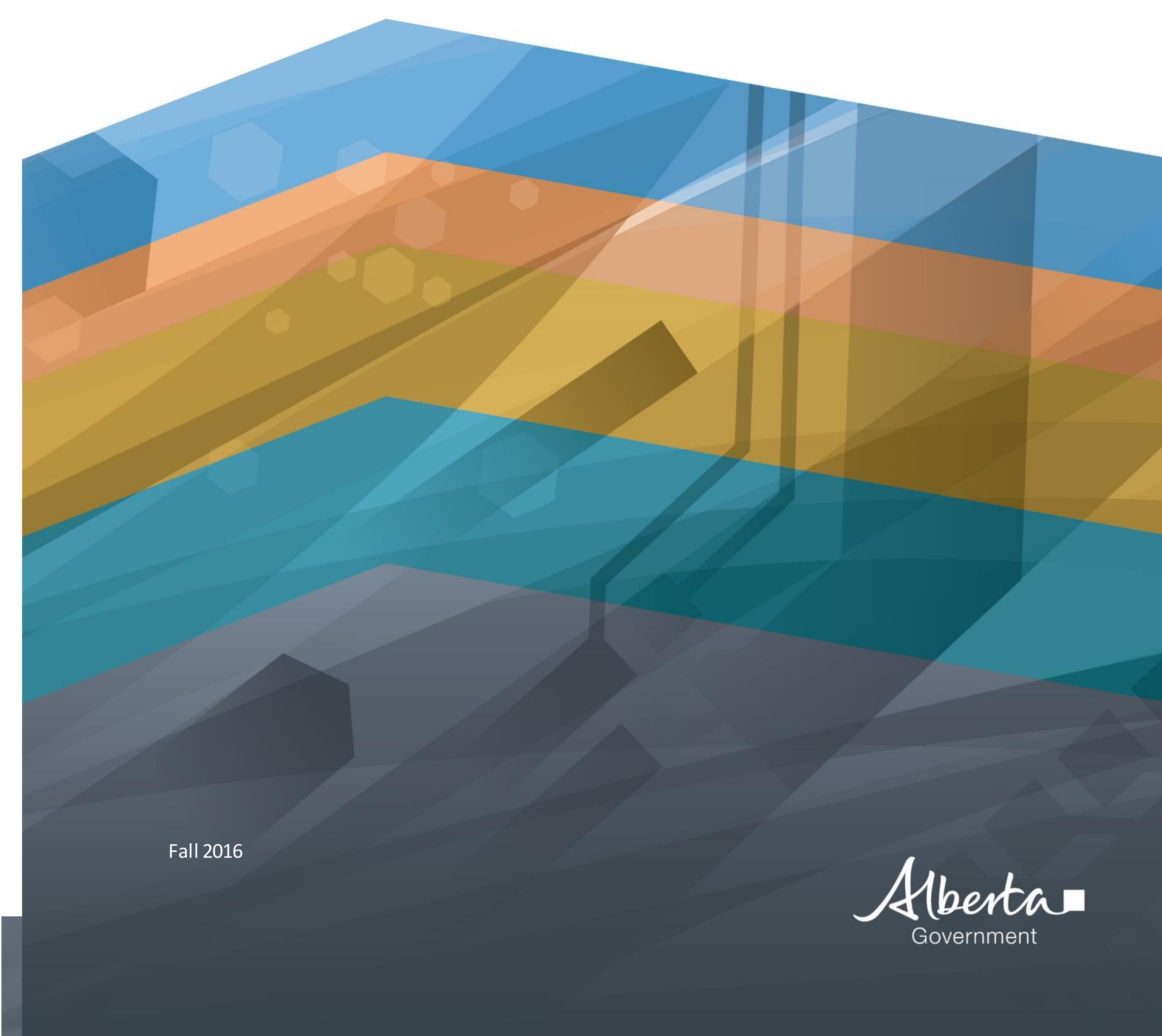
# IT Disaster Recovery Planning Guide



Fall 2016

Alberta
Government

## TABLE OF CONTENTS

## LEGAL DISCLAIMER

The IT Disaster Recovery Planning Toolkit has been prepared and made available to Alberta school authorities for general information purposes only. The information herein does not constitute legal advice, nor should you rely solely on the toolkit in order to assess risk or make plans. The content may be, or may become inaccurate or incomplete, and particular facts unique to your situation may render the content inapplicable to your situation. The toolkit is but one source of information available to you. You may wish to consider multiple sources in order to make plans.

The Government of Alberta does not accept liability for any loss or damage arising from, connected with, or relating to the use or reliance on the toolkit by you or any other person. School authorities remain wholly responsible for evaluating the completeness and effectiveness of their own IT disaster recovery plans.

## TABLE OF FIGURES

# I. INTRODUCTION TO GUIDE

## WHY DOES YOUR SCHOOL AUTHORITY NEED AN IT DISASTER RECOVERY PLAN?

***Learning and Technology Policy Framework* Policy Direction 5:**[1]

All students, teachers, administrators and other education professionals have access to appropriate devices, reliable infrastructure, high-speed networks and digital learning environments.

**Actions**
School Authorities:

d. ensure administration of safe and secure networks, infrastructure and technologies

f. provide and maintain timely technical support and services

g. adopt and maintain effective practices and up-to-date technological standards with respect to Information Technology (IT) governance, IT management and information security management

**Imagine this.** It's early June and floodwaters have peaked. Your school authority's data centre is under three feet of water. The servers that hold your financial and student information systems are in that data centre. The community has been evacuated, including the staff and students from three local schools.

How do you respond?

**The next disaster could happen to you – sooner than you think.**

Disasters such as the 2011 Slave Lake wildfire, the 2013 floods in southern Alberta and the 2016 Fort McMurray wildfire remind us that disasters can happen to anyone at any time. Every year in Alberta, significant unforeseen events like fires, floods and severe weather impact the day-to-day operations of school authorities. Even minor incidents such as a burst water pipe or small fire can result in a significant disruption if risk mitigation strategies have not been put in place. These disruptive events can last as little as a day or can have such a significant impact that full recovery can take years.

**Your school authority is more reliant on technology services and infrastructure than you think.**

School authorities are increasingly dependent on technology services and infrastructure for providing learning, teaching and administration services. Loss of service can significantly disrupt school operations and may put personal student or staff information at risk of unauthorized access, disclosure or destruction.

[1] Alberta Ministry of Education. (2013). *Learning and Technology Policy Framework (LTPF)*. Pg. 39-40. Retrieved from Alberta Education website: https://education.alberta.ca/media/7792655/learning-and-technology-policy-framework-web.pdf.

**You need an IT disaster recovery plan more than you think you do.**

During a disaster, you and your team need to know who their staff and students are and how to contact them. People need to be paid. Operations in schools not immediately affected by the disaster need to continue. The confidentiality, integrity and availability of information needs to be safeguarded.

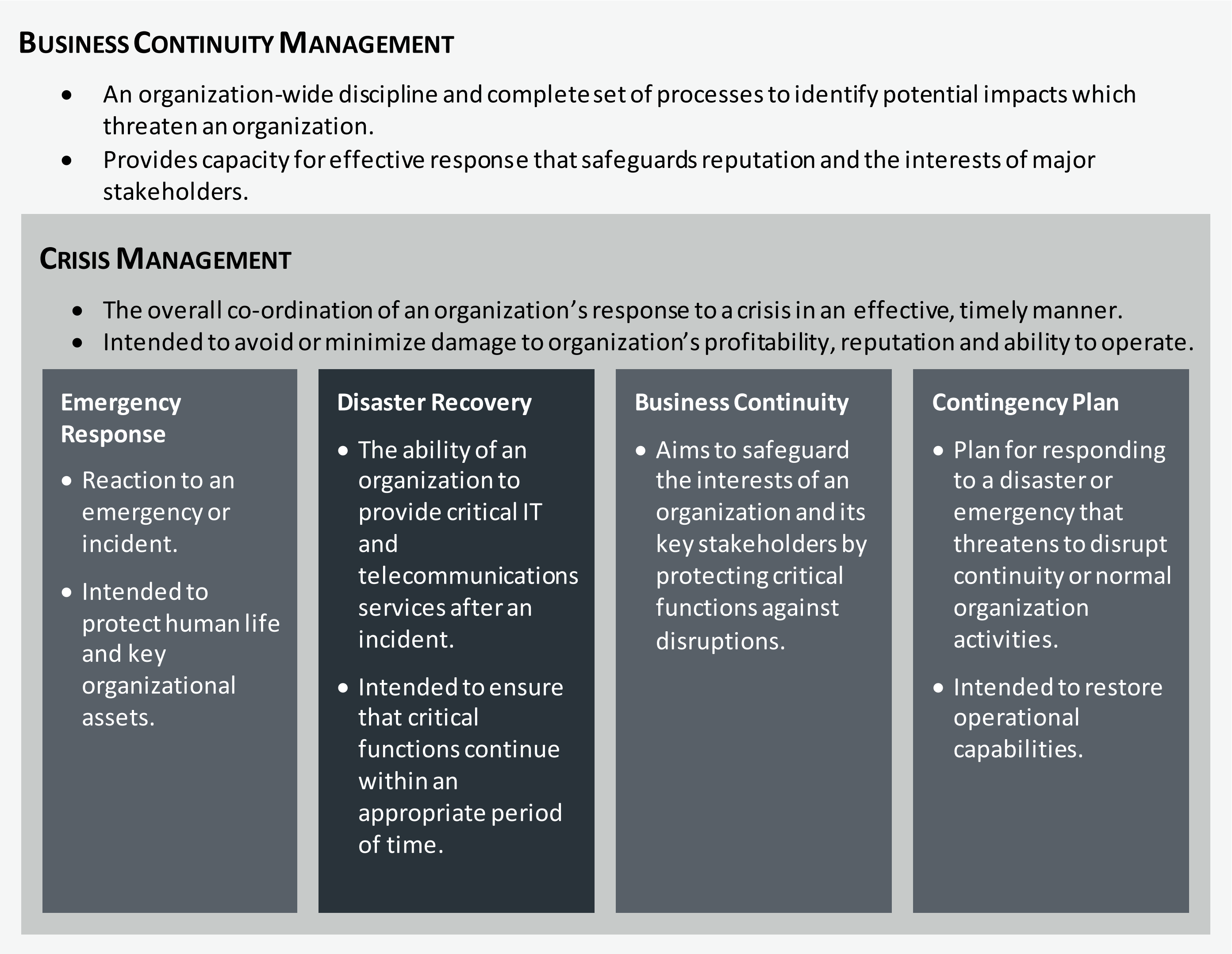
By preparing a formal IT disaster recovery plan and exercising the plan, you can reduce the probability and impact of a disruptive event on your school authority.

## WHAT IS AN IT DISASTER RECOVERY PLAN?

- An IT disaster recovery plan documents:
  - school authority leadership's objectives for disaster recovery;
  - who is on the disaster recovery team and their roles and responsibilities; and
  - detailed procedures for protecting and recovering required technical services after a disruptive event such as a flood or fire.
- IT disaster recovery planning does not include:
  - managing routine incidents such as minor hardware failures. The IT help desk or service desk typically handles routine incidents through IT incident response procedures.
- IT disaster recovery can include, but should not be limited to, creating server and data backups.
  - The time required to restore from backup may not meet the organization's requirements and timelines to restore core services.

## HOW DOES DISASTER RECOVERY FIT WITHIN BUSINESS CONTINUITY MANAGEMENT?

- Business continuity management focuses on assessing how threats to a school authority could impact its critical education and business functions and planning an effective response.
- Disaster recovery is a component of business continuity management. It focuses on recovering critical information technology and telecommunications services after a disruption to ensure that critical education and business functions can continue within an acceptable period of time.



**BUSINESS CONTINUITY MANAGEMENT**

- An organization-wide discipline and complete set of processes to identify potential impacts which threaten an organization.
- Provides capacity for effective response that safeguards reputation and the interests of major stakeholders.

**CRISIS MANAGEMENT**

- The overall co-ordination of an organization's response to a crisis in an effective, timely manner.
- Intended to avoid or minimize damage to organization's profitability, reputation and ability to operate.

**Emergency Response**

- Reaction to an emergency or incident.
- Intended to protect human life and key organizational assets.

**Disaster Recovery**

- The ability of an organization to provide critical IT and telecommunications services after an incident.
- Intended to ensure that critical functions continue within an appropriate period of time.

**Business Continuity**

- Aims to safeguard the interests of an organization and its key stakeholders by protecting critical functions against disruptions.

**Contingency Plan**

- Plan for responding to a disaster or emergency that threatens to disrupt continuity or normal organization activities.
- Intended to restore operational capabilities.

Figure 1: Overview of Business Continuity Management[2]

## WHO IS INVOLVED IN IT DISASTER RECOVERY PLANNING?

- The school authority's IT leader or designate typically leads IT disaster recovery planning efforts. It is important to involve a diverse group of people including trustees, the superintendent, senior leaders and principals in setting priorities to ensure that IT disaster recovery plans meet organization needs.

- The IT leader often works with the IT department and possibly contractors to determine technical approaches and to develop and test recovery plans.

[2] Goh, Moh Heng (2008). BCMPedia. A Wiki Glossary for Business Continuity Management, Crisis Management and Disaster Recovery, BCM Institute. Retrieved from BCMPedia website: http://www.bcmpedia.org

## How do you develop an IT disaster recovery plan?

Developing an IT disaster recovery plan involves choosing the right people to be involved, following a process and selecting technologies.

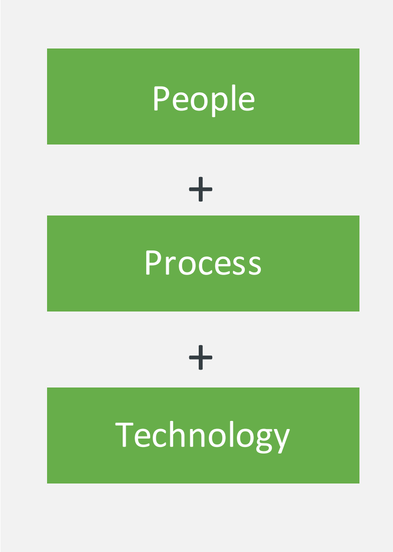


*Figure 2: Needed Components for Developing Disaster Recovery Plans*

If your organization does not yet have a process in place to develop, maintain and exercise a disaster recovery plan, consider initiating a project with a designated project leader and team members to develop the first version of your IT disaster recovery plan.

Once your school authority has identified who should be involved, the team:

- obtains senior leadership authorization and commitment to developing a plan;
- works with key members of your organization to establish planning priorities based on risks and the criticality of technology services;
- establishes roles and responsibilities for developing and carrying out the disaster recovery plan;
- determines technical approach and budget; and
- develops and tests recovery plans regularly, especially if there are changes to applications or IT infrastructure.

Leaders monitor and evaluate progress throughout to ensure that disaster recovery planning stays on track and achieves intended outcomes.

*Start with the simplest acceptable disaster recovery plan and improve your plan over time.*

# II. Overview of Developing a Disaster Recovery Plan

Developing an IT disaster recovery plan involves choosing the right people to be involved, following a process and selecting technologies. The following section discusses roles and responsibilities to assist in determining who should be involved with developing the plan.

## Roles and Responsibilities

Developing an IT disaster recovery plan requires involvement from two main groups:

1. A steering committee to make decisions, authorize time and resources and provide oversight; and
2. A working group that determines technical approach, develops service recovery plans and tests/implements the plan.

When determining who should participate in each group, consider decision-making authority, resources available to the person, and their knowledge, skills and attributes.

*It is not necessary to establish an additional steering committee for disaster recovery if there is an existing governing body with an appropriate mix of stakeholders. At minimum, the steering committee needs to have representation from trustees, the superintendent, senior leaders, the IT leader and principals. A technology advisory group or change advisory board could work if it has sufficient decision-making authority.*

*Also, a separate working group may not need to be formed if only one or two people will be developing and testing the recovery plan and they are members of the steering committee. The most critical aspect of planning is ensuring that stakeholders outside of the IT department are involved in the process.*

The steering committee provides oversight to the development of the disaster recovery plan. This group:

- authorizes the project to start;
- identifies and assigns members to the working group based on availability and subject matter expertise;
- approves the scope of work;
- allocates resources to the work;
- ensures resources are available when required;
- reviews and approves policies, procedures and standards related to disaster recovery;
- reviews and validates strategy to communicate disaster recovery activities to stakeholders and employees;
- monitors implementation; and
- removes barriers to the successful completion of the disaster recovery plan.

The working group performs the work of the project and provides advice to the steering committee to support decision-making, including:

- why this work is important;
- recommending initial scope;
- recommending resource allocations;
- advising of barriers and recommending solutions; and
- communicating the status of the work to develop, implement and test the IT disaster recovery plan.

The following diagram shows an overview of the main tasks each group is involved in when developing the disaster recovery plan.

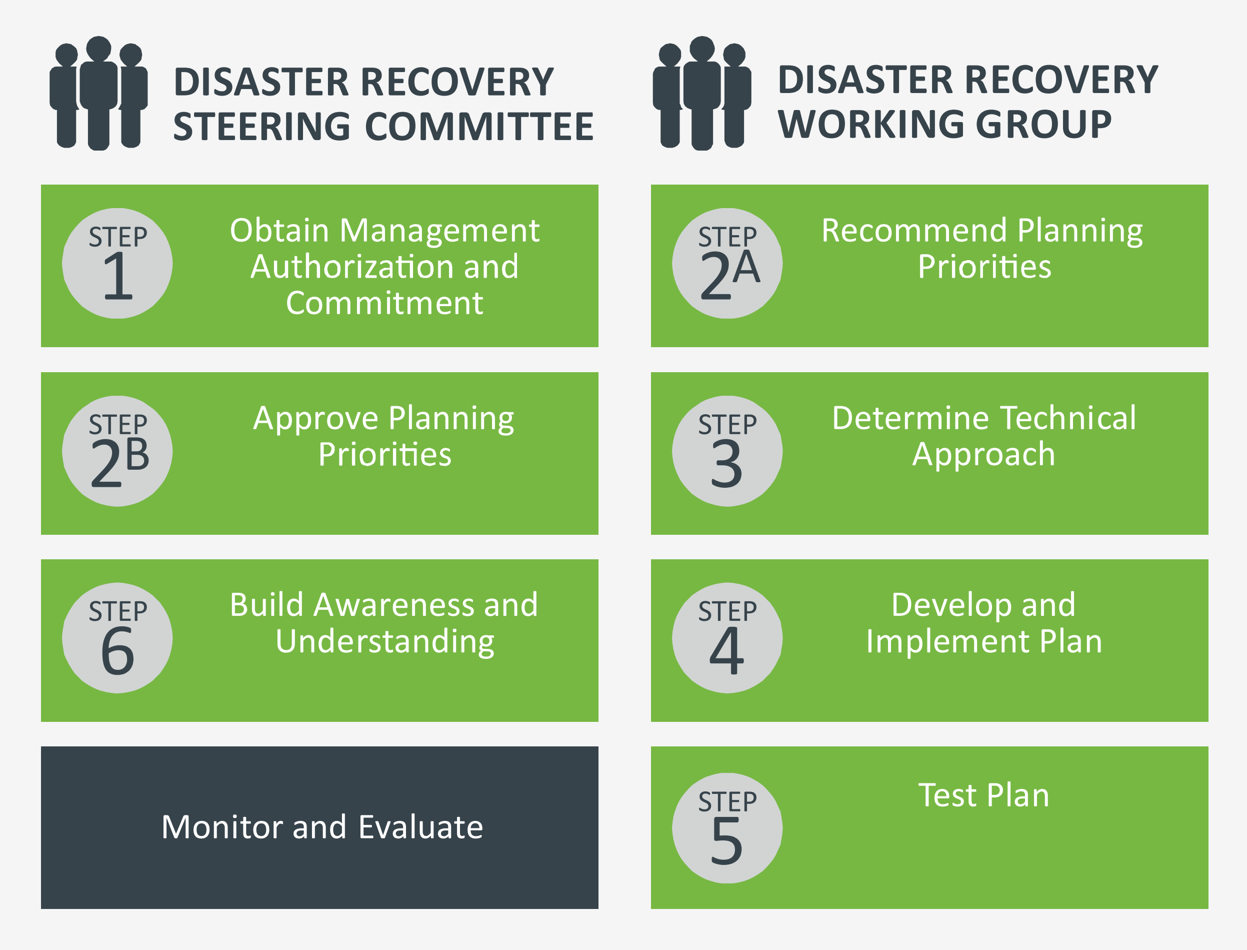

DISASTER RECOVERY STEERING COMMITTEE
DISASTER RECOVERY WORKING GROUP
STEP 1 Obtain Management Authorization and Commitment
STEP 2A Recommend Planning Priorities
STEP 2B Approve Planning Priorities
STEP 3 Determine Technical Approach
STEP 6 Build Awareness and Understanding
STEP 4 Develop and Implement Plan
Monitor and Evaluate
STEP 5 Test Plan

*Figure 3: Division of Work for Effective Disaster Recovery Planning*

## THE IT DISASTER RECOVERY PLANNING PROCESS

Disaster recovery planning is an ongoing and iterative process. Each step includes several activities to be performed. During initial development of the disaster recovery plan, steps 4 and 5 are repeated several times, each time focusing on developing and testing recovery plans for a different set of IT services.

After obtaining leadership commitment to the disaster recovery planning program in step 1, steps 2 through 6 are repeated periodically. IT services are dynamic – new services are created and outmoded services are retired. Priorities and disaster recovery plans must be revisited periodically to ensure that they are current.

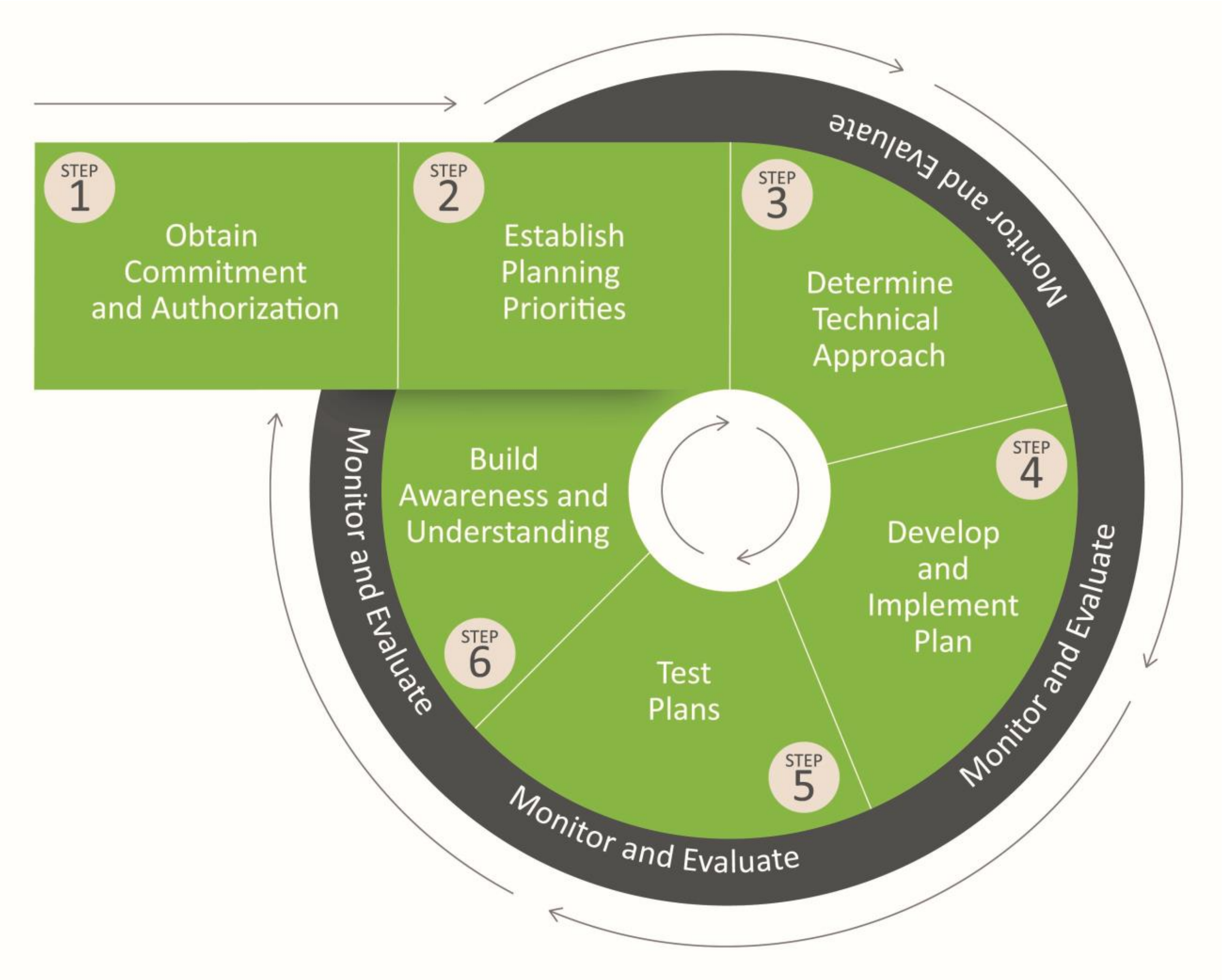

STEP 1
Obtain Commitment and Authorization
STEP 2
Establish Planning Priorities
STEP 3
Determine Technical Approach
STEP 4
Develop and Implement Plan
STEP 5
Test Plans
STEP 6
Build Awareness and Understanding
Monitor and Evaluate
Monitor and Evaluate
Monitor and Evaluate
Monitor and Evaluate

*Figure 4: IT Disaster Recovery Planning Process*

*After your initial disaster recovery plan is created, consider performing annual reviews to determine what changes are needed and update the plan accordingly.*

# Step 1 OBTAIN MANAGEMENT COMMITMENT AND AUTHORIZATION

STEP 1

## 1.1 WHAT IS INVOLVED?

- Increase awareness of disaster recovery planning and the importance of leadership support.
- Increase understanding of what is involved in disaster recovery planning.
- Determine who needs to be involved in disaster recovery planning and why.
- Estimate costs and resources.
- Obtain authorization to proceed.
- Set up an IT disaster recovery plan steering committee or identify an existing governing body to oversee the implementation of the plan.

## 1.2 WHY IS THIS IMPORTANT?

- Effective disaster recovery planning requires commitment from all business areas and all levels of management.
- Leaders in your school authority need to understand why disaster recovery planning is important, so they give it the time, attention, resources and budget necessary.
- Obtaining authorization commits the school authority to having a disaster recovery plan and increases the probability that that the disaster recovery program will be sustainable. It also facilitates the development of a disaster recovery plan by making it easier to obtain time and resources from other areas of the organization.

## 1.3 WHO NEEDS TO BE INVOLVED?

- Superintendents, senior leaders and the IT leader should be involved in authorizing the IT disaster recovery program.

| | Authorize Disaster Recovery Planning Program | |
|---|---|---|
| | Input | Decide |
| Trustees | 🟩 | |
| Superintendent | | 🟩 |
| Secretary Treasurer | 🟩 | |
| Senior Leaders | 🟩 | |
| Business Areas | 🟩 | |
| IT Leader | 🟩 | |
| IT Team | | |
| Principals | | |
| Secretary Treasurer | | |

*Figure 5: Authorize Disaster Recovery Planning Program Task Matrix*

## 1.4 HOW DO WE DO THIS?

**Gather background information:**

- Determine if there is an administrative procedure or policy in your school authority that specifies the requirement to create and maintain a business continuity plan or disaster recovery plan.

- Determine if your school authority has a disaster recovery plan, and the date of its last update if appropriate.

- Determine if IT services are included in these plans, and identify any gaps or outdated information in the documentation.

- Determine who is responsible for maintaining your school authority's disaster recovery or business continuity plan and consider meeting with him or her to gain insight to guide development of the IT disaster recovery plan.

**Determine next steps:**

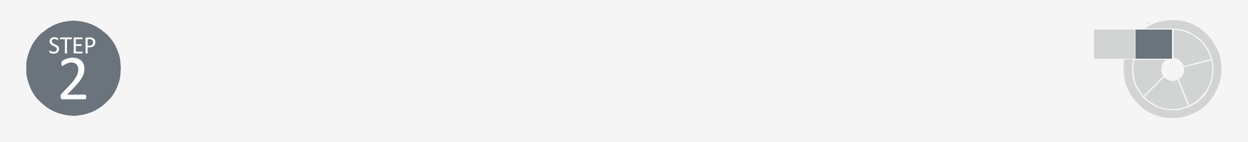
- Meet with key decision-makers to determine their level of awareness and support for developing an IT disaster recovery plan, and to determine how to present to senior leaders, how to obtain formal authorization to proceed, if it is necessary to develop an administrative policy or procedure, etc.

- If necessary, prepare a brief presentation for senior leaders that outlines the issue, including why this important, what has already been done, an overview of the process and next steps.

*Make disaster recovery relevant to senior leaders by communicating the benefits of disaster recovery planning in their terms. A presentation template for building awareness and understanding with senior leaders is included with this toolkit and can be customized for your context.*

- Identify an existing governing body with the right mix of stakeholders or form an IT disaster recovery plan steering committee if needed. Consider knowledge, skills, attributes, decision-making authority and available resources when forming the committee. See section *Roles and Responsibilities* on page 10 for more information on how to do this and the role the committee will play.
- If it is necessary to develop or revise an administrative regulation or procedure, follow your school authority's current process for development, review and approval. Formal authorization may require creating or amending an administrative procedure. Consult with appropriate personnel for advice on how to proceed.

# Step 2 ESTABLISH PLANNING PRIORITIES



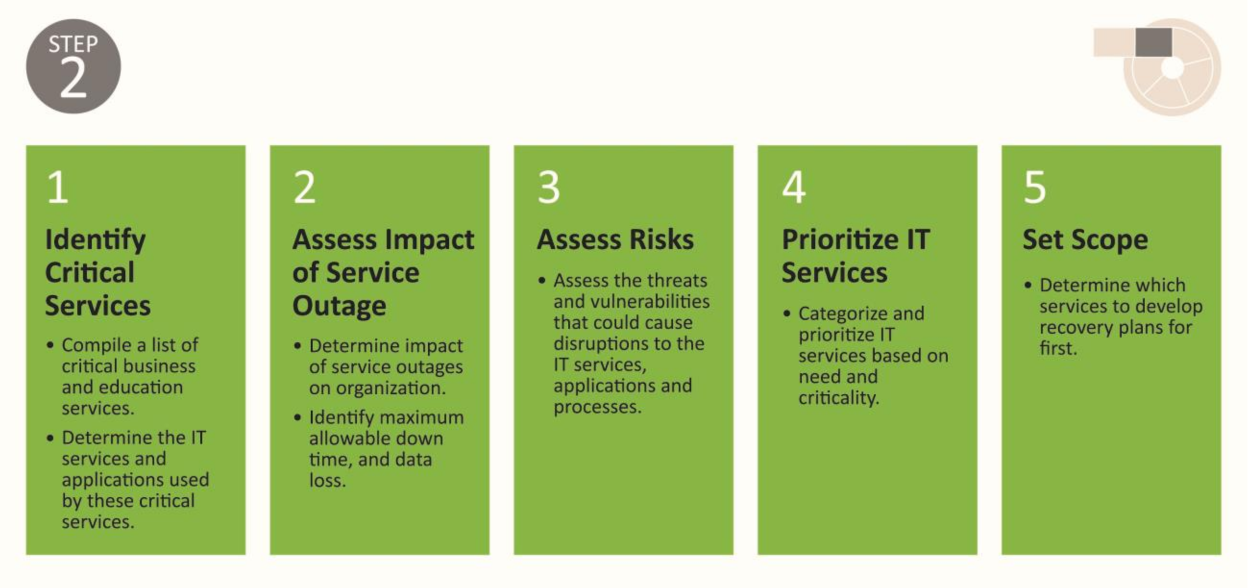
## 2.1 WHY IS THIS IMPORTANT?

- Given limited time and resources, prioritizing risk reduction and recovery efforts based on service criticality and level of risk to the organization supports effective budgeting.
- Setting a reasonable scope of services to include in the first version of the disaster recovery plan reduces the risk of taking on too much and feeling ove rwhelmed.

## 2.2 WHAT IS INVOLVED?

At this stage, the school authority prioritizes services for recovery and sets the scope of initial planning efforts by determining and documenting the impact of a disruption to key IT services on the organization.

**Phases for Establishing Planning Priorities**



1 **Identify Critical Services**

- Compile a list of critical business and education services.
- Determine the IT services and applications used by these critical services.

2 **Assess Impact of Service Outage**

- Determine impact of service outages on organization.
- Identify maximum allowable down time, and data loss.

3 **Assess Risks**

- Assess the threats and vulnerabilities that could cause disruptions to the IT services, applications and processes.

4 **Prioritize IT Services**

- Categorize and prioritize IT services based on need and criticality.

5 **Set Scope**

- Determine which services to develop recovery plans for first.

*Figure 6: Phases for Establishing Planning Priorities*

**Required outcomes/outputs:**

- Prioritized list of technology services including maximum allowable downtime and maximum allowable data loss for each.

## 2.3 WHO NEEDS TO BE INVOLVED?

| | Identify Critical Services | | Assess Impact of Outages | | Prioritize IT Services | |
|---|---|---|---|---|---|---|
| | Input | Decide | Input | Decide | Input | Decide |
| Steering Committee | | 🟩 | | 🟩 | | 🟩 |
| Trustees | | | | | | |
| Superintendent | 🟩 | | 🟩 | | 🟩 | |
| Secretary Treasurer | 🟩 | | 🟩 | | 🟩 | |
| Senior Leaders | 🟩 | | 🟩 | | 🟩 | |
| Business Areas | 🟩 | | 🟩 | | 🟩 | |
| IT Leader | 🟩 | | 🟩 | | 🟩 | |
| Working Group | 🟩 | | 🟩 | | 🟩 | |
| Principals | 🟩 | | 🟩 | | 🟩 | |

*Figure 7: Establish Planning Priorities Task Matrix*

## 2.4 HOW DO WE DO THIS?

### Business Impact Analysis and Risk Assessment

- Work with business areas to identify critical business and education services, and determine how quickly each service must be restored to meet the needs of the school authority.
- Identify the supporting technology applications or services used for each business or education service. Include dependencies on back office IT services.
- Identify IT processes fundamental to support the recovery of IT services and applications. For example, incident management, change management and access provisioning.

*Refer to the list of services from your IT service portfolio or service catalogue if you have one. If not, create a list of applications in use by other areas of the organization.*

### Assess Impact of Service Outages

When assessing impacts, consider those that relate to your school authority's overall objectives and its stakeholders such as:

- the impact on staff;
- the impact of damage to, or loss of premises, technology or information;
- the impact of breaches of regulatory requirements;
- damage to reputation;
- damage to financial viability;
- deterioration of service quality; and
- environmental damage.

The impact assessment identifies the IT services necessary to enable time critical and essential business and education processes to continue operating at a minimum acceptable level.

**Key question:** What is the impact of a technical service outage on the school authority? Could an outage affect student or staff safety? Could it affect the organization's reputation?

Set up a meeting with senior leaders and representatives from various areas of your organization to discuss the impact of IT service outages on their area and the organization as a whole.

**Additional questions to discuss:**

- Does the impact vary by time of month or year? Are there any specific deadlines that organization stakeholders must meet?
- What is the maximum allowable outage time for each critical business or education service?
- How feasible are manual workarounds?
- How soon does each technology service need to be available? (recovery time objective)

  The *recovery time objective* is the goal for how fast to restore technology services after a disruption (based on the acceptable amount of down time and level of performance)[3]. For example, a recovery time objective of 24 hours with local accessibility for payroll services means that the payroll application must be up and running within 24 hours as well as accessible locally.

- How much data or information can we afford to lose? (recovery point objective)

  The *recovery point objective* is the goal for the point at which to restore data or information after a disruption (based on the acceptable amount of data or information loss)[3]. For example, a recovery point objective of 6 hours for payroll services means that the payroll data must be backed-up every 6 hours so that no more than 6 hours of data entered into the payroll application is lost after a disruption.

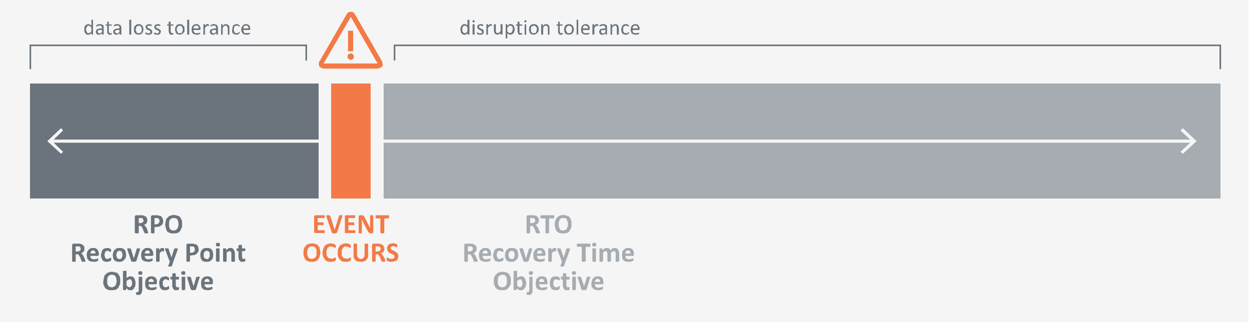


*Figure 8: Recovery Time Objective and Recovery Point Objective*

[3] Disaster Recovery Institute International. *International Glossary for Resiliency*. Retrieved July 23, 2015 from: https://www.drii.org/assets/glossary_doc/International_Glossary_for%20_Resiliency_06102014.pdf

### Assess Risks

**Key question:** What are the threats and vulnerabilities that could cause disruptions to the IT services, applications and processes identified in the business impact analysis at the beginning of step 2?

### Prioritize Services

**Key question:** What is the order and priority for recovering services?

This step involves classifying and prioritizing services. Based on information gathered in step 2, each service can be classified as follows[4]:

| Service Classification | Recovery Time Objective |
|---|---|
| Critical | within 24 hours |
| Vital | within 72 hours |
| Necessary | within 2 weeks |
| Desired | longer than 2 weeks but necessary to return to normal operating conditions |

*Figure 9: Service Classifications*

Once you have classified services and confirmed them with other areas of the organization, determine the priority of services within each classification.

**Questions to discuss when considering priorities:**

- Does the service affect student or staff safety?
- Does the service affect the ability of the organization to communicate to stakeholders?
- Does the service involve vital records?
- Are there monthly or seasonal variations in the importance and priority of this service?
- Does the service affect the ability of the organization to pay employees or suppliers?
- Does the service need to be restored before other critical services?

*Completing step 2 of the IT Disaster Recovery Workbook included with this toolkit will assist with prioritizing services.*

### Set Scope

**Key Question:** For which services will we develop a service recovery plan?

After establishing priorities, determine which services you will develop and document recovery procedures for in the first iteration of the disaster recovery plan and which will be left to a later date. Revisit this before budget planning time, and reinforce the need to continue. Then propose which services could be planned during the upcoming fiscal year, and negotiate priorities by encouraging leaders to consider the cost, value and risk of the planning effort.

[4] Alberta Emergency Management Agency. *Business Resumption.* Retrieved November 20, 2015 from Alberta Emergency Management Agency website: http://www.aema.alberta.ca/business-resumption
Note: Alberta Emergency Management Agency uses the term service *categories.* This document uses the term service *classifications* in order to avoid confusion with Service Portfolio terminology.

# Step 3 DETERMINE TECHNICAL APPROACH

## 3.1 WHY IS THIS IMPORTANT?

With limited time and resources, this step focuses your efforts and resources on where they will make the most difference for disaster recovery planning. This stage is critical for determining how to meet the organization's needs identified in step 2: Establish Planning Priorities.

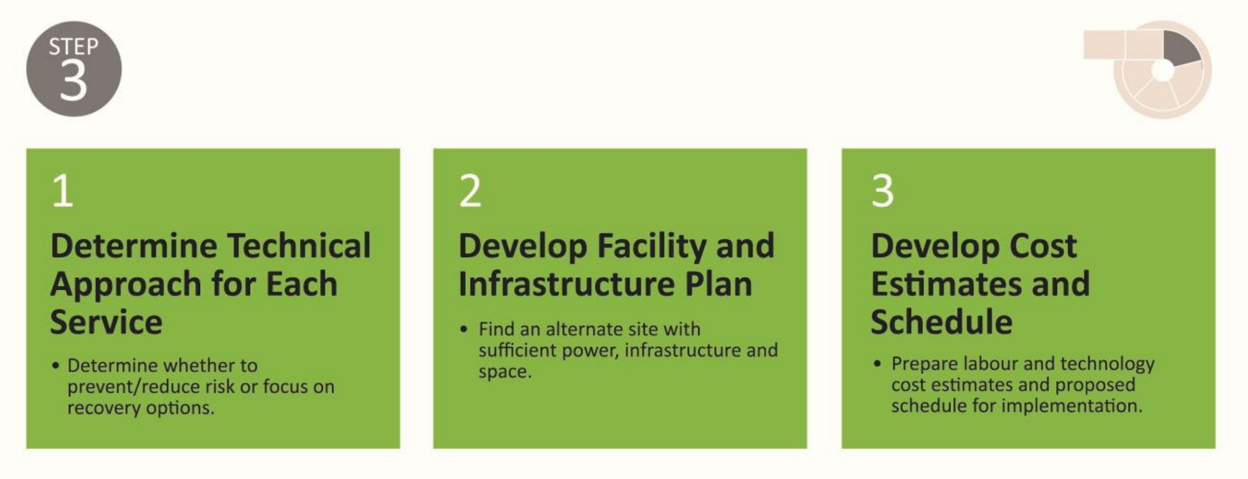
## 3.2 WHAT IS INVOLVED?

This stage involves determining how much to invest in preventing a disaster (such as by having redundant components or equipment) as opposed to recovering from a disaster.

After establishing investment priorities, determine the facilities and technologies needed as well as how much they will cost and a proposed schedule for implementation.

**Desired outcomes/outputs:**

- prioritized list of technology services with proposed approach to either prevent/reduce risk or focus on recovery options;
- proposed facilities/technologies required to meet organization requirements;
- labour and technology cost estimates to implement approach; and
- proposed schedule for implementation.



1 Determine Technical Approach for Each Service

- Determine whether to prevent/reduce risk or focus on recovery options.

2 Develop Facility and Infrastructure Plan

- Find an alternate site with sufficient power, infrastructure and space.

3 Develop Cost Estimates and Schedule

- Prepare labour and technology cost estimates and proposed schedule for implementation.

*Figure 10: Determine Technical Approach*

## 3.3 WHO NEEDS TO BE INVOLVED?

- The IT leader and working group research and recommend technical approaches.
- Senior leaders and the IT leader decide the best cost/benefit approach to disaster recovery.

| | Determine Technical Approach | | Develop Facility and Infrastructure Plan | | Develop Cost Estimates and Schedule | |
|---|---|---|---|---|---|---|
| | Input | Decide | Input | Decide | Input | Decide |
| Steering Committee | 🟩 | | 🟩 | | | 🟩 |
| Trustees | | | | | | |
| Superintendent | | | | | | |
| Secretary Treasurer | | | | | | |
| Senior Leaders | | | | | | |
| Business Areas | | | | | | |
| IT Leader | | 🟩 | | 🟩 | 🟩 | |
| Working Group | 🟩 | | 🟩 | | 🟩 | |
| Principals | | | | | | |

*Figure 11: Determine Technical Approach Task Matrix*

## 3.4 HOW DO WE DO THIS?

### Determine Technical Approach for Each Service

Using the prioritized list of technology services identified in the step 2: Establish Planning Priorities phase, determine whether to follow a strategy of preventing outages (through implementing redundant components, etc.) or to focus on recovery options such as manual workarounds and alternate sites to recover technology services and applications within the required timeframe. Consider the following factors when determining the technical approach:

- **Recovery time objective and recovery point objective:** Services with a short recovery time objective or recovery point objective are more likely to require a preventative approach in order to meet organizational needs. It may not be possible to recover services quickly enough.
- **Risks and risk mitigation strategies:** Each service faces numerous risks, which would be time consuming to identify and mitigate. A more effective use of time is to determine a technical approach for handling each of the following five risk scenarios, such as a redundant failover site, redundant network components or relying on backups. This will address the majority of risks to a service.

| Risk Scenario | Scenario Assumptions (adjust as needed) | Recommended Technical Approach to Address Risk |
|---|---|---|
| Loss of facility through a destructive event | • Permanent destruction of facility (data centre or place of work).<br>• Includes destruction of all items in the facility (e.g. infrastructure, records, etc.).<br>• Other facilities are still available. | |

| Risk Scenario | Scenario Assumptions (adjust as needed) | Recommended Technical Approach to Address Risk |
|---|---|---|
| Loss of physical access to a facility | • Facility is temporarily inaccessible.<br>• Employees can return once the event has been resolved. | |
| Loss of network | • Internet and intranet access is temporarily unavailable.<br>• Network access will be available within 72-168 hours.<br>• Remote VPN access is available immediately. | |
| Loss of applications | • Applications are temporarily unavailable and may need to be recovered.<br>• Applications will be available within 72-168 hours.<br>• Recovery point objective is within 24 hours for most applications. | |
| Loss of employees | • Absenteeism rises to a level that significantly impairs ability to operate normally.<br>• 50% of staff in each area are unavailable for seven days.<br>• Not all employees return to work after absence. | |

Choosing preventative approaches such as having redundant equipment or planning for faster recovery times typically costs more money and requires more resources. Some areas of the organization may need to accept longer recovery time objectives or recovery point objectives due to budget or resource constraints.

*Consider following a preventative or risk reduction approach for technology services where outages have a high impact in a short timeframe and a recovery approach for technology services with lower impacts that take longer to develop.*

*See step 3 of the IT Disaster Recovery Workbook included with this toolkit to support discussions on this topic.*

### Develop Facility and Infrastructure Plan

***Key questions:***

- Facility Plan: Where will we go when a disaster occurs?
- Infrastructure Plan: How will we restore our infrastructure services?

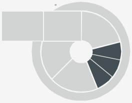
Work with your team to find an alternate site that has the power, infrastructure and space requirements needed to restore your IT services. The alternate site should be a sufficient distance away from your primary site so that a disaster does not affect both sites.

### Develop Cost Estimates and Schedule

Prepare labour and technology cost estimates and a proposed schedule for implementation. Negotiate and obtain approval from the IT Disaster Recovery Plan Steering Committee (or equivalent body).

# Step 4 DEVELOP AND IMPLEMENT PLAN

STEP 4



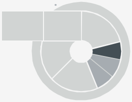
Step 4 is where the IT Disaster Recovery Plan Working Group focuses its efforts. During this step, the team develops the detailed contents of the plan, including:

- determining who does what during an event, including who can declare a disaster, who has what authority to purchase equipment, etc.; and
- developing processes to respond to an event, including how an incident is assessed to determine if a disaster should be declared, how services will be recovered, and how normal operations will be resumed.

> *While some activities in this step, like determining who can declare a disaster, will be performed only once, other activities, like developing recovery processes, will have to be done for each service.*

## 4.1 ESTABLISH ROLES AND RESPONSIBILITIES

STEP 4.1



### Why is this important?

It is critical to establish roles and responsibilities beforehand in order to respond effectively to a disaster.

### What is involved?

- Establish roles and responsibilities (see section 4.1 Roles and Responsibilities in the IT Disaster Recovery Plan Template for suggestions).
- Decide who will lead disaster recovery efforts and who will handle the technical recovery.
- Designate alternates in case primary members are not available.
- Document roles and responsibilities as well as the call list in section 4 of the disaster recovery plan. (A call list specifies names, roles and contact information of leaders and team members responsible for responding to an incident or event and handling recovery efforts).

### Who needs to be involved?

- Senior leaders and IT leaders define roles and responsibilities including who will lead from the business side.

- The IT leader and working group determine who will be responsible for each role required for IT disaster recovery.

| | Establish Roles and Responsibilities | |
|---|---|---|
| | Input | Decide |
| Steering Committee | | 🟩 |
| Trustees | | |
| Superintendent | 🟩 | |
| Secretary Treasurer | 🟩 | |
| Senior Leaders | 🟩 | |
| Business Areas | 🟩 | |
| Working Group | 🟩 | |
| Principals | | |

*Figure 12: Establish Roles and Responsibilities Task Matrix*

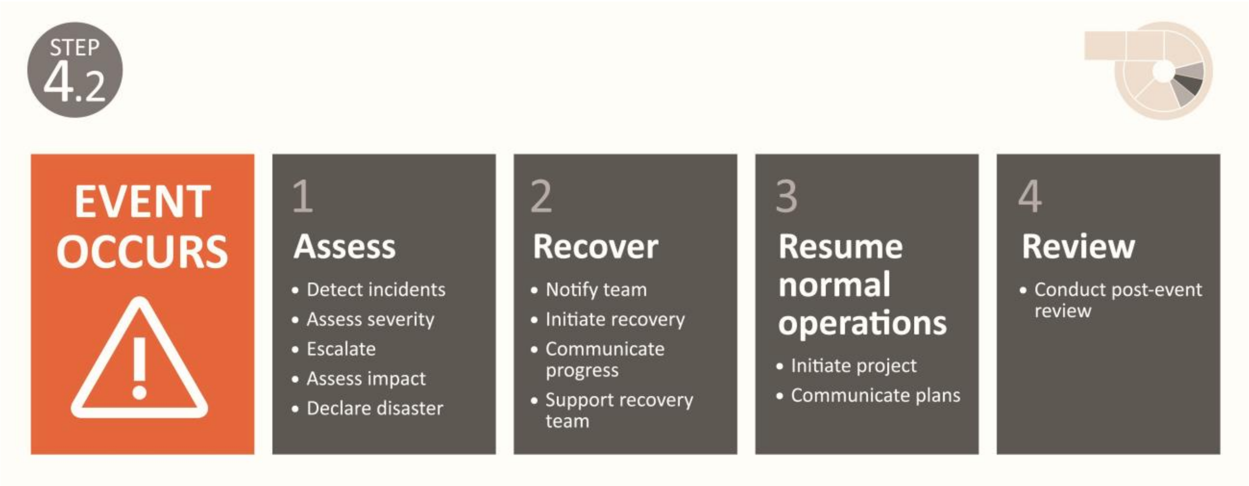
### How do we do this?

- Meet with the working group to determine who will do what during disaster recovery (see planning template for suggestions).
- Meet with senior leaders to discuss and approve roles and responsibilities.
- Document roles and responsibilities in the disaster recovery plan.

## 4.2 Determine Disaster Response Processes

### Overview

Responding to a disaster occurs in several phases as shown below. After an event occurs, the team assesses the event and determines whether to declare a disaster. If a disaster has occurred, the team initiates recovery of the IT service(s), in an alternate location if necessary. Once required IT Services are up and running, the team can focus on resuming normal operations. The final phase is to conduct a post-event review to discuss lessons learned.



STEP 4.2

EVENT OCCURS

1 Assess
- Detect incidents
- Assess severity
- Escalate
- Assess impact
- Declare disaster

2 Recover
- Notify team
- Initiate recovery
- Communicate progress
- Support recovery team

3 Resume normal operations
- Initiate project
- Communicate plans

4 Review
- Conduct post-event review

*Figure 13: Disaster Response Process Overview*

The phases of the disaster response include a number of key processes that you need to develop, test and add to the disaster recovery plan.

### Why do you need to develop disaster response processes?

Determining and documenting key processes for responding to a disaster increases the speed and effectiveness of response.

### What is involved?

This phase involves developing, testing and documenting key processes for each step of response.

### Who needs to be involved?

- The IT leader and working group develop and document disaster response processes.
- The IT leader approves the processes.

| | Determine Disaster Recovery Response Processes | |
|---|---|---|
| | Input | Decide |
| Steering Committee | | |
| Trustees | | |
| Superintendent | | |
| Secretary Treasurer | | |
| Senior Leaders | | |
| Business Areas | | |
| IT Leader | | 🟩 |
| Working Group | 🟩 | |
| Principals | | |

*Figure 14: Approve Disaster Response Processes Task Matrix*

### How do we do this?

This section contains key questions to discuss with your team and guidance for developing key processes for each phase of the disaster response.

*Assess*

**Key question:**

How do we determine if a disaster has occurred? What criteria will we use?

**Processes to develop:**

- **Assess severity of incident or event:**
  - document the process for determining the severity of the incident or event and provide escalation criteria; and
  - document linkages with service desk processes that detect incidents.
- **Escalate severe incidents:** document the escalation process for engaging the IT team and senior leadership to assess the impact of the incident.
- **Assess impact:** determine information needed to declare a disaster such as approximate amount of damage and estimated recovery time. Recommend a response to leadership to recover in place or to declare a disaster and begin recovery in an alternate site.
- **Declare disaster:** establish and document clear criteria for when to declare a disaster and a delegation of authority process so that IT team members are empowered to act if designated leaders are not available.

> *Handle minor incidents causing service outage through incident response procedures. Escalate severe incidents or events such as loss of all communications, loss of power, flooding/fire, or loss of the building to appropriate personnel.*

***Recover***

**Key questions:**

- How do we mobilize the disaster recovery team and initiate recovery?
- How do we communicate progress? Whom do we need to keep informed?
- How do we take care of the disaster recovery team's needs (food, water, rest, etc.)?

**Processes to develop:**

**Notify team**

- Document the call out process to ensure quick mobilization of disaster recovery team.

**Initiate recovery**

- Document process for activating disaster recovery plan, setting up recovery site and recovering systems based on priority.

**Processes to develop (continued):**

**Communicate progress**

- Document suggested communication channels, identify key stakeholder groups and recommend frequency of communication.

**Support recovery team**

- Establish systems and policies to ensure the recovery team is getting enough food, water and rest to be effective.
- Provide guidance for dealing with personal needs of employees such as time off for family matters, injury or loss of property.

> *Disasters can create a great deal of stress. Team members may work long hours and try to push through exhaustion, which can cause additional problems. Plan ahead to ensure people are taken care of.*

***Resume***

**Key questions:**

- How do we return to normal operations?

**Processes to develop:**

**Resume Normal Operations:**

- Document the process for resuming normal operations including ensuring readiness to resume and communicating plans to stakeholders.

***Review***

**Conduct review**

- Determine lessons learned. Include broad based group of stakeholders for the post-event review.

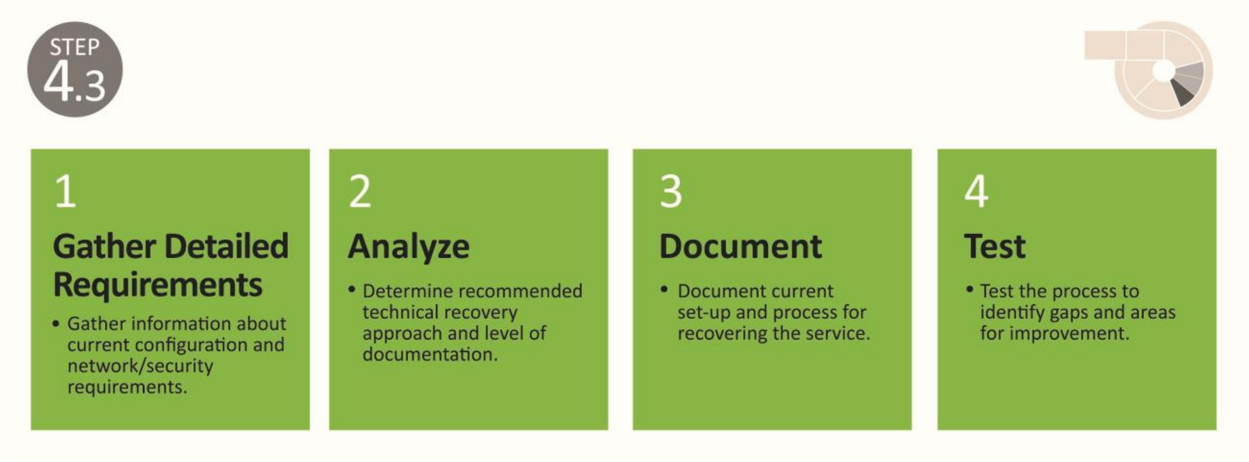
## 4.3 Develop Detailed Service Recovery Plans

### Why is this important?

IT team members with knowledge of how to restore the systems may not be available when a disaster occurs. Enough documentation needs to exist for others to be able to restore the systems.

### What is involved?

For each service included in the current scope, develop a detailed service recovery plan by gatheri ng detailed requirements, analyzing and documenting a recovery plan, implementing the required recovery technologies and performing a unit test.



STEP 4.3

1 **Gather Detailed Requirements**

- Gather information about current configuration and network/security requirements.

2 **Analyze**

- Determine recommended technical recovery approach and level of documentation.

3 **Document**

- Document current set-up and process for recovering the service.

4 **Test**

- Test the process to identify gaps and areas for improvement.

*Figure 15: Develop Detailed Service Recovery Plans*

## Who needs to be involved?

The working group is responsible for developing and documenting detailed service recovery plans.

## How do we do this?

Start with a simple service the first time you go through this process to become familiar with the process and set the foundation for future success. Next, select services based on the prioritized list developed earlier.

As you gather requirements and determine the required approach, you may need to renegotiate budget and resources in order to implement these plans.

***Gather Detailed Requirements***

- Gather information about the current set-up of the service including:
  - server and storage configuration (for in-house services);
  - network and security requirements; and
  - application configuration details.

***Analyze***

- **Determine recommended technical recovery approach**

  Consider your alternatives for recovery such as running on identical hardware or a virtual machine in your recovery facility, sharing equipment with a partner organization or using a cloud-based disaster recovery environment. Consider time and cost constraints.

- **Gather facility requirements**

  Determine requirements for restoring the service in your recovery facility if needed (e.g. space, power, telecommunications, etc.). Cloud-based services probably will not need this step.

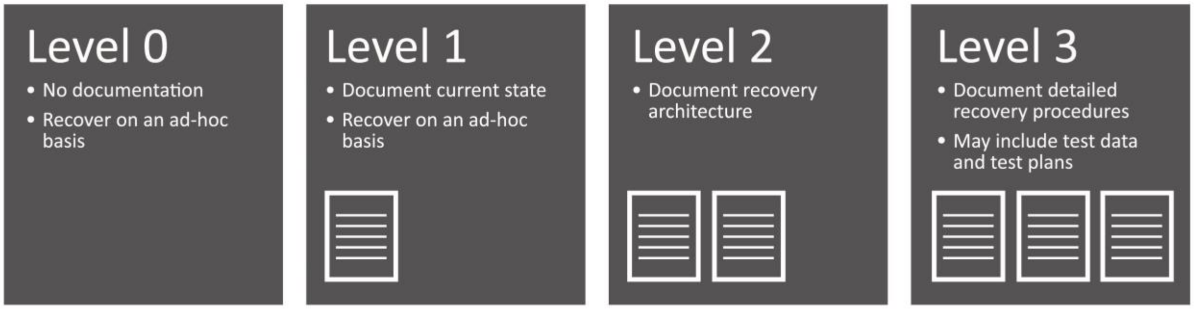
- **Identify and analyze dependencies**

  Determine dependencies on infrastructure services and any other service s.

- **Determine how much documentation is needed**

  Determine the level of detail needed for recovery documentation. Select the level of documentation based on criticality and/or complexity of service with higher levels of documentation needed for services that are more critical and/or complex.

> *Select the minimum level of documentation possible that reduces risk to an acceptable level. Higher levels of documentation require more time to create and maintain. They also get out of date more easily.*



Level 0
- No documentation
- Recover on an ad-hoc basis

Level 1
- Document current state
- Recover on an ad-hoc basis

Level 2
- Document recovery architecture

Level 3
- Document detailed recovery procedures
- May include test data and test plans

*Figure 16: Determine how much documentation is needed*

***Document***

**Level 0 – No Documentation**

- List name of service in disaster recovery plan and indicate that there is no recovery plan. Include minimal current state information such as where backups are stored.

**Level 1 – Current State Documentation**

Gather current state documentation, including:

- network diagrams and configuration;
- storage configuration;
- application configuration;
- backup/restore details;
- administration credentials;
- vendor contact details;
- location of installation media and licensing; and
- dependencies on other services.

**Level 2 – Recovery Architecture Documentation**

- In addition to level 1 documentation, a level 2 plan documents the recovery environment including recovery facility location and required components such as power, A/C, racks, and network connectivity. It also documents how to recover the infrastructure, data and applications used by the service and any dependencies on other services.
- If possible, set up the recovery facility location so that the documentation is applicable to the specific facility.

- When developing the documentation, assume that team members completing the recovery are familiar with the systems and understand their configuration and setup.

Note: Guidance on designing technical architecture for the recovery site is outside of the scope of this guide.

**Level 3 – Detailed Recovery Documentation**

- In addition to level 2 documentation, a level 3 plan includes detailed recovery procedures for the service.
- Assume that team members completing the recovery are NOT familiar with the systems and required configuration and setup. Include screenshots and detailed descriptions.

*For services in the current scope, document the current state of services (level 1) to begin with and increase documentation as needed in future iterations. With time and dedicated people, you can recover your systems with level 1 documentation.*

***Test***

- Meet with a team member and verbally go through the process documented in the plan to identify gaps, bottlenecks or other weaknesses.

# Step 5 TEST THE PLAN

## 5.1 WHY IS THIS IMPORTANT?

- Testing is the most important part of developing a disaster recovery plan. You do not know if your disaster recovery plan will work in a real disaster unless you test it ahead of time.

## 5.2 WHAT IS INVOLVED?

- It is important to test your disaster recovery plans after initial development and to retest them periodically on an ongoing basis.
- There are different types of tests varying in complexity and amount of time and resources to complete. Tabletop walkthroughs where team members verbally go through steps in the plan are least time consuming. Disaster simulations and full failover testing requires more time and resources.
- The following activities could be included as part of the testing:
    - define exercise and test activities in the test plan;
    - assign roles and responsibilities for performing disaster recovery plan exercises and tests;
    - invite end users to participate in the exercises;
    - include restoring from backup as part of the test activities;
    - document post-exercise debriefing and analysis; and
    - document recommendations for improving the disaster recovery plan based on the results.

## 5.3 WHO NEEDS TO BE INVOLVED?

- Initial testing and tabletop walkthroughs involve the disaster recovery team. Simulations or full failover testing require additional people to be involved to make them more realistic. The IT leader and/or the steering committee need to be involved in determining when to run a disaster simulation or full failover testing due to the potential impact and the need to involve other areas of the organization.

| | Determine Plans for Testing the Disaster Recovery Plan | |
|---|---|---|
| | Input | Decide |
| Steering Committee | | 🟩 |
| Trustees | | |
| Superintendent | | |
| Secretary Treasurer | | |
| Senior Leaders | | |
| Business Areas | | |
| IT Leader | | 🟩 |
| Working Group | 🟩 | |
| Principals | | |

*Figure 17: Test The Plan Task Matrix*

## 5.4 How do we do this?

- **Tabletop Walkthrough:** Team members gather in a meeting room and verbally go through the specific steps as documented in the plan to confirm effectiveness, and identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with the full team and familiarize staff with procedures, equipment and offsite facilities.
- **Disaster Simulation:** A mock disaster is simulated so that normal operations are not interrupted. A simulation involves testing hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities and alternate site processing. If possible, test against production data. Analyze the results to capture lessons learned and update the plan as appropriate.

  Disaster simulation could include:

  1) **Component testing**
     a. Test individual parts of the environment.
     b. Execute tests at different times throughout the year.
     c. Include participation of a limited number of business areas.
     d. Only test connectivity.

  2) **Environment segment testing**
     a. Test segments of the environment together (for example, groups of services like routers and firewalls).
     b. Execute a limited number of tests per year.
     c. Execute limited functional testing.

3) **Real time testing**

   a. Test all aspects of the environment within scope.

   b. Test all applications on one day.

   c. Execute connectivity and some functional testing.

   d. Isolate production.

- **Full Failover Testing:** A full failover test exercises the total disaster recovery plan. The test is likely to be costly and involves risk to normal operations. If your focus is on resiliency, and failing over automatically, these tests are required to ensure successful failovers during a disaster.

*Capture lessons learned and apply knowledge gained from the tests to improve your disaster recovery plan.*

# Step 6 BUILD AWARENESS AND UNDERSTANDING

STEP 6

## 6.1 WHY IS THIS IMPORTANT?

- Training and awareness is crucial to ensure that people know who to contact and what to do in a disaster situation.

## 6.2 WHAT IS INVOLVED?

- This phase involves training staff and ensuring that everyone is aware of the disaster recovery plan and knows where it is stored.

| | Monitor and Evaluate | |
|---|---|---|
| | Input | Decide |
| Steering Committee | | 🟩 |
| Trustees | | |
| Superintendent | | |
| Secretary Treasurer | | |
| Senior Leaders | | |
| Business Areas | | |
| IT Leader | | 🟩 |
| Working Group | 🟩 | |
| Principals | | |

*Figure 18: Build Awareness and Understanding Task Matrix*

## 6.3 WHO NEEDS TO BE INVOLVED?

- Everyone who has roles and responsibilities for disaster recovery needs to receive training. The rest of the organization needs to have general awareness.

## 6.4 HOW DO WE DO THIS?

- Schedule training sessions for current staff members.
- Include training in disaster recovery planning when onboarding new staff members.

# Step 7 MONITOR AND EVALUATE

STEP 7

## 7.1 WHY IS THIS IMPORTANT?

- The purpose for monitoring and evaluating the disaster recovery program is to take corrective action as needed to meet objectives, to manage risks, and to provide assurance of progress and risk reduction to stakeholders, particularly senior leaders.

## 7.2 WHAT IS INVOLVED?

- Develop measures that will assess progress towards objectives.
- Periodically assess progress towards the objectives and report to senior leaders.
- Define and document how the IT disaster recovery plan and related documentation is updated and where it is stored.
- Define and document the IT disaster recovery plan review process.

## 7.3 WHO NEEDS TO BE INVOLVED?

- The IT leader is responsible for monitoring and evaluating the disaster recovery team's work and progress.
- The IT disaster recovery plan steering committee and senior leaders are responsible for providing oversight of disaster recovery planning efforts.

| | Monitor and Evaluate | |
|---|---|---|
| | **Input** | **Decide** |
| **Steering Committee** | | 🟩 |
| **Trustees** | | |
| **Superintendent** | | |
| **Secretary Treasurer** | | |
| **Senior Leaders** | | |
| **Business Areas** | | |
| **IT Leader** | | 🟩 |
| **Working Group** | 🟩 | |
| **Principals** | | |

*Figure 19: Monitor and Evaluate Task Matrix*

## 7.4 HOW DO WE DO THIS?

- Work with the IT disaster recovery plan steering committee and senior leaders to develop measures that will assess progress towards objectives.
- Schedule regular meetings with the steering committee (or equivalent body) to monitor and evaluate progress.

# APPENDIX A – GLOSSARY

**Recovery time objective (RTO):** the goal for how fast to restore technology services after a disruption (based on the acceptable amount of down time and level of performance)[5]. For example, an RTO of 24 hours with local accessibility for payroll services means that the payroll application must be up and running within 24 hours as well as accessible locally.

**Recovery point objective (RPO):** the goal for the point at which to restore data or information after a disruption (based on the acceptable amount of data or information loss)[5]. For example, an RPO of 6 hours for payroll services means that the payroll data must be backed-up every 6 hours so that no more than 6 hours of data entered into the payroll application is lost after a disruption.

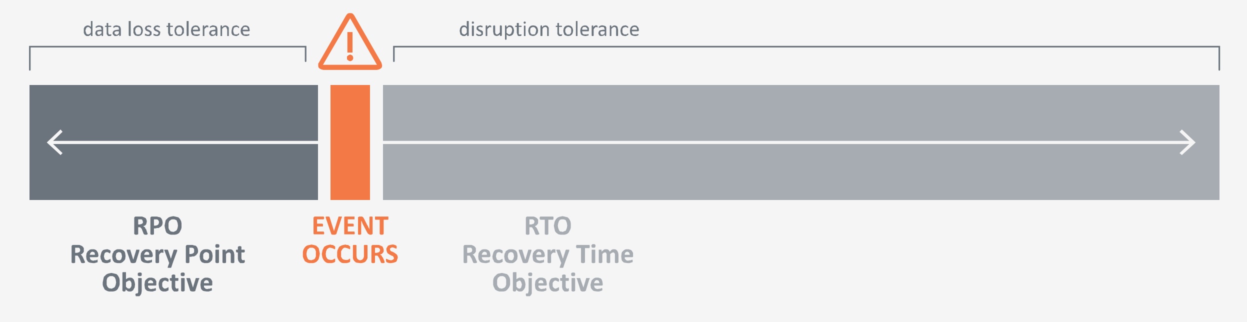


*Figure 25: Recovery Time Objective and Recovery Point Objective*

[5] Disaster Recovery Institute International. *International Glossary for Resiliency*. Retrieved July 23, 2015 from: https://www.drii.org/assets/glossary_doc/International_Glossary_for%20_Resiliency_06102014.pdf