



Major Incident Management  
Process Guide  
Version 1.0

## Contents

## Contents

Contents .....	2
1. Document Information .....	4
1.1. Document Version Control .....	4
1.2. Assumptions .....	4
2. Introduction .....	4
2.1 Welcome .....	4
2.2 Target Audience .....	4
3. Process Key Concepts .....	5
3.1 What is an Incident? .....	5
3.2 What is a Major Incident? .....	5
3.3 Criteria for a Major Incident .....	5
4. Roles and Responsibilities .....	7
4.1 Major Incident Manager .....	7
Service Owner .....	7
Major Incident Response Team .....	7
Digital Innovation and Technology staff .....	7
Digital Innovation and Technology Management .....	8
ITSM Team .....	8
RACI .....	<b>Error! Bookmark not defined.</b>
5. Major Incident Process .....	9
Major Incident Process Flow .....	9
5.1 Potential Major Incident Identified .....	10
5.2 Validate and Declare Major Incident .....	10
5.3 Issue Communication .....	10
5.4 Assemble Major Incident Response Team .....	11
5.5 Develop Resolution Plan .....	11
5.6 Resolve Major Incident .....	12
5.7 Issue Communications .....	13
5.8 Monitor Status .....	13
5.9 Escalate to Senior Management, Vendors and Senior Resources .....	14

5.10 Major Incident Review ..... 14

5.11 Close Major Incident ..... 15

# 1. Document Information

## 1.1. Document Version Control

Version	Changes	Author	Date
0.1	Draft	Erin Tramble	July 20, 2018
1.0	Published	Erin Tramble	

## 1.2. Assumptions

Readers should be familiar with the ITIL® V3/2011 ITSM best practice framework and have basic process terminology knowledge.

# 2. Introduction

## 2.1 Welcome

Thank you for participating in the NSCC Major Incident (MI) process. By participating you are taking an active role in transforming Digital Innovation and Technology into a service-focused organization.

The MI Process brings extra-ordinary resources to bear to return an affected IT service to its normal operational state as quickly as possible.

This document is designed to provide an overview of:

- The MI process
- The responsibilities of the stakeholders

The most up to date version of this document can be found in the Knowledge Base of Technology Service Desk, along with the most recent versions of supplemental documentation.

This process is subject to continual service improvement, as are all Service Management processes. If you have suggestions for improvements please log a Service Request in Technology Service Request under Tech to Tech > Technology Service Desk > [Get assistance with Technology Service Desk](#).

## 2.2 Target Audience

This document is targeted at all members of the Digital Innovation & Technology team who may be called upon to take part resolving in a Major Incident.

All members of the Digital Innovation & Technology team who may be involved in resolving a Major Incident should ensure that they have copies of all MI documentation and supplementary information available in the event that access is lost to Technology Service Desk where the documents are hosted.

Individuals should have PDF copies stored in a location that is accessible regardless of the state of the NSCC network. A hard copy will be stored with the Manager, Digital Innovation & Technology for use in the event of a complete NSCC infrastructure failure.

### 3. Process Key Concepts

#### 3.1 What is an Incident?

An **Incident** is an unplanned interruption to an IT service or reduction in the quality of an IT service.

The purpose of **Incident Management** is to repair IT System/Application issues and return to normal business operations as quickly as possible by repairing the issue, or alternatively, by implementing an acceptable work around that restores normal operations.

Major Incidents are predicated by the scale/scope/impact of the Incident.

#### 3.2 What is a Major Incident?

A **Major Incident (MI)** is an incident that has a significant impact to users and essential services where there is no workaround to enable the return to business operations.

Major Incidents include situations where there is a degradation of a service including data, applications or infrastructure.

Note: An Emergency change that requires an outage that impacts an essential service with no workaround will be considered a Major Incident.

A Major Incident requires immediate, continuous action to restore the affected service.

The declaration of a Major Incident does not override the processes used for the resolution of an Incident; however, it does bring a requirement for a higher level of visibility and documentation.

By consistently employing a common process throughout NSCC, we can ensure Major Incidents are quickly identified and appropriately acted on.

#### 3.3 Criteria for a Major Incident

**Major Incidents** are incidents that have a high impact on the business and have a high urgency to resolve.

Prior to declaring a Major Incident, the Service Criticality spreadsheet should be consulted to ensure that the Service is eligible for Major Incident Management.

The Service Criticality spreadsheet is located in the Technology Service Desk Knowledge Base.

A Major Incident is declared when:

- NSCC students, staff or faculty are directly impacted and unable to work or access DigIT services.
- The loss of one or more DigIT Business Services has or has the potential to have a significant or extensive impact on College operations. (Business users cannot perform business functions.)
- Loss of one or more DigIT Business or Technical Services results in an incident having a critical urgency.

**Priority** is the category used to identify the relative importance of an incident. Priority is based on impact and urgency, and is used to identify required times for actions to be taken

**Impact** is the measure of the effect of an incident on business operations.

Impact is determined by the following criteria:

- 1 – Significant percentage of users impacted
- 2 – Some, but not a significant percentage of users are impacted
- 3 – Low percentage of users impacted

**Urgency** is the measure of how long it will be until an incident has a significant impact on business operations.

Urgency is determined by the following criteria:

**High** – Ability to work is blocked or delivery of service is unavailable to students, faculty and/or staff.

**Medium** – Ability to work is degraded

**Low** – Impact to ability to work is minimal

Priority is calculated as follows:

Impact				
Urgency		1 Significant % of users impacted	2 Some, but not a significant % of users are impacted	3 Low % of users impacted
	<b>High</b> – Ability to work is blocked or delivery of service is unavailable to students, faculty and/or staff.	Critical	High	Medium
	<b>Medium</b> – Ability to work is degraded	High	Medium	Medium
	<b>Low</b> – Impact to ability to work is minimal	Medium	Medium	Low

## 4. Roles and Responsibilities

### 4.1 Major Incident Manager

- Typically, the Manager responsible for service or application encountering issue, or their designate.
  - May also be the Service Owner, Project Manager, Core Services Team member, Campus Lead, or any other member of the Digital Innovation and Technology team designated by the owner.
- Determines if incident meets Major incident criteria.
- Determines members of MI Response team.
- Establishes communication method for MI Response Team call. This method may include Teams, Skype, email, telephone conference bridge or other available method.
- Chairs MI call/chat.
- Records chronology of events.
- Composes communication updates for stakeholders and directs ITSM team to send to appropriate distribution lists and methods.
- Logs additional Incidents, Service Requests and Requests for Change as necessary
- Chairs Post-Incident Review meeting and determines invitees.
- Publishes Major Incident Review document no later than one week after the MI has been stood down.

### Service Owner

- Ensure contact information for support groups, vendor groups and business owners is up to date and available.
- Engages additional support resources and vendor resources as required.

### Major Incident Response Team

- Includes members of various Digital Innovation and Technology and vendor teams who usually assist in determining that an MI should be declared.
- Determine the impact to the business and identify other responders who need to be involved in the MI.
- Participate in MI Response Team call/chats.
- Help develop the Resolution plan
- Responsible for performing and reporting on analysis and resolution tasks assigned to them.
- Complete monitoring tasks as required.

### Digital Innovation and Technology staff

- Participate as a member of the Major Incident Response team as required to do so by the MI Manager or Service Owner.
- Provide support to the MI Response Team as needed.

## Digital Innovation and Technology Management

- Contact point for Senior and Executive Leadership Team.
- Advises and assist the IT teams as necessary (with escalations, etc.).

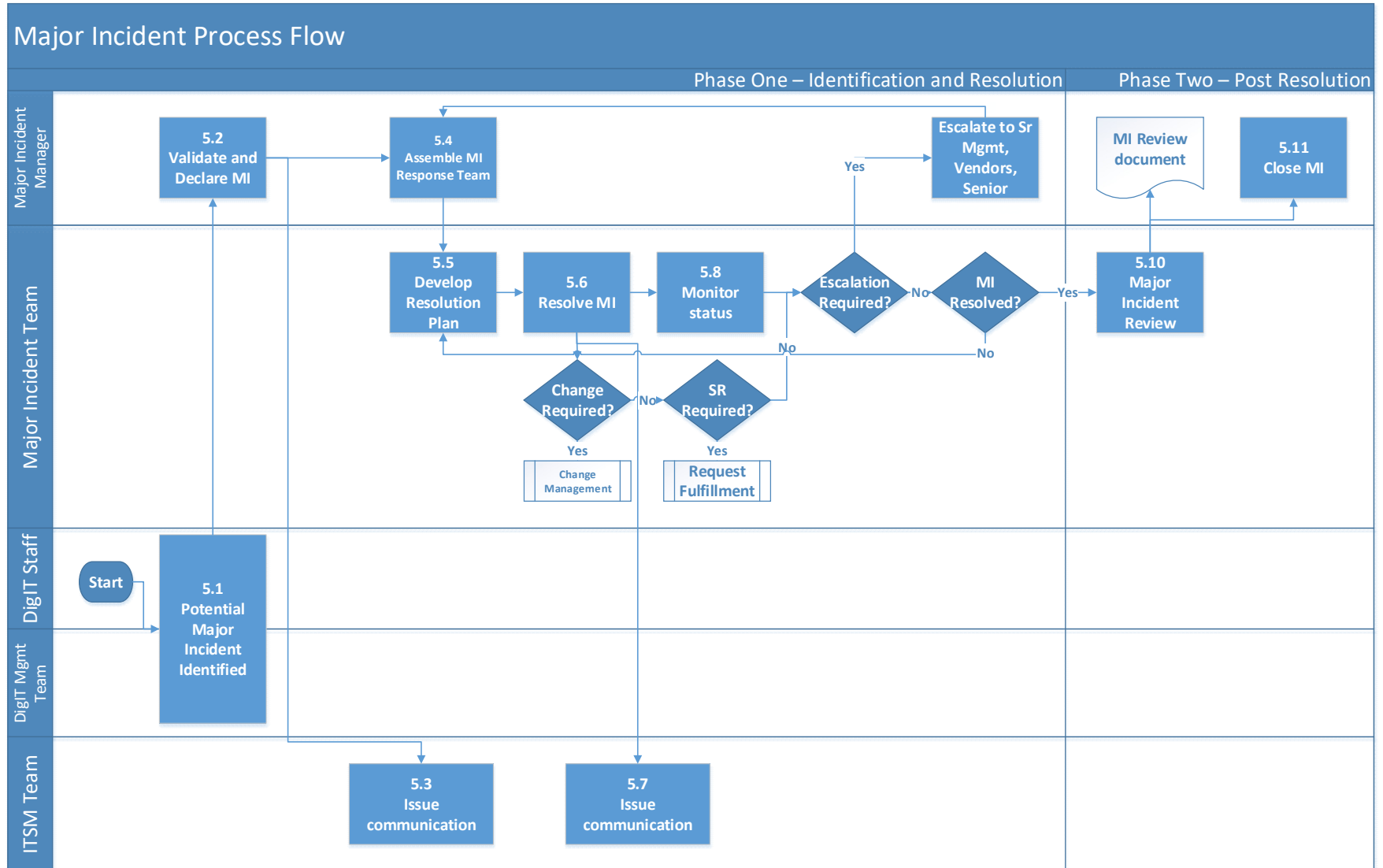
## ITSM Team

- Sends communications as required or requested by Major Incident Team.
- Participates in the MI Response Team call as required.



## 5. Major Incident Process

### Major Incident Process Flow



## 5.1 Potential Major Incident Identified

### Purpose

A potential Major Incident is identified

- when a user is impacted and contacts Digital Innovation and Technology via Technology Service Desk self-service, phone, email, or a direct visit.
- Operational monitoring of key infrastructure and components indicates a degradation or failure of a critical service, or the impending degradation or failure of a critical service.

### Roles Engaged:

- Digital Innovation and Technology Staff
- Digital Innovation and Technology Management

## 5.2 Validate and Declare Major Incident

### Purpose

- Efficient and effective determination of an event that requires major incident communication and coordination.

### Inputs

- Incidents requiring enhanced resolution and communication methods.
- Reports or monitors from Core Services to indicate a possible Major Incident.

### Tasks

- **Identify the Major Incident:** Major Incident Manager reviews potential Major Incident to determine if it meets MI criteria.
- **Select the Major Incident** - Create a Major incident from an existing incident.
  - Create a Major incident from an existing incident and add other incidents to it using Link functionality.

### Roles Engaged

- Major Incident Manager

## 5.3 Issue Communication

### Purpose

Advise impacted users of service degradation or unavailability.

### Inputs

- Information and data gathered from Step 5.3 - Assemble Major Incident Response Team
- Communication Plan

### Tasks

- Create initial communication
- Determine notification schedule
- Determine notification method(s) – Email, Twitter, etc
- Send communication

### **Roles Required**

- Major Incident Manager
- ITSM Team

## **5.4 Assemble Major Incident Response Team**

### **Purpose**

- Assemble the appropriate team to resolve the Major Incident.

### **Inputs:**

- Major Incident Manager
- Major Incident Event information
- On call and support schedules
- Additional SME and resource information from Digital Innovation and Technology Management.

### **Tasks**

- Determine who should be part of the team
- Determine communication methods needed for the team depending on situation (Teams chat, Teams Call, Skype Call, Telecommunications conference bridge, Email distribution, in-person, etc.)
- Debrief on situation
- Discuss possible causes, impacts, responses, solutions, communication
- Define Roles
- Gather information for the Resolution Plan

### **Roles required and descriptions**

- Major Incident Manager
- Digital Innovation and Technology Management
- Digital Innovation and Technology Staff
- ITSM Team
- Vendors (if required)

## **5.5 Develop Resolution Plan**

### **Purpose**

To establish a “Plan of Action” to respond to the Major Incident

## **Inputs**

- Information and data gathered from Step 5.3 - Assemble Major Incident Response Team

## **Tasks**

- Establish tasks to investigate and resolve Major Incident Event
- Assign tasks to assembled team
- Update the Major Incident Event

## **Roles required and descriptions**

- Major Incident Manager
- Major Incident Response Team

## **5.6 Resolve Major Incident**

### **Purpose**

To resolve the Major Incident

### **Input**

- Major Incident Event
- Major Incident resolution plan – created in Step 5.5 – Develop Resolution Plan
- Communication Plan (for updates)

### **Tasks**

- Major Incident team members will update the Major Incident event as progress is made.
- Major Incident Manager is responsible for regular updates to the Major Incident Event and communication updates.
- Major Incident Manager will escalate the Major Incident as required, to appropriate management levels or suppliers to ensure the Major Incident can be resolved as quickly as possible.
- Submit an RFC through the Change Management process (if required)
- Submit Service Requests (if required)
- Update Knowledge Base if a workaround is available for use (if required).
- Close events associated with the Major Incident (if required).

### **Decisions**

- Major Incident Manager needs to decide if the suggested resolution is acceptable and successful.
- If resolution is successful and acceptable, then update the status of the Major Incident to Resolved.

### **Roles required and descriptions**

- Major Incident Manager
- Major Incident Response Team

## 5.7 Issue Communications

### Purpose

To ensure that the Major Incident stakeholders are kept informed of the status of the incident through the complete Major Incident life cycle from open to close, and to ensure proactive response as quickly as possible.

### Inputs

- Major Incident event details.
- Stakeholder lists
- Impact assessment to determine communication channels to use.

### Tasks

- Issue communications identified in previous process tasks to stakeholders outlining necessary information for each audience.
- Communications are initiated in various stages of the Major Incident Process
  - Discovery and Creation of Major Incident
  - On updates and changes of status.
  - Resolution of Major Incident
  - Post Major Incident review

### Roles required and descriptions

- Major Incident Manager – Coordinates and determines communication path
- Major Incident Response Team:
  - SME and team leads (working the incident) – Responsible to communicate and update the incident and Major Incident Manager.
- ITSM Team – Responsible for formal communications

## 5.8 Monitor Status

### Purpose

To ensure that the Major Incident is being worked on or has been resolved.

### Inputs

- Major Incident event information
- Major Incident Resolution Plan

### Tasks

- Check progress against Resolution Plan
- Identify additional required resources
- Escalate if:
  - Priority increases
  - Resolution is not progressing

### **Roles required and descriptions**

- Major Incident Manager
- Major Incident Response Team

## **5.9 Escalate to Senior Management, Vendors and Senior Resources**

### **Purpose**

To add additional resources and communicate that the current resolution plan is not progressing as planned.

### **Input**

- Major Incident event information
- Resolution Plan

### **Tasks**

- Contact Escalation resource (Senior Management, Team Leads, Executive Team, Business Liaison, Etc)

### **Roles required and descriptions**

- Major Incident Manager
- Digital Innovation and Technology Managers
- Vendors

## **5.10 Major Incident Review**

### **Purpose**

To provide information that will allow improvement in the Major Incident Process and to improve Service Delivery.

### **Input**

- In scope Major Incident event
- Major Incident Resolution Plan
- Communication Plan
- Team member feedback

## **Tasks**

- When the resolution of a Major Incident has been implemented, it is the responsibility of the Major Incident Coordinator to ensure that a Major Incident Review is performed.
- The Major Incident Review will include the completion and review of the Major Incident Review document, which includes:
  - Incident Information, including related incidents, incident create time and incident resolve time.
  - MI Overview
  - Impact, including End User Impact and Severely Impacted Services
  - Incident Timeline
  - Customer Communications
  - Root Cause
  - Lessons Learned
  - Corrective Actions
  - Related Incidents, Problems and/or Changes
- Send review to IT Management for approval.
- Post the complete Major Incident Review document in the Knowledge Base of Technology Service Desk.

## **Roles required and descriptions**

- Major Incident Manager
- Major Incident Response Team
- Digital Innovation and Technology Managers and Leads

### **5.11 Close Major Incident**

## **Purpose**

- To ensure that a Major Incident is assessed and completed as required.

## **Input**

- Updated Major Incident event.

## **Tasks**

- Review the Major Incident event. Check for completeness.
- Close the Major Incident with cause.
- Close all related incidents.

## **Roles required and descriptions**

- Major Incident Manager