soon as possible via designated “incident and notification” contacts.
- OSP to activate MDM/R Disaster Recovery Environment if required.
- Instructions to *MDM/R Service Recipients* for communicating with MDM/R Disaster Recovery environment if required.
- Status updates to *MDM/R Service Recipients*.

4.4 Recovery

Recovery in general terms: Establish stabilized business operations at the alternate site, when the primary site is deemed unusable (temporarily or permanently) or at the primary site should the decision be made to not transfer production operations to the alternate site.

4.4.1 Identification of Recovery environment

Action

The *MDM/R Service Recipients* will be notified on which environment the recovery activities will be performed once the OSP has determined whether the fastest estimated path to service recovery. This may involve the transfer of production operations to the MDM/R Disaster Recovery environment or a focused restoration of the primary MDM/R Production environment.

Communication

- The SME will send an email to all contacts identified with a ‘Incident and Notification’ contact type identifying:
 - The environment in which the recovery actions will be performed,
 - The proposed recovery steps and actions identified by the OSP,
 - The estimated timeframe over which these recovery steps will take place,
 - The communication channel and method for use by *MDM/R Service Recipients* to provide information to the SME through the duration of the *MDM/R business interruption event*,
 - An escalation framework that may be used during a MDM/R business interruption event, and
 - The time and conference bridge information for an SME hosted conference call regarding the incident and anticipated recovery.
- The SME will host a conference call to provide information regarding the incident and recovery activities.
 - Attendance at the conference call is optional and will be left to the discretion of the *MDM/R Service Recipient*.

- The purpose of the conference call will be to provide information to the *MDM/R Service Recipients*. We will not be seeking or accepting input from the *MDM/R Service Recipients* on recovery options at this call.
- The SME **WILL NOT** be initiating phone calls to individual contacts and/or *MDM/R Service Recipients*.

4.4.2 Identification of Recovery Point

Action

The OSP will perform an analysis to determine the Recovery Point (the last point in time of files that were successfully received and fully processed by the MDM/R). The OSP will analyze the last files received from each *MDM/R Service Recipient* to determine which files were processed prior to the MDM/R business interruption event (i.e. files that DO NOT have to be retransmitted by the *MDM/R Service Recipient*).

For synchronization file sets, the sequence number of the last successfully processed synchronization file set will be identified. Any subsequent file set that was sent by the *MDM/R Service Recipient* would need to be resubmitted once production operations have been reestablished, either at the primary or alternative site.

For meter read files, the OSP will attempt to identify the last successfully processed meter read file. However, this may not be possible depending upon when the MDM/R business interruption event occurred. If last successfully processed file cannot be identified, the OSP will identify the most recent insert date/time stamp for interval data for that *MDM/R Service Recipient*. If uncertainty remains over the processing status of a particular meter read file submitted by the *MDM/R Service Recipient* the file should be resubmitted.

For Billing Quantity Request files, the OSP will identify the filename of the last file received and processed.

Communication

- The SME will notify *MDM/R Service Recipients* with information recovery point information as outlined above by email to all contacts identified with an 'Incident and Notification' contact type.

4.4.3 Production Environment Recovery

Action

The OSP will proceed to re-establish a MDM/R Production environment, either at the primary or alternate site. Priority will be given to the restoration of the 'Critical Services' in the Production environment. Appendix 'A' identifies the category assigned to each service: critical; essential; or desired and the Recovery Time Objective (RTO) for each category of service. Where applicable, normal service levels targets for MDM/R services are set out in the *MDM/R Terms of Service*.

During this time, *MDM/R Service Recipients* are urged to perform an analysis of their individual Recovery Point using the information provided by the SME in section 4.4.2 above and their own internal information. This analysis will be used later when files transmission to the MDM/R resumes.

Communication

- The SME will undertake to update *MDM/R Service Recipients* on the status *MDM/R business interruption event* on an hourly basis by email to all contacts identified with a ‘Incident and Notification’ contact type.

4.4.4 Re-establishing AS2 Connectivity

Action

Once the OSP has re-established the MDM/R Production environment, the next priority will be to ensure that AS2 connectivity has been restored with all *MDM/R Service Recipients*.

The SME will confirm to all *MDM/R Service Recipients* that the MDM/R production environment is operational and that AS2 connectivity restoration activities have commenced.

NOTE: Once AS2 connectivity has been re-established, following the steps below, *MDM/R Service Recipients* are asked to refrain from transmitting their backlog of files until instructed to do so by the SME. The transmission of the backlog of files is discussed in section 4.4.5 below.

If the restoration of the MDM/R production environment involved transferring production operations to the alternate, or Disaster Recovery, environment the following actions apply:

- The SME/OSP will update the DNS mapping of the MDM/R production environment so that the existing DNS name will now point to the correct environment. *MDM/R Service Recipients* that have configured their AS2 client to use the MDM/R ‘DNS’ name for connecting to the MDM/R may not have any recovery actions at this point. The following notes apply to this scenario:
 - It may take a number of hours for the new DNS mapping to propagate through the internet and take effect.
 - Once the change has taken effect, *MDM/R Service Recipients* may have to restart their AS2 client to utilize the new DNS mapping. This step is dependent upon the *MDM/R Service Recipient’s* AS2 Client and its configuration. The configuration of the MDM/R’s AS2 software has no effect on whether the *MDM/R Service Recipient* is required to take this step and the SME/OSP does not have any ability to determine the need for this step on behalf of the *MDM/R Service Recipient*. *MDM/R Service Recipients* are urged to understand whether this step is required within their AS2 deployment at their site.
- *MDM/R Service Recipients* that have configured their AS2 client to use the actual IP address for the MDM/R Production environment will have to update the IP address within their AS2 client. Once the IP address has been updated, the *MDM/R Service Recipient* can test the connectivity by sending a ‘ping’ file (i.e. a file type ‘0000’ file). Receipt of a MDN from the MDM/R for this file is positive confirmation that connectivity has been reestablished. Lack of a MDN being returned should be identified to the SME via the communication channel identified in section 4.4.1 above.

Communication

- The SME will send an email to all contacts identified with a ‘Incident and Notification’ contact type confirming:
 - MDM/R production operations have been re-established and whether or not the environment is operating at normal Service Levels.

- The IP Address of the environment that is currently operating as the MDM/R Production environment.
- The SME will host a conference call to provide information regarding the incident and recovery activities.
 - Attendance at the conference call is optional and will be left to the discretion of the *MDM/R Service Recipient*.
 - The purpose of the conference call will be to provide information to the *MDM/R Service Recipients* and provide clarification to *MDM/R Service Recipients* where requested.

4.4.5 Processing File Backlog

Action

The SME/OSP will communicate to *MDM/R Service Recipients* when they can resume the transmission of files to the MDM/R. *Recipient*. *MDM/R Service Recipients* are requested to:

- Submit all files in the chronological order in which they were created and would have been processed by the MDM/R under normal circumstances.
- Where possible, refrain from submitting synchronization file sets during this period.

The OSP will monitor the incoming file volumes and may decide on the processing priority of the incoming files. The goal of the backlog processing will be to process files in the chronological order and priority, where possible, will be given to the oldest chronological files. Priority will be given by date and time of receipt, not by *MDM/R Service Recipient*. For example, the OSP will attempt to process meter read files for a meter read date of a 'Friday' for all *MDM/R Service Recipients* prior to processing meter read file for a meter read date of a 'Saturday'.

Communication

- The SME will send an email to all contacts identified with an 'Incident and Notification' contact type confirming when files may be transmitted to the MDM/R Production environment.

4.4.6 Resumption of Production Operations

Action

Once the backlog of files has been processed, the SME will communicate this to the *MDM/R Service Recipients* and confirm that the MDM/R Production environment is operating at normal service levels.

Once production operations has been stabilized, the OSP will and SME will proceed to process the backlog of files requiring processing. The SME will provide regular updates to the *MDM/R Service Recipients* on the status of the backlog processing.

Communication

- The SME will send an email to all contacts identified with an 'Incident and Notification' contact type confirming that all recovery activities have been completed.
- The SME will host a conference call to provide information regarding the incident and recovery activities.

- Attendance at the conference call is optional and will be left to the discretion of the *MDM/R Service Recipient*.
- The purpose of the conference call will be to provide information to the *MDM/R Service Recipients* and provide clarification to *MDM/R Service Recipients* where requested.

4.5 Restoration

Restoration in general terms: Restore or re-establish normal business operations at the primary site within one month of activation of the secondary (disaster recovery) , or an additional , second site identified that is capability of assuming primary or back-up responsibilities.

Depending on the nature of the *MDM/R business interruption event* restoring MDM/R operations to the MDM/R Production Environment may involve specific actions on the part of *MDM/R Service Recipients* and potentially a temporary loss of service depending on the nature of the original *MDM/R business interruption event* and the subsequent needs of the restoration process. Unless otherwise indicated by the SME, these actions will be communicated through the normal communications channels to your “incident and notifications” contacts as set out in the *MDM/R Incident Management Manual*. As part of this process, positive confirmation will be provided to confirm that operations of production operations at the primary or an alternate site have been restored. .

– End of Section –

5. Disruptions to SME Operations

5.1 Pre-Planning

The SME maintains its own internal Business Continuity Plan, which among other things, addresses situations in which a catastrophic incident renders the IESO's primary production facility unusable. In such situations, rapid evacuation of the facility may be necessary, and an orderly shutdown of business processes may not be possible. A core goal of the SME business continuity plan therefore, is to re-establish communications with *MDM/R Service Recipients* and the MDM/R OSP from its back-up operations centre as quickly as possible.

SME business continuity planning is separate and distinct from the operation of the MDM/R. The MDM/R itself, is located in a geographically distinct location separate from the SME facilities. Business continuity planning involving the MDM/R itself falls within the scope of section 4 of this document.

5.2 Initial Response

Once the SME re-established operations from its back-up operations centre, *MDM/R Service Recipients* will be notified through their duly registered "incident and notifications" contacts.

In addition, a broader emergency affecting the IESO's principal operations centre may trigger additional communications through the main IESO website (www.ieso.ca) and through communications channels governed by the *Ontario Electricity Emergency Plan* (IMO_PLAN_0002).

5.3 Recovery

As part of recovering SME support services from its back-up operations centre, the SME may designate new communications channels. In such cases *MDM/R Service Recipients* will be notified through their duly registered "incident and notifications" contacts.

SME services will be recovered from the back-up operations centre in the following order of priority:

1. MDM/R incident management processes
2. MDM/R change management processes
3. MDM/R registration and enrollment processes
4. All other SME business activities.

5.4 Restoration

Once the extent of the emergency situation is assessed the SME will make a more fulsome statement regarding the longer-term restoration of the various services it provides, be it from the restored principal operations centre or a new location.

– End of Section –

Appendix A: MDM/R Recovery Time Objectives

A.1 MDM/R Recovery Time Objectives

Table A-1 - Recovery Time Objective for MDM/R Services

Service Category	Recovery Time Objective (RTO)
Category I - Critical Services	<ul style="list-style-type: none"> Systems functioning within 3 to 6 hours of the declaration of a <i>MDM/R Business Interruption event</i>. All systems supporting these services will be receiving and processing real-time data in accordance with Service Levels within 24 hours.
Category II - Essential Services	<ul style="list-style-type: none"> All services in this category and systems supporting these services will be made available within 7 calendar days.
Category III - Desired Services	<ul style="list-style-type: none"> All services in this category and systems supporting these services will be made available within 30 calendar days.

A.2 Category I - Critical Services

- MSC1 - Automatic Meter Read processing and all its supporting services including the VEE Service.
- MCS2 - Automatic Billing Quantity processing and all supporting services.
- MSC3 - Automatic MMD processing (synchronization) and all supporting services.
- MSC4 - User Interface (GUI) and all supporting services.
- MSNC1 – Help Desk
- FTS – File Transfer Services Errors and Exceptions handling.

A.3 Category II - Essential Services

- MSNC2 - IVR Services
- Web Services
- LDC Enrollment Services

A.4 Category III - Desired Services

- Includes services supported outside of the production environment other than those noted in Category II.

– End of Section –

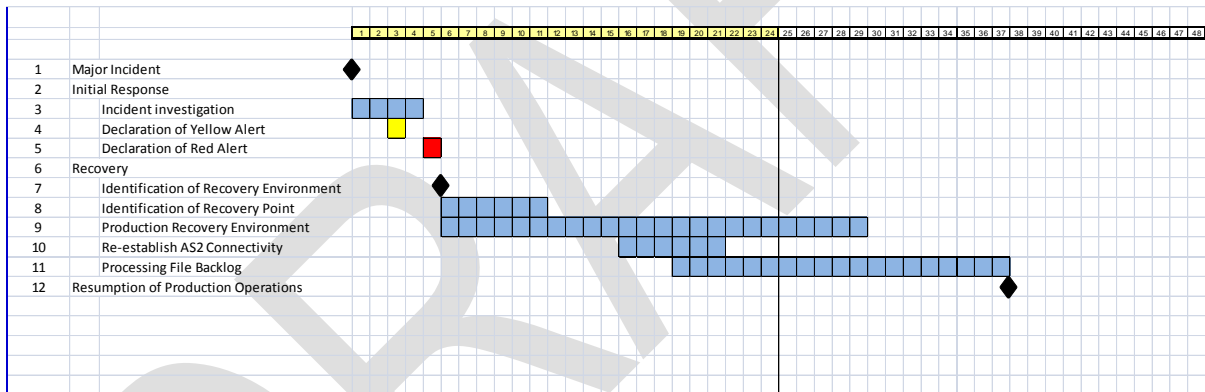
Appendix B:

This appendix provides potential scenarios resulting from a Major Incident. These scenarios provide forecasted timelines for a scenario where:

- The decision to failover to the Disaster Recovery site is made within 4 hours of occurrence of the Major Incident
- The decision to failover to the Disaster Recovery site is made within 24 hours of occurrence of the Major Incident, and
- The decision was made to restore production operations on the Primary site. Failover to the Disaster Recover site was not performed and recovery of the Primary site took 24 hours.

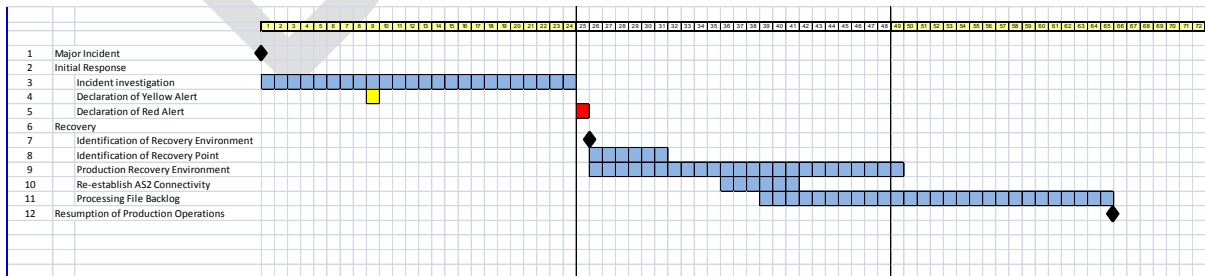
B.1 Scenario A

Loss of primary environment. The declaration of a red alert and the decision to failover to the Disaster Recovery environment was made 4 hours after the occurrence of the initial incident.



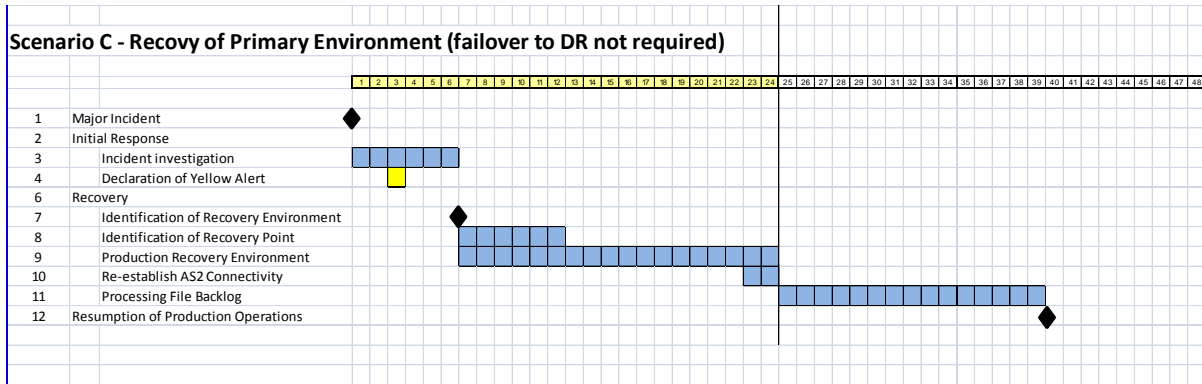
B.2 Scenario B

Loss of primary environment. The declaration of a red alert and the decision to failover to the Disaster Recovery environment was made 24 hours after the occurrence of the initial incident.



B.3 Scenario C

Major incident in the primary environment. The decision to recover the primary environment and not fail over to the Disaster Recovery environment was made 6 hours after the occurrence of the initial incident.



– End of Section –

References

Document Name	Document ID
<i>MDM/R Terms of Service</i> – NOT IN FORCE	SME_AGR_0002
<i>MDM/R Temporary Change Control Process</i>	SME_PRCs_0001
<i>MDM/R Change and Baseline Management Manual</i> – NOT IN FORCE	SME_MAN_0006
<i>MDM/R Incident Management Manual</i> – NOT IN FORCE	SME_MAN_0007
<i>Ontario Electricity Emergency Plan</i>	IMO_PLAN_0002
<i>SME-LDC Agreement</i> – NOT IN FORCE	SME_AGR_0001

– End of Document –