Business Continuity/ Disaster Recovery Program

Disaster Recovery Plan

Township of Scugog

Contents

Document Control	
Document creation and edit records should be maintained by the Township of Scugog recovery coordination (or equivalent) or business continuity manager (or equivalent)	
Document Name	Disaster Recovery Plan
Version	V1.0
Date Created	October, 2022
Date Last Modified	
Last Modified By	

Document Change History

Version	Date	Description	Approval

REPORT SUMMARY

This report delineates Township of Scugog "Township" policies and procedures for technology disaster recovery, as well as the process- level plans for recovery critical technology platforms and the telecommunications infrastructure. This report summarizes the recommended procedures that will underpin the Township's business continuity strategy. In the event of an actual emergency situation, modifications to the processes outlined in the report may be made to ensure physical safety of staff, systems, and digital assets.

The scope of this report includes the Township's IT service continuity strategy; a subset of business continuity management (BCM). Often referred to as Disaster Recovery "DR", IT service continuity management "ITSCM" is focused on planning for the restoration of IT-based services and technologies. ITSCM addresses the gaps in the traditional disaster recovery approach by introducing layers of resilience that provide higher levels of protection. This layering is realized by using technologies that are readily available such as virtualization and high availability fail over. This approach aligns with [1]ITIL best practices.

Methodology

Perry Group Consulting "PGC" developed the Township's strategy using a Business Continuity Management (BCM) framework based on best practices from the Disaster Recovery Institute International (DRII). PGC places a clear distinction between IT Service Continuity Management (ITSCM), and the requirements for the Township to establish a sound BCM strategy that addresses the following key areas:

1. BCM Framework Definition – initiation, roles, policy
2. Impact Analysis & Risk Identification – Business Impact Analysis "BIA", Risk Assessment "RA", [2]Recovery Time Objectives "RTO", and [3]Recovery Point Objectives "RPO"
3. Design & Delivery – recovery, strategy, plans (crisis, emergency, communication)
4. Testing & Maintenance – plan, test, review

The project was launched in May, 2022 with the development of a BIA questionnaire that was distributed to selected departments within the Township. The questionnaire was used to identify services within each department along with the criticality of each service:

1. Community Services
2. Corporate Services
3. Development Services
4. Finance
5. Fire & Emergency Services
6. Public Works & Infrastructure Services
7. By-Law
8. Building
9. Administration

[1] *IT Service Continuity Management (ITSCM)* aims to manage risks that could seriously impact IT services, ensuring that the IT service provider can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.

[2] RTO defines the impact on Township services in the event of a disruption coupled with the required recovery time expectations expressed in hours/days/weeks.

[3] RPO defines the Townships tolerance for data loss as expressed in hours/days/weeks.

The Information Technology “IT” team were engaged to help define a catalogue of IT services that were then mapped to all services defined by the business units.

Risk Assessment

A risk assessment was performed to identify threats and risks that could impact the delivery of Township services. The results of the assessment were then uploaded to a risk register that will be used by the IT team to track and manage all risks identified in the report.

Online Dashboard

All components of the Township’s BCP/DR strategy have been uploaded to a secure dashboard that will allow the IT team to manage the lifecycle of the BCP/DR program. All modifications to Township services, including changed in technology, will be updated in “real-time” within the dashboard.

This process will support the Township’s desire to have a current, always validated BCP/DR program. Historically, BCP/DR documents can quickly become outdated and ineffective to organizations. The process adopted by the Township will mitigate the risk of stale information and ensure the Township’s BCP/DR posture is aligned with the DRII best practices.

Program Benefits

- **Roadmap:** A well-defined business continuity plan is like a roadmap during a disruption. It allows the Township to react swiftly and effectively and maintain continuity of core services.
- **Build Confidence with the Public and Township Employees:** A great benefit of a business continuity plan is that it can give both employees and the public the needed assurance on the capability of the Township to deliver services in times of disaster.
- **Avoid Excessive Downtime:** Cyber-attacks are common within municipalities. These attacks often lead to data breaches, data loss, or infection that can cause many problems to the daily operations.

Summary

Initiating the BCP/DR program has positioned the Township as a municipal leader in business continuity disaster recovery planning. The program will support cybersecurity initiatives and risk management processes.

Next steps within the BCP/DR program throughout 2022 and beyond will include:

- **Validate all Service Recovery Times:** The Township will review all services and validate recovery times.
- **Develop Tabletop Exercises:** A schedule will be developed to initiate annual tabletop exercises.
- **Develop an IT Recovery Plan:** Based on the business recovery time objectives, IT will implement a technical solution to provide redundancy in the event of a disruption in IT services.
- **Develop Recovery Playbooks:** IT will start the process of creating recovery playbooks to be used in the event of a disruption.

TERMS AND DEFINITIONS

Term	Definition
Alternate Site	A site held in readiness for use during/following an invocation of business or disaster recovery plans to continue urgent and important activities of an organization.
Application Recovery	The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.
Business Continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level. The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Business Impact Analysis (BIA)	Process of analyzing activities and the effect that a business disruption might have on them.
Business Interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization's location.
Call Tree	A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.
Crisis Management	The overall direction of an organization's response to a disruptive event; in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate. Development and application of the organizational capability to deal with a crisis.
Crisis Management Team	Crisis Management will protect the Board against situations that may have a negative effect on business operations and reputation (part of business continuity management). The Crisis Management Team would typically be led by senior leadership with authority to invoke the IT disaster recovery plan and/or business continuity plans.

Datacenter Recovery	The component of disaster recovery which deals with the restoration of datacenter services and computer processing capabilities at an alternate location and the migration back to the production site.

Term	Definition
Declaration (DR)	A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged response and mitigating actions.
Disaster Declaration	The staff should be familiar with the list of assessment criteria of an incident versus disaster situation established by the BCM or DR Steering Committee and the notification procedure when a disaster occurs.
Disaster Recovery Plan (DRP)	The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort.
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. The facility used by the Incident or Crisis Management Team after the first phase of a plan invocation. An organization must have a primary and secondary location for an EOC in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts
Incident	An event which is not part of standard business operations which may impact or interrupt services and, in some cases, may lead to disaster. Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
Incident Management Team (IM)	Comprises management, technical and other support staff who will be responsible for notification of all relevant staff, activation of recovery services provided by third party organizations and establishing operational capability at the Township administration building. The team is also responsible for the overall management of recovery activities.
Incident Response Team (IRT)	As it relates to technology, Incident response relies on the IT Department personnel and decisions/ classification capabilities defined by Incident Management. A decision must be made to decide if ITSCM contingencies and capabilities should be used, and when the trigger should be pulled after a disruption (based on senior management decisions).
ITIL	A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.
IT Service Continuity Management (ITSCM)	Aims to manage risks that could seriously impact IT services. This is an ITIL process that ensures the IT service provider(s) can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.
Maximum Tolerable Downtime (MTD)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable
Qualitative Risk Assessment	The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories (e.g., customer service, regulatory requirements)

Quantitative Risk Assessment	The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values

Term	Definition
Recovery Point Objective	The point in time to which data is restored and/or systems are recovered after an outage. The point to which information used by an activity must be restored to enable the activity to operate on resumption.
Recovery Time Objective	The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. The period of time following an incident within which a product or service or an activity must be resumed, or resources must be recovered.
Risk Acceptance	A management decision to take no action to mitigate the impact of a particular risk.
Risk Analysis	The quantification of threats to an organization and the probability of them being realized.
Risk Appetite	Total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	Overall process of risk identification, risk analysis, and risk evaluation.
Risk Mitigation	Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner. Activities taken to reduce the severity or consequences of an emergency.
Risk Register	All risks of an organization, listed, ranked and categorized so that appropriate treatments can be assigned to them.
Single Point of Failure	A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative, and a loss of that element could lead to a failure of a critical function. Unique (single) source or pathway of a service, activity and/or process; typically, there is no alternative, and loss of that element could lead to total failure of a mission critical activity and/or dependency.
Tabletop Exercise	Technique for rehearsing teams in which participants review and discuss the actions they would take according to their plans, but do not perform any of these actions.
Vital Records	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

INTRODUCTION

Emergency preparedness, business continuity, crisis response, disaster recovery: These and other related terms are often discussed as if they are synonyms that all refer to the process of responding to and mitigating a crisis event. However, they provide very different business functions and it is particularly important for the Township of Scugog Township to document and communicate the differences between emergency preparedness and business continuity throughout the organization in order to establish correct accountability for each discipline.

A clear distinction should be made between emergencies, crises, and disasters in order to develop and provide appropriate response plans. However, what may begin as a small routine emergency may turn into a major crisis or a major disaster. Conversely, not all emergencies end up being a crisis. It would all depend on the timing, nature and surrounding context of the event.

Emergency Preparedness: typically involves directing people and resources away from danger, holding emergency drills and training sessions, evacuating facilities and working with first responders to ensure the health and safety of all stakeholders.

Business Continuity: involves protecting the business' reputation, establishing and maintaining redundant systems and support teams, restoring IT systems and ensuring employees are able to return to their daily work tasks following an emergency.

Of course, despite the differences between emergency management and business continuity, in the end these two distinct departments are both working toward the same objective: to help ensure the success of the business.

The scope of this document pertains to the Township IT service continuity strategy; a subset of business continuity management (BCM). Often referred to as "DR", IT service contunity management "ITSCM" is focused on planning for the restoration of IT-based services and technologies. ITSCM addresses the gaps in the traditional disaster recovery approach by introducing layers of resilience that provide higher levels of protection. This layering is realized by using technologies that are readily available such as virtualization and high availability fail over. This approach aligns with ITIL best practices.

Aligning ITIL processes to the Township's DR plan will lead to more efficient and effective use of IT infrastructure. Inadequate planning is a risk to the business and is often overlooked until it is too late, when a crisis event such as a major infrastructure outage, security or other breach results in the loss of supporting IT systems.

Recovery options need to be considered for IT systems and networks, and critical services such as Telecommunications, Internet and power. The various recovery options are as follows:

- **Do nothing** - However, few organizations can afford to forgo all business activities supported by IT services and simply wait until services are restored.
- **Manual system** - For businesses without a large number of critical IT services, manual workarounds may present a feasible option until IT services can resume.
- **Reciprocal arrangement** - This option involves forming an arrangement with another company that uses similar technology.
- **Gradual recovery** - This option is often chosen by organizations that have certain business services supported by IT that are not required for 72 hours or longer.

- **Warm start** - This is an option used by organizations that need to recover IT services and facilities within a 24- to 72-hour period. To accomplish this, organizations often use commercial facilities that include operations, system management, and technical support.
- **Hot start** - This is also known as an immediate recovery. This option is used for critical services that cannot be down for any length of time. A hot start provides for immediate restoration of IT services. It is also one of the most expensive options to implement.

Common problems associated with ITSCM are issues that prevent an organization from committing to continuity management - in terms of both implementing the process and maintaining it. One example is when organizations seem unable to move out of the planning stage and into actual implementation.

Other examples are being unable to find facilities or resources, having someone unfamiliar with the business implement the process, not understanding ITSCM's role in disaster recovery, or thinking IT has already handled continuity planning.

Common costs associated with ITSCM are the expenses incurred from risk management and recovery arrangements. An example of a common cost is the investment required by the introduction of risk management.

Additional examples of common costs are returning operational costs and the hardware needed to support the ITSCM process, and fees for the recovery facility. There will always be problems and costs associated with implementing ITSCM. But the resulting benefits, especially when a disaster is prevented or quickly controlled, outweigh the associated difficulties and costs.

This document provides policies and guidance to be used by the Township's IT department to carry out responsibilities under ITSCM for information systems security and availability regarding system contingency plans and recovery after a disruption or disaster.

This document also references departmental business continuity plans which are the responsibility of each department identified in the Business Impact Analysis (BIA). Please refer to section Departmental Business Continuity Planning for further details.

STATEMENT OF INTENT

This document delineates Township of Scugog "Township" policies and procedures for technology disaster recovery, as well as the process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes the recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our staff, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity for the Township.

POLICY STATEMENT

- The Township shall develop a comprehensive IT disaster recovery plan which will be stored in the BCP/DR online portal;
- An updated risk assessment shall be undertaken to determine the requirements for the disaster recovery plan;
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities;
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed;
- All staff must be made aware of the disaster recovery plan and their own respective roles; and
- The disaster recovery plan is to be kept up to date to take into account changing circumstances including core services, recovery time objectives, business applications, and all supporting information technology.

OBJECTIVES

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the Township recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

1. The need to ensure that all staff fully understand their duties in implementing such a plan;
2. The need to ensure that operational policies are adhered to within all planned activities;
3. The need to ensure that proposed contingency arrangements are cost-effective;
4. The need to consider implications on other Township sites; and
5. Disaster recovery capabilities as applicable to key customers, vendors, and others.

DISASTER RECOVERY PLAN OVERVIEW

No DR initiative can ever work without people. Township staff will constitute part of the resources and capabilities required to deliver a quality recovery strategy to users and customer alike. And since quality service delivery is all about dealing with customers, users and suppliers, the value of instituting proper roles and responsibilities in within the DRP cannot be understated.

Since Disaster Recovery falls within the scope of Business Continuity Management (BCM) it is important to highlight the keys areas of disciple that require well-define roles and responsibilities. Depending on the size of an organization, the number and size of these teams will vary.

The primary objective of this document is to address the need to develop a disaster recovery team structure as highlighted in red in *figure1,* however ancillary teams to support incident management, crisis management, and business continuity will be covered at a high-level.

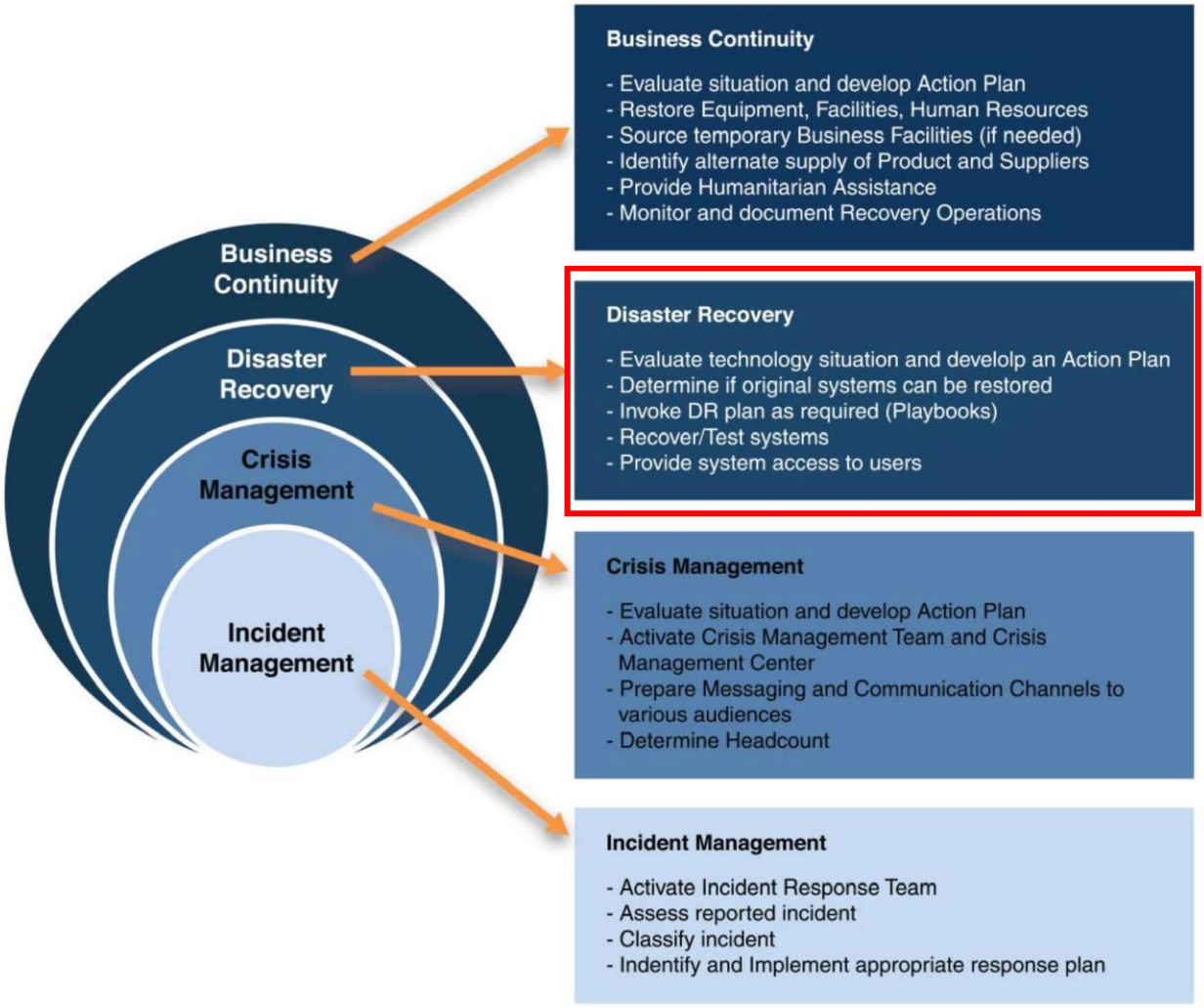


Figure 1 - Business Continuity Management

CRISIS MANAGEMENT TEAM (CMT)

Decision making falls under the purview of the crisis management team (CMT). They are responsible for optimizing the use of assets and resources as well as monitoring the effectiveness of BCP/DR plans. Besides initiating, executing, and maintaining business continuity and disaster recovery plans, the CMT also has the authority to modify plans to adapt responses to specific scenarios.

The CMT should have five or seven members: there cannot be any “split-votes” in a crisis. Every division or business line does not need to be represented. The CMT should include decision-makers with a broad perspective on the business priorities. At a minimum the CMT should include representatives from information technology, human resources, and facilities.

Crisis Management will protect the Township against situations that may have a negative effect on business operations and reputation (part of business continuity management).

The CMT will be led by senior leadership with authority to invoke the IT disaster recovery plan and/or business continuity plans.

Note: Emergency Management (life safety) and Business Continuity (continuity of business operations) are two distinct disciplines that operate as separate groups although the emergency management team would report to the crisis management team if there was a "crisis".

Crisis Management Team

Name, Title	Contact Option	Contact Information
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	

IT Disaster Recovery Team & Business Recovery Team

At a minimum a DR coordinator should be in place and responsible for:

- establishing ITSC plans to provide agreed-on levels of service within agreed timelines following a disruption/disaster;
- ensuring that IT service areas are able to respond to an invocation of the continuity plans;
- maintaining a comprehensive IT testing schedule and undertaking regular reviews; and
- selecting the appropriate business recovery team(s) at time of disruption/disaster to assist in the recovery/testing of critical business applications.

Additional roles will include recovery team members from the infrastructure team to cover the network, servers, storage, databases, and telecommunications.

Disaster Recovery Team

Name, Title	Contact Option	Contact Information
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	

INTERNAL CONTACT LIST

Internal Contact List

Name, Title, Department	Contact Option	Contact Information
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	

VENDOR CONTACT LIST

Vendor Contact List

Name, Title, Department	Contact Option	Contact Information
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	
	Mobile: Email: Alternate email:	

Departmental Business Continuity Planning

Business continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business Continuity Management further defines business continuity as the development of strategies, plans, and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

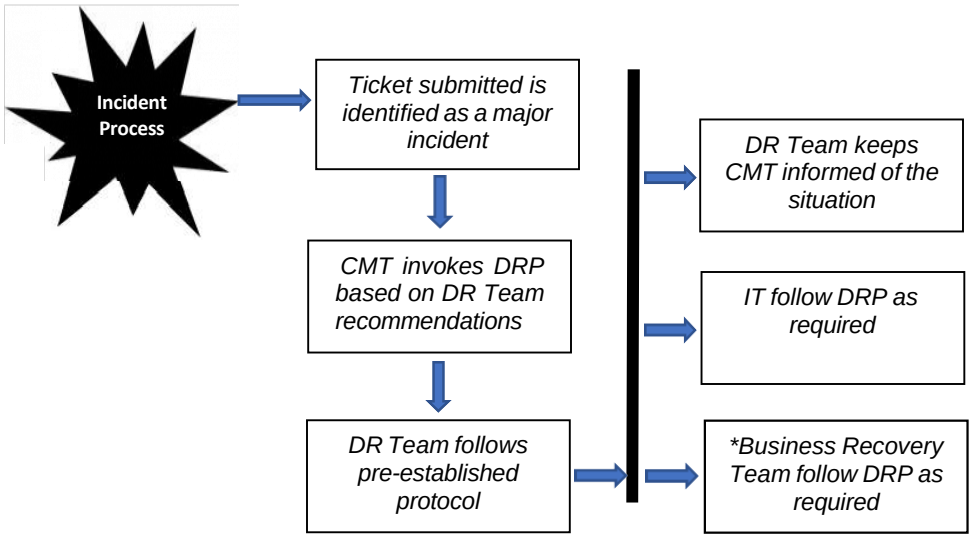
The Township has developed a **Departmental Business Continuity** framework which is mandatory throughout the organization. Every business unit, regardless of size, is expected to comply with its provisions. Each business unit needs to identify its key products and services within the scope of its business continuity management capability.

Departmental BCP forms have been provided to all departments by IT for completion. IT has uploaded the first draft of the forms to an online BCP portal as part of the BCM program. Updates, and necessary revisions, are to be emailed to designated IT staff in order to ensure all BCP information in the portal is current and has been validated.

Business Continuity Plans will be tested at least annually through a tabletop exercise program defined in the BCP/DR online portal.

Notification Call Tree

All incidents should be reported to the IT helpdesk as outlined in the Township's Helpdesk Standard Operating Procedure. The following call tree will be used to coordinate system recovery:



Please refer to Appendix A IT Incident Process Flow for a complete overview of the incident process flow.

PLAN ACTIVATION STEPS

- The CMT are responsible for invoking the DRP once they have consulted with the Disaster Recovery Team (DRT)
- In the event that the primary administration building cannot be occupied the follow location will be used as an alternate facility:
    - *INSERT ALTERNATE FACILITY (TBD)*
- The DRT will refer to **Appendix B - Disaster Recovery Plan Activation Form** this form contains up to date activation steps to be followed by the DRT.
- The DRT will refer to all required **System Recovery Playbooks** to be located within the BCP/DR portal at time of disruption (TOD).
- The DRT will complete **Appendix C- Disaster Recovery Event Recording Form** this form is to be completed by the disaster recovery team leader once the infrastructure has been recovered and core applications are available to end users.
- A copy of **Appendix D- Business Resumption Form (Application Recovery)** should be completed with sign-off by the business recovery lead and the designated lead for each department for all applications recovered during the disruption.

INFRASTRUCTURE OVERVIEW

IT CRITICAL ASSET LIST

IT assets are considered " critical" if they are supporting the delivery of Tier 1-3 services/processes. The following list (*Table 1)* has been identified through the BIA process:

Table 1 - Critical IT Asset List

Township of Scugog: Critical IT Asset List
This list captures all IT assets required to support business processes/services with recovery time objective (RTO) ranging from 0-3 days.

Asset	Type/Sub-Type	Location	Description/Notes

DATACENTER ACCESS CONTROL

Maintain an up-to-date access control list (ACL) specifying who, within the Township and any service partners, has access to the datacenter and resources herein (*Table 2*).

Be sure to specify which individuals can introduce guests to the datacenter. This is required for determining, in the event of an emergency, who may be the designated point person for facilitating access to critical infrastructure. During a recovery event, the primary operations team will be involved in system recovery, making contact and datacenter access information critical to the success of the recovery process.

Table 2 - Datacenter Access Control List

Datacenter Access Control List			
Name	Role	Contact Info	Access Level

BACKUP AND RECOVERY PROCEDURES

IT System Backup Procedures			
Backups for systems are listed in the following schedule:			
System	Frequency	Responsibility	Description/Notes