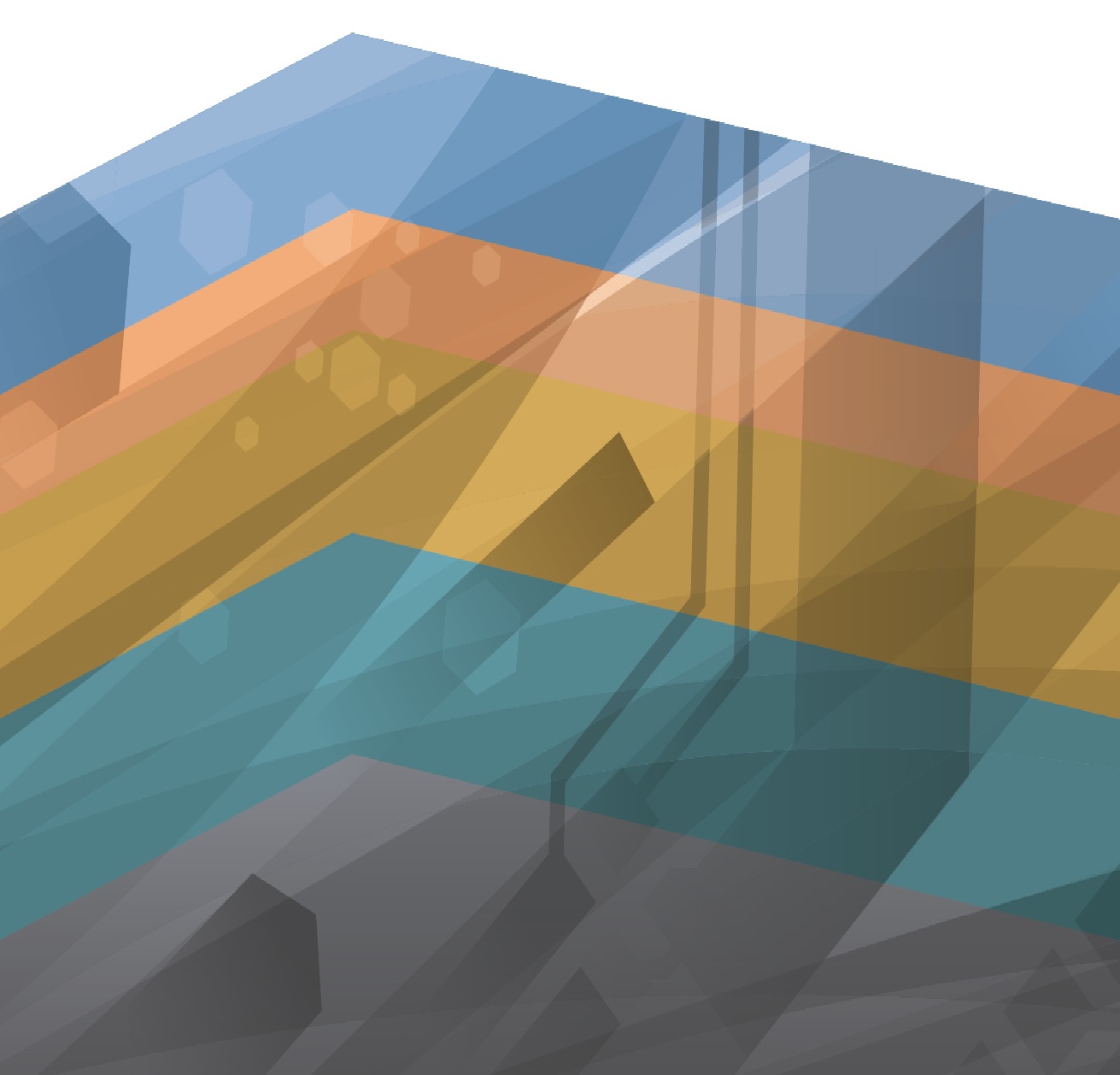
**IT Disaster Recovery Workbook and Template**

****[includes sample content]

# How to Use this Document

## Directions

Developing an IT disaster recovery plan involves choosing the right people to be involved, following a process and selecting technologies as outlined in the *IT Disaster Recovery Planning Guide* on pages 10-12. Some preparatory work needs to be completed prior to developing a documented IT disaster recovery plan. This document is split into two sections:

| **Section** | **Description** |
| --- | --- |
| Section I: Disaster Recovery Planning Workbook | Assists with working through steps 1, 2 and 3 of the IT Disaster Recovery Guide to obtain authorization, establish planning priorities and determine the technical approach. |
| Section II: IT Disaster Recovery Plan Template | Provides an IT Disaster Recovery Plan template with some sample content included that you can refer to when you are developing your DR plan. |

## 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.

**IT Disaster Recovery Planning Workbook**

[includes sample content]

Table of Contents for Disaster Recovery Planning Workbook

[I. Disaster Recovery Planning Workbook 5](#_Toc433182812)

[How to Use This Workbook 5](#_Toc433182813)

[Step 1: Obtain Management Commitment and Authorization 5](#_Toc433182814)

[Gather Background Info - Optional 5](#_Toc433182815)

[Determine Next Steps 5](#_Toc433182816)

[Step 2: Establish Planning Priorities 7](#_Toc433182817)

[Step 2.1: Identify Critical Services 7](#_Toc433182818)

[Step 2.2: Assess Impact of Service Outages 8](#_Toc433182819)

[Step 2.3: Assess Risks 8](#_Toc433182820)

[Step 2.4: Classify and Prioritize 9](#_Toc433182821)

[Step 2.5: Set Scope 10](#_Toc433182822)

[Step 3: Determine Technical Approach 11](#_Toc433182823)

[Step 3.1: Determine Technical Approach for Each Service 11](#_Toc433182824)

[Step 3.2: Develop Facility and Infrastructure Plan 12](#_Toc433182825)

[Step 3.3: Develop Cost Estimates and Schedule 12](#_Toc433182826)

# Disaster Recovery Planning Workbook

This section assists with working through steps 1, 2 and 3 of the *IT Disaster Recovery Planning Guide* to obtain authorization, establish planning priorities and determine the technical approach.

## How to Use This Workbook

The content in grey text is sample content that you can refer to or adapt as you complete the workbook.

## Step 1: Obtain Management Commitment and Authorization

Effective IT disaster recovery planning requires commitment from all business/education 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. This step commits the school authority to having a disaster recovery plan and facilitates the development of a plan by making it easier to obtain time and resources from other areas of the organization.

### Gather Background Info - Optional

If you are not aware of the current status of IT disaster recovery planning/business continuity planning at your school authority, consider gathering the following information before proceeding (see section 1.4 of the *IT Disaster Recovery Planning Guide* for more information):

| **Info to gather** | **Response** |
| --- | --- |
| Administrative procedure or policy that specifies requirement to maintain a business continuity plan or IT disaster recovery plan (if available): | Operations of Schools in Emergency Circumstances |
| Location of current IT disaster recovery plan (if available): |  |
| Date IT disaster recovery plan was last updated: |  |
| Gaps or outdated info in plan: |  |
| Person responsible for maintaining disaster recovery or business continuity plan: |  |

### Determine Next Steps

After gathering background information, consider what needs to be done to obtain management commitment and authorization (if needed).

Some possible steps:

* Determine the level of awareness and support among senior leaders for developing an IT disaster recovery plan.
* Prepare a brief presentation to senior leaders that outlines the issues, including why this is important, what has already been done, an overview of the process and next steps.

The sample slide deck included with this toolkit can be used as a starting point for preparing to meet with senior leaders.

**Disaster Recovery Toolkit - Resource**

***Building the Case for DR Planning* slide deck**

* Build The Team
  + Determine if a steering committee needs to be formed. An existing governing body with an appropriate mix of stakeholders may already exist. For example, a technology steering committee or change advisory board may be suitable. See section Roles and Responsibilities on page 10 of the *IT Disaster Recovery Planning Guide* for more details.

**Disaster Recovery Steering Committee Members (if needed)**

| **Member Name** | **Position** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

* + Decide who will be on the working group

**Disaster Recovery Working Group Members**

| **Member Name** | **Position** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

* Develop/Revise Administrative Regulation

If needed, follow your school authority’s current process to develop or revise an administrative regulation or policy statement.

## Step 2: Establish Planning Priorities

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. The following activities help establish planning priorities:

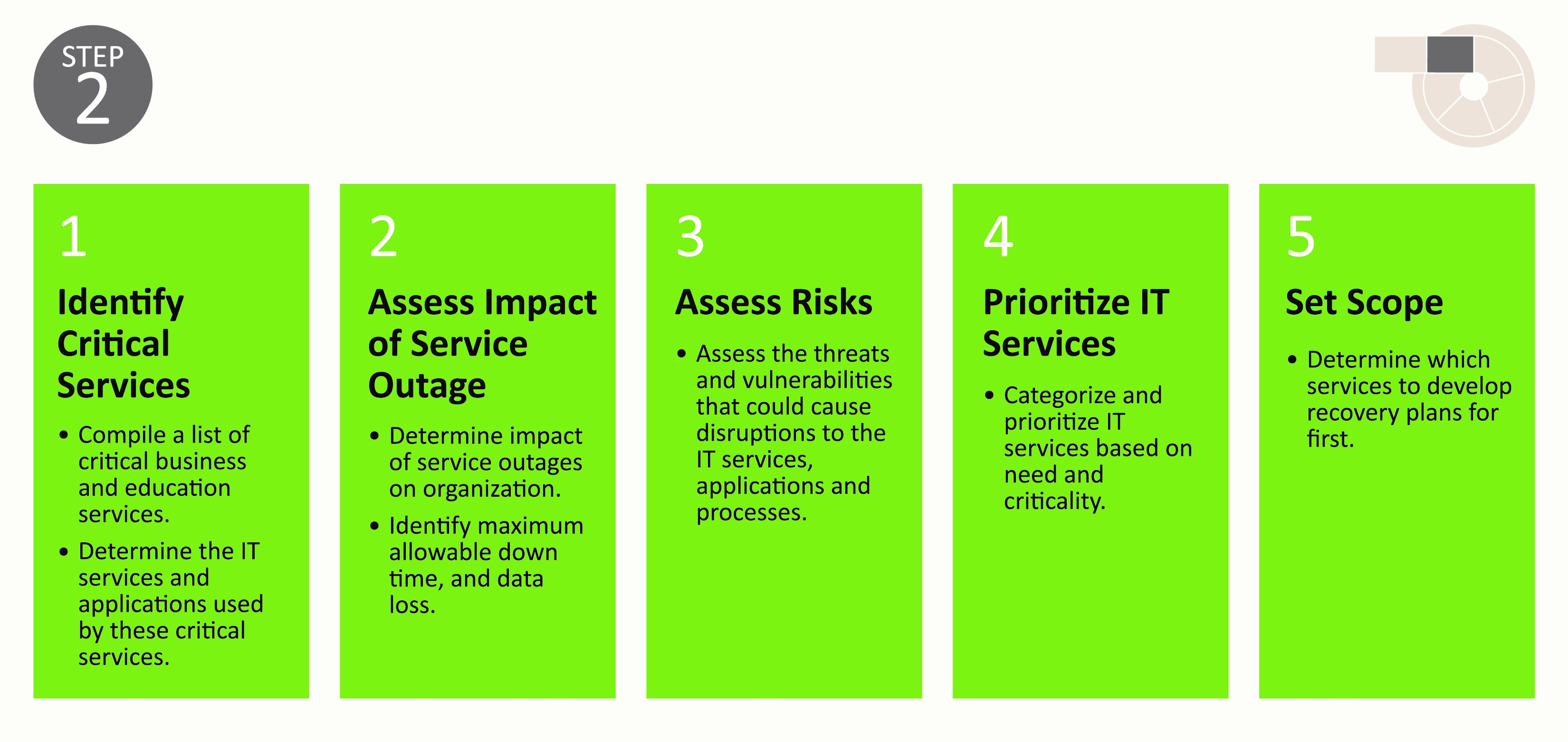


Figure 1: Phases for Establishing Planning Priorities

### Step 2.1: Identify Critical Services

Work with each department at your school authority to identify critical business and education services. Identify the supporting technology applications or services used for each business or education service.

Fill in the table below to capture this information (some sample content has been included). Definitions of the column headings are included in the glossary.

| **Department** | **Process or Service** | **Current Location** | [**Criticality Period**](#_Criticality_Period) | **Manual Workaround** | **Maximum Allowable Outage Time** | [**Supporting IT Services or Applications**](#_Applications) |
| --- | --- | --- | --- | --- | --- | --- |
| Financial Services | Payroll | Central Office | Last Week of Month | None | 24 hours | SRB Financial Services |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

See Appendix A – Sample Critical Services for examples of critical functions or services to include.

### Step 2.2: Assess Impact of Service Outages

Determine the impact of service outages and the required recovery time objective (how soon the service needs to be recovered) and recovery point objective (how much data can be lost).

Fill in the table below to capture this information. Note that the columns with grey backgrounds contain information that was captured in the previous step.

|  | | | [**Impact if Business Service is Not Available**](#_Business_Impact) | | | | | **Time Sensitivity** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dep’t** | **Service** | **Supporting IT Services or Applications** | **Safety/**  **Human Life** | **Financial** | **Operations** | **Reputation** | **Regulatory/**  **Legal/ Contractual** | [**Recovery Time Objective**](#_Recovery_Time_Objective) | [**Recovery Point Objective**](#_Recovery_Point_Objective) |
| Finances | Payroll | SRB Financial Services | Minor | Major | Major | Moderate | Major | 24 hours | 24 hours |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

### Step 2.3: Assess Risks

Document the known risks that could cause disruptions to IT services, applications and processes. For example, a server room that does not have a backup source of power will mean that services will not be available during a power outage. Specify the implications if the risk occurs and whether or not a strategy needs to be developed to address the risk.

Fill in the table below to capture this information. Note that the columns with grey backgrounds contain information that was captured in previous steps.

| **Department** | **Process**  **or Service** | **Supporting IT Services or Applications** | [**Known Risks**](#_Known_Risk_1) | **Implications** | **Need Strategy to Address?** |
| --- | --- | --- | --- | --- | --- |
| Finances | Payroll | SRB Financial Services | No backup power supply | Finance information will not be available if there is a power outage | Yes, make plans to install a backup generator |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Step 2.4: Classify and Prioritize

The next steps is to classify and prioritize IT Services based on need and criticality.

Fill in the table below to capture this information. Include core IT services that other IT services or applications depend on in order to function under the “Dependencies” section of the table. For example, the financial services application in the first line below depends on Network Infrastructure and SuperNet in order to function.

|  | | | **Time Sensitivity** | |  | |
| --- | --- | --- | --- | --- | --- | --- |
| **Department** | **Process**  **or Service** | **Supporting IT Services or Applications** | **Recovery Time Objective** | **Recovery Point Objective** | [**Service Classification**](#_Service_Classification) | [**Service Tier**](#_Service_Tier_–) |
| Finances | Payroll | SRB Financial Services | 24 hours | 24 hours | Critical | Tier 1 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Dependencies | | | | | | |
|  |  | Network Infrastructure | 12 hours | 12 hours | Critical | Tier 0 |
|  |  | SuperNet Connectivity | 12 hours | 12 hours | Critical | Tier 0 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Step 2.5: Set Scope

Based on the set of prioritized services from step 2.4, determine which services will be in scope for this iteration of disaster recovery planning and which will be left to a later date. Consider documenting core IT services and infrastructure used by other applications and services first due to their criticality. Once you have identified the list of services in step 2.5, copy the list to [Section 2 of the Disaster Recovery Plan Template](#_Scope_of_DR).

Sample list of services to include in the plan:

| **[Service](#_Service_Tier)**  **[Tier](#_Service_Tier)** | **IT Service or Application Name** | [**Recovery Time Objective**](#_Recovery_Time_Objective) | [**Recovery Point Objective**](#_Recovery_Point_Objective) |
| --- | --- | --- | --- |
| 0 | Data Centre Facility | 4 | N/A |
| 0 | Core Routing | 12 | 24 |
| 0 | Storage Services | 12 | 24 |
| 0 | Server Services | 12 | 24 |
| 0 | SuperNet Connectivity | 12 | 24 |
| 0 | Firewall Services | 12 | 24 |
| 0 | Active Directory | 12 | 24 |
|  |  |  |  |
| 1 | SRB Financial Services | 24 | 24 |
| 1 | Email | 24 | 24 |
|  |  |  |  |
|  |  |  |  |

## Step 3: Determine Technical Approach

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.



Figure 2: Determine Technical Approach

### Step 3.1: 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 develop a strategy for handling each of the following five risk scenarios. This approach will address the majority of risks to a service.

Fill in the following table to determine the technical approach for each IT Service.

| **IT Service** | **Risk Scenario** | **Recommended Technical Approach** |
| --- | --- | --- |
| SRB Financial Services | Loss of Facility Through Destructive Event | Have similar network/servers/software set up at alternate data centre. Recover data from backup. Recovery facility will function as primary facility. |
| Loss of Facility Through Non-destructive Event | Have similar network/servers/software set up at alternate data centre. Recover data from backup until access to the main facility has been restored. |
| Loss of Network | Take preventative approach through setting up redundant network components and agreement with alternate internet provider. |
| Loss of Application | Have application set up on standby server in data centre. Restore application data from backups. |
| Loss of Employees | Create more detailed documentation due to criticality of service. If needed, bring in temporary qualified staff during a disaster. |
| Student Information System | Loss of Facility Through Destructive Event |  |
| Loss of Facility Through Non-destructive Event |  |
| Loss of Network |  |
| Loss of Application |  |
| Loss of Employees |  |

### Step 3.2: Develop Facility and Infrastructure Plan

Work with your teamto 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. Document your facility plan in [*Section 3.1 Facility*](#_Recovery_Facility) *Plan* and your infrastructure plan in[*Section 3.2 Infrastructure Plan*](#_Infrastructure_Plan).

### Step 3.3: Develop Cost Estimates and Schedule

Prepare labour and technology cost estimates to implement steps 3.1 and 3.2. Develop a proposed schedule for implementation. Negotiate and obtain approval from the IT disaster recovery plan steering committee (or equivalent body).

**IT Disaster Recovery Template**

[includes sample content]

Table of Contents for Disaster Recovery Template

[II. IT Disaster Recovery Plan Template 16](#_Toc433182853)

[How to Use This Template 16](#_Toc433182854)

[1. Authorization for IT Disaster Recovery Plan 17](#_Toc433182855)

[1.1 Policy/Administrative Regulation 17](#_Toc433182856)

[1.2 Objectives 17](#_Toc433182857)

[2. Scope of Disaster Recovery Plan 17](#_Toc433182858)

[2.1 Assumptions 18](#_Toc433182859)

[3. Facility and Infrastructure Plan 19](#_Toc433182860)

[3.1 Facility Plan 19](#_Toc433182861)

[3.2 Infrastructure Plan 20](#_Toc433182862)

[Voice Communications Service Recovery Plan 20](#_Toc433182863)

[Local Area Network Recovery Plan 20](#_Toc433182864)

[Recovery Plans for Additional Infrastructure Services 20](#_Toc433182865)

[4. Plan Implementation 21](#_Toc433182866)

[4.1 Roles and Responsibilities 21](#_Toc433182867)

[Disaster Recovery Team Org Chart (Optional) 21](#_Toc433182868)

[Incident Commander 21](#_Toc433182869)

[Incident Manager (IT Lead) 22](#_Toc433182870)

[Facilities Team 22](#_Toc433182871)

[Network Team 22](#_Toc433182872)

[Server/Storage Team 22](#_Toc433182873)

[Applications/Processes Team 23](#_Toc433182874)

[Call List 23](#_Toc433182875)

[4.2 Disaster Response Processes 23](#_Toc433182876)

[Processes for Assess Phase 24](#_Toc433182877)

[Processes for Recover Phase 25](#_Toc433182878)

[Processes for Resume Phase 25](#_Toc433182879)

[Processes for Review Phase 25](#_Toc433182880)

[4.3 IT Service Recovery Plans 25](#_Toc433182881)

[Payroll Service Recovery Plan 26](#_Toc433182882)

[Transportation Service Recovery Plan 26](#_Toc433182883)

[5. Plan Testing 26](#_Toc433182884)

[Appendix A – IT Disaster Recovery Plan Maintenance 28](#_Toc433182885)

[Responsibility of IT Operations 28](#_Toc433182886)

[Project Team Responsibilities 28](#_Toc433182887)

[Documentation Storage 28](#_Toc433182888)

[Appendix B – Sample Critical Services 29](#_Toc433182889)

[Appendix C – Service Recovery Plan Template 30](#_Toc433182890)

[Appendix D – Sample Voice Communications Service Recovery Plan 31](#_Toc433182891)

[Appendix E – Local Area Network Recovery Plan 33](#_Toc433182892)

[Appendix F – Glossary 35](#_Toc433182893)

[Applications and Services 35](#_Toc433182894)

[Business Impact 35](#_Toc433182895)

[Impact Rating 35](#_Toc433182896)

[Criticality Period 36](#_Toc433182897)

[Known Risk 36](#_Toc433182898)

[Process 36](#_Toc433182899)

[Recovery Point Objective (RPO) 37](#_Toc433182900)

[Recovery Time Objective (RTO) 37](#_Toc433182901)

[Service Classification 37](#_Toc433182902)

[Service Tier 37](#_Toc433182903)

# IT Disaster Recovery Plan Template

This section provides a template of an IT disaster recovery plan with some sample content that can be adapted for your context.

## How to Use This Template

The content in blue text in the sections below contains instructions and is intended to be deleted. The content in grey text is sample content that you can refer to or adapt as you are developing your disaster recovery plan.

The following table shows the mapping between the steps for developing a disaster recovery plan (as listed in the *IT Disaster Recovery Planning Guide*) and the corresponding sections of the *IT Disaster Recovery Plan Template*.

| **Mapping Between Steps in the *IT Disaster Recovery Planning Guide* and this Template** | | |
| --- | --- | --- |
| **IT Disaster Recovery Guide** | | **IT Disaster Recovery Plan Template** |
| Step 1: Obtain Management Commitment and Authorization | | Section 1: Authorization for Disaster Recovery Plan |
| Step 2: Establish Planning Priorities | | Section 2: Scope of DR Plan |
| Step 3: Determine Technical Approach (for each service) | | Section 3: Facility and Infrastructure Plan |
| Step 4: Develop and Implement Plan | | Section 4: Plan Implementation |
|  | Step 4.1: Establish Roles and Responsibilities | Section 4.1: Roles and Responsibilities |
| Step 4.2: Determine Disaster Response Processes | Section 4.2: Disaster Response Processes |
| Step 4.3: Develop Detailed Service Recovery Plans | Section 4.3: IT Service Recovery Plans |
| Step 5: Test plans | | Section 5: Plan testing |
| Step 6: Build Awareness and Understanding | | No corresponding section in Template |
| Monitor and Evaluate | | Appendix A: IT Disaster Recovery Plan Maintenance |

# Authorization for IT Disaster Recovery Plan

[Instructions:

* The purpose of this section is to document why the IT disaster recovery plan was developed and the main objectives of the plan.
* This section corresponds to step 1: Obtain Management Commitment and Authorization in the *IT Disaster Recovery Planning Guide*.]

## Policy/Administrative Regulation

[Instructions:

* Document why the IT disaster recovery plan was developed.
* List applicable legislation or school authority policies/administrative regulations that specify requirements to create and maintain a business continuity plan or IT disaster recovery plan.

*For example, under Alberta’s privacy laws, school authorities are required to safeguard copies of personal information (including metadata) from unauthorized access, use, disclosure or destruction. An IT disaster recovery plan can help mitigate the risk of disclosure or destruction of digital student and staff information as the result of an event or disaster*.]

This plan has been created as per the requirements of the following administrative regulations:

1. **Creation, Use and Maintenance of District Information**

Board Policy Code: CN.AR

1. **Operation of Schools in Emergency Circumstances**

Board Policy Code: DBC.AR

## Objectives

[Instructions:

* Document the main objectives of the IT disaster recovery plan.]

[The IT Department] has developed this IT disaster recovery plan to be used in the event of a significant disruption to critical IT services at [School Authority]. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption so that critical IT and telecommunication services continue within an appropriate period of time after an incident has occurred.

# Scope of Disaster Recovery Plan

[Instructions:

* The purpose of this section is to list the IT services covered in the scope of this IT disaster recovery plan, as well as the recovery time objectives, recovery point objectives and order in which to recover these services.
* This section corresponds to step 2: Establish Planning Priorities in the *IT Disaster Recovery Planning Guide*.]

Sample list of services covered in this plan:

| **[Service](#_Service_Tier_–)**  **[Tier](#_Service_Tier_–)** | [**IT Service or Application Name**](#_Applications) | **Recovery Time Objective** | **Recovery Point Objective** |
| --- | --- | --- | --- |
| 0 | Data Centre Facility | 4 | N/A |
| 0 | Core Routing | 12 | 24 |
| 0 | Storage Services | 12 | 24 |
| 0 | Server Services | 12 | 24 |
| 0 | WAN Connectivity | 12 | 24 |
| 0 | Firewall Services | 12 | 24 |
| 0 | Active Directory | 12 | 24 |
|  |  |  |  |
| 1 | Payroll | 24 | 24 |
| 1 | Email | 24 | 24 |

## Assumptions

[Instructions:

* Consider listing assumptions that must be true in order to meet the specified recovery time objectives and recovery point objectives.]

This IT disaster recovery plan intends to provide the school authority with the necessary information needed to resume information technology services in a proper and timely manner to support the identified essential business processes for the following scenarios:

* destruction or inability to access data centre/server room facility;
* loss of systems (network and/or applications); and
* loss of employees.

In addition, the detailed recovery procedures as well as recovery strategies, estimated recovery time objectives and recovery point objectives are based on the following general assumptions and will need to be validated:

* continuous efforts to allocate the space required in the current data centre to restore information systems in case this site is deemed unavailable;
* continuous efforts to establish the alternate site for the current data centre in case the data centre is deemed unavailable; and
* backups are readily available to initiate restoration efforts.

Staff

* Key IT staff or their alternates required to assist in the recovery efforts will be available.
* IT staff involved in recovery efforts have the necessary technical skills to restore critical information systems identified in this document.

Users

* Key users will have their laptops or a suitable device with them during a disaster.
* Key users will have internet access and telephone/voice communication capability available to work from a remote location.

Networking

* There is ample bandwidth at the recovery site to connect to the internet.
* Bandwidth expansion is possible at the recovery site.
* Configuration files can be uploaded to network devices through a laptop or other type of device.

Note: assumptions for each specific IT service are listed in a different section.

# Facility and Infrastructure Plan

[Instructions:

* The purpose of this section is to document plans for recovering IT services in an alternate facility (if required), and plans for recovering infrastructure.
* This section corresponds to step 3.2: Develop Facility and Infrastructure Plan in the *IT Disaster Recovery Planning Guide* and answers the key questions:
  + Where will we go when a disaster occurs?
  + How will we restore our infrastructure services?]

## Facility Plan

[Instructions:

Consider documenting items such as:

* the power, infrastructure and space requirements for a recovery facility;
* the circumstances under which a recovery facility will be used;
* who is authorized to make the decision to use it;
* who will be involved in setting up the recovery facility; and
* where the recovery facility is located and plans to identify an alternate facility if needed.]

**Facility Requirements**

| **Requirement** | **Description** |
| --- | --- |
| Power |  |
| Infrastructure |  |
| Space |  |

If the incident manager determines that the primary facility is no longer sufficiently functional or operational to restore normal business operations, the team will be instructed that the recovery of systems will be done at the recovery facility. Once this determination has been made, the facilities team will be engaged to bring the alternate facility to a functional state. The incident manager will co-ordinate travel and logistics to ensure that the team can operate out of the alternate site.

If the recovery facility is unavailable, the facilities team will contact hotels, other schools or public buildings to see if they can provide the required space and power.

## Infrastructure Plan

[Instructions:

* Focus on recovering the minimum core infrastructure required to recover mission critical IT services.
* Create a separate section in the document for each core service that includes detailed recovery procedures.
* See Appendix C – Service Recovery Plan Template for suggestions of the types of information to include in the service recovery plan for each service.]

**Sample List of Critical Infrastructure Services:**

| **System** |
| --- |
| Voice Communications |
| Local Area Network (LAN) |
| Wide Area Network (WAN) |
| Server – Hosts |
| Storage – Device 1 |
| Core Network |
| Firewalls |
| Remote Connectivity |
| … |
| … |
| … |

### Voice Communications Service Recovery Plan

[Instructions:

See Appendix D – Sample Voice Communications Service Recovery Planfor an example of what the recovery plan might look like.]

### Local Area Network Recovery Plan

[Instructions:

See Appendix E – Sample Local Area Network Recovery Planfor an example of what the recovery plan might look like.]

### Recovery Plans for Additional Infrastructure Services

[Instructions:

Include service recovery plans for additional infrastructure services as identified in the table above.]

# Plan Implementation

## Roles and Responsibilities

[Instructions:

* The purpose of this section is to document roles, responsibilities and contact information for the disaster recovery team in order to respond effectively to an incident or disaster.
* Depending on the size and organization of your team, some roles may be combined.
* This section corresponds to step 4.1: Establish Roles and Responsibilitiesin the *IT Disaster Recovery Planning Guide*.]

### Disaster Recovery Team Org Chart (Optional)

[Instructions:

Consider adding an org chart to show the team roles and how they are interrelated.]

The following chart shows the key roles involved in preparing for and responding to a disaster. It also shows that the IT incident manager usually reports to an incident commander who is in charge of the overall response to a disaster.

Figure 3: Sample Disaster Recovery Team Org Chart

### Incident Commander

[Note: The incident commander’s responsibilities are likely documented elsewhere already as they are in charge of the overall response to a disaster.]

### Incident Manager (IT Lead)

The disaster recovery incident manager is responsible for making all decisions related to the IT disaster recovery efforts. This person’s primary role is to guide the disaster recovery process. The entire IT recovery team reports to this person during an incident.

**Responsibilities**

* Initiate the IT disaster recovery call tree.
* Provide status updates to senior leaders and information needed for making decisions.
* Co-ordinate communications.

### Facilities Team

The facilities team is responsible for all issues related to the physical facilities that house IT systems, including both the primary and recovery facilities. They also are responsible for assessing the damage and overseeing the repairs to the primary location in the event of the primary location’s destruction or damage.

**Responsibilities**

* Ensure that the recovery facility is maintained in working order.
* Ensure transportation, sufficient supplies, food and water and sleeping arrangements are provided for all employees working at the recovery facility.
* Assess physical damage to the primary facility.
* Ensure that measures are taken to prevent further damage to the primary facility and appropriate resources are provisioned to rebuild or repair the main facilities if necessary.

### Network Team

The network team is responsible for assessing damage to network infrastructure and for providing data and voice network connectivity during a disaster.

**Responsibilities**

* Assess damage to network infrastructure at the primary facility and prioritize the recovery of services in the manner and order that has the least impact.
* Communicate and co-ordinate with third parties to ensure recovery of connectivity.
* Ensure that needed network services are available at the recovery facility (if needed).
* Restore network services at the primary facility.

### Server/Storage Team

The server/storage team is responsible for providing the physical server and storage infrastructure required to run IT operations and applications.

**Responsibilities**

* Assess damage to servers/storage and prioritize the recovery of servers and storage devices in the manner and order that has the least impact.
* Ensure that servers and storage services are kept up-to-date with patches and copies of data.
* Ensure appropriate back-ups.
* Install and implement required tools, hardware and systems in the facilities.

### Applications and Processes Team

The applications and processes team is responsible for ensuring that all applications operate as required to meet organization objectives as well as managing IT processes that are fundamental to support the recovery of IT services and applications (for example: incident management, change management, etc.).

**Responsibilities**

* Assess impact to applications and prioritize the recovery of applications in the manner and order that has the least impact.
* Ensure that the following IT processes are followed when managing applications:
  + incident management;
  + change management;
  + access provisioning;
  + security; and
  + other.
* Ensure that servers in the facilities are kept up-to-date with application patches and copies of data.
* Install and implement any tools, software and patches required in the facilities as appropriate.

### Call List

[Instructions:

Document the names, roles and contact information of leaders and team members responsible for responding to an incident and handling recovery efforts.]

| **Name** | **Role/Title** | **Work Phone Number** | **Mobile Phone Number** | **Home Phone Number** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

## Disaster Response Processes

[Instructions:

* The purpose of this section is to document key processes for responding to a disaster as this increases the speed and effectiveness of response.
* Consider including the following information for each process:
  + process name & description;
  + steps;
  + inputs/outputs; and
  + roles (i.e., who is involved in executing the process?).
* This section corresponds to step 4.2: Determine Disaster Response Processes in the *IT Disaster Recovery Planning Guide*.]

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.

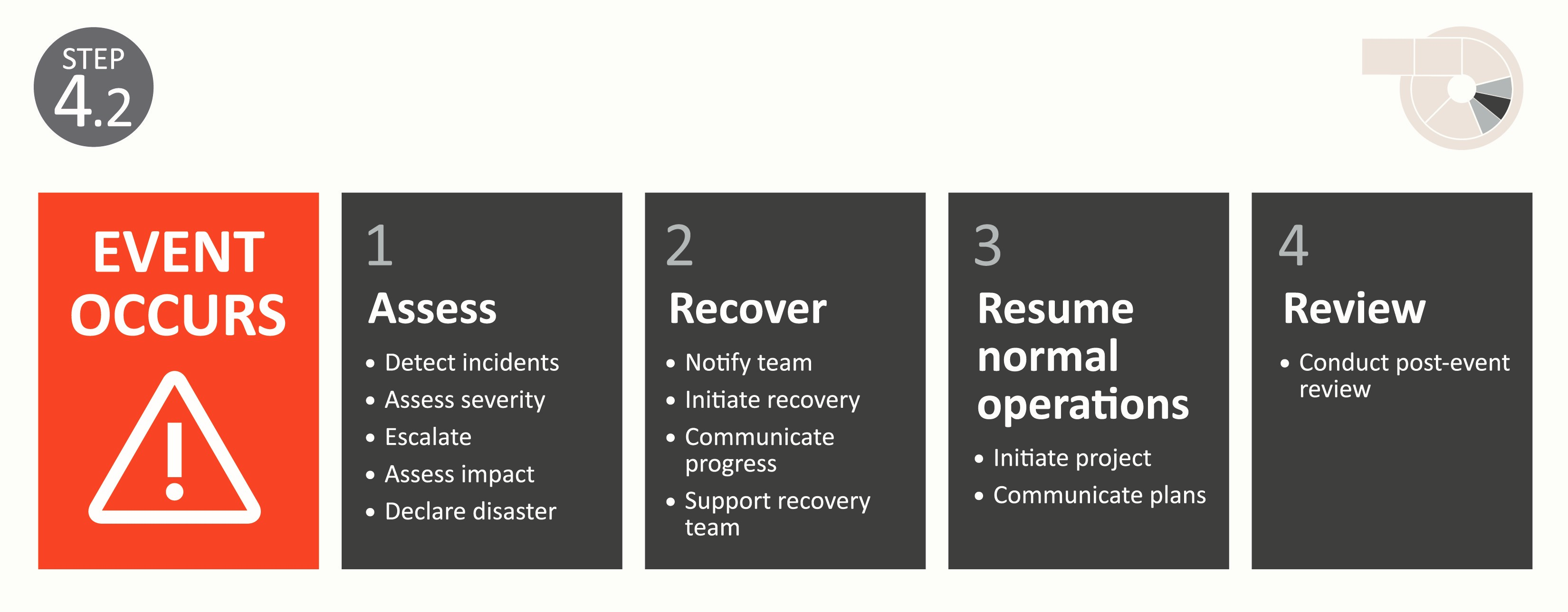


Figure 4: Disaster Response Process Overview

### Processes for Assess Phase

#### Process to Assess Severity of Incident or Event

[Instructions:

* Document the process for determining the severity of the incident and provide escalation criteria.
* Tips:
  + Handle minor incidents causing service outage through incident response procedures. Escalate severe incidents such as loss of all communications, loss of power, flooding/fire, or loss of the building to appropriate personnel.
  + Document linkages with service desk processes.]

#### Process to Escalate Severe Incidents

[Instructions:

* Document the escalation process for engaging the IT team and senior leadership to assess the impact of the incident.]

#### Process to Assess Impact

[Instructions:

* Document what information needs to be gathered to declare a disaster such as approximate amount of damage and estimated recovery time.
* Include recommendation to recover in place or to declare a disaster and begin recovery in an alternate site.]

#### Process to Declare Disaster

[Instructions:

* 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.]

### Processes for Recover Phase

#### Process to Notify Team

[Instructions:

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

#### Process to Initiate Recovery

[Instructions:

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

#### Process to Communicate Progress

[Instructions:

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

#### Process to Support Recovery Team

[Instructions:

* Document 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.]

### Processes for Resume Phase

#### Process to Resume Normal Operations

[Instructions:

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

### Processes for Review Phase

#### Process to Conduct Review

[Instructions:

* Document the process for conducting a review and determining lessons learned. Include broad based group of stakeholders for the post‑event review.]

## IT Service Recovery Plans

[Instructions:

* The purpose of this section is to document plans for recovering IT services identified in step 2.5 – Set Scope*.*

*Note: This section does not include core infrastructure services, which are documented in* [Section 3.2](#_Recovering_Critical_Infrastructure) *of the IT Disaster Recovery Plan).*

* See [Appendix C –Service Recovery Plan Template](#_Appendix_C_–) for suggestions of the types of information to include in the service recovery plan for each service.
* This section corresponds to step 4.3: Develop Detailed Service Recovery Plansin the *IT Disaster Recovery Planning Guide*.]

**Sample List of IT Services:**

| **System** |
| --- |
| Payroll |
| Transportation |
| Financial Services |
| Student Information System |
| … |
| … |
| … |

### Payroll Service Recovery Plan

[Instructions:

See [Appendix C – Service Recovery Plan Template](#_Appendix_C_–) for suggestions of the types of information to include in the service recovery plan.]

### Transportation Service Recovery Plan

[Instructions:

See [Appendix C – Service Recovery Plan Template](#_Appendix_C_–) for suggestions of the types of information to include in the service recovery plan.]

# Plan Testing

[Instructions:

* The purpose of this section is to document why plan testing and review is important, how often the disaster recovery plan will be tested and what types of tests will be executed.
* This section corresponds to step 5: Test the Planin the *IT Disaster Recovery Planning Guide*.]

Disaster recovery plan reviews are an essential part of the plan development process. Building a quality IT disaster recovery plan is a team activity, so practice and testing are critical to success.

Periodic disaster recovery plan reviews need to happen, because non-technical changes can affect the plans.

1. Reflect any updated organizational priorities, changes or goals.
2. Ensure that all team lists are up to date.
3. Ensure that call lists are up to date.
4. Confirm that changes due to configuration changes in the environment have been made.

The goal of a good disaster recovery plan is that it can be executed smoothly and effectively at any time. To make this happen, everyone that has a role to play in the plan needs to be involved in practicing.

The disaster recovery plan will be tested every six months in order to ensure that it is still effective. Each period, a table top walkthrough, disaster simulation, or full failover testing will be executed (see step 5.4 in the *IT Disaster Recovery Planning Guide* for more details about the different types of tests).

# Appendix A – IT Disaster Recovery Plan Maintenance

[Instructions:

* The purpose of this section is to document how the organization will manage maintenance of the plan over time.
* This section corresponds to step 7: Monitor and Evaluatein the *IT Disaster Recovery Planning Guide*.]

Over time, the disaster recovery needs of the organization will change. The following responsibilities and processes need to be executed to ensure a useful plan remains in place.

## Responsibility of IT Operations

[Instructions: If your school authority has implemented service management processes such as ITIL, delegate plan update responsibility to the change advisory board (CAB).]

The IT operations team will be responsible for the day-to-day management of the disaster recovery plan. The specific responsibility is delegated to the change advisory board (CAB). Whenever changes are made to the environment CAB is responsible for ensuring that they are fully reflected and tested in the disaster recovery plan.

This will make updating the disaster recovery plan a part of the formalized change control procedures under the management of the IT director.

## Project Team Responsibilities

[Instructions: As part of your project discipline, make disaster recovery plan updates part of your transition to operations process.]

Each project will, as part of their transition to operations, plan to ensure that all documentation related to recovery of the system is updated when making a change.

## Documentation Storage

[Instructions: Decide where and how you will access your documentation in the event of a disaster.]

Each member of the disaster recovery team will be issued a USB flash drive with the disaster recovery plan documentation. A master copy will be stored in a cloud based location. Printed copies of the plan are to be kept at all IT staff homes.

The online version can be accessed at:

URL: [www.online.com](http://www.online.com)

UserID: DRplanning

Password: DRPlanAccesss

# Appendix B – Sample Critical Services

The following list contains examples of critical services that school authorities typically provide. This list can assist with developing the list of services for step 2: Establish Planning Priorities*.*

| **Department** | **Critical Services or Functions (Example)** |
| --- | --- |
| Finance | * Cash and liquidity management * Commercial card processing * Receiving and paying emergency invoices and disbursements |
| Transportation | * Transportation services |
| Human Resources | * Corporate communication * Moral support * Processing payroll |
| Superintendent | * Crisis communication * Labour relations |
| Learning / Education Services | * Learning services |
| Facilities | * Emergency property acquisition and infrastructure setup * Physical security * Contract services and unplanned maintenance * Providing utilities (power, gas, water and sewage) |
| Information Technology | * Help desk * Access management * Change management * IT procurement * Request fulfillment |
| Others | * General council * Critical incident response team * Mail room |

# Appendix C – Service Recovery Plan Template

[Instructions: The purpose of this template is to provide an overview of the information to consider including in a service recovery plan.]

#### Responsibility

[Specify who is responsible for managing this service as well as any backup contacts in the event they are not available.]

#### Service Context

[Document the service context such as:

* Who uses the service.
* Criticality periods (i.e., periods during which the service is critical such as for payroll processing or year-end processes, etc.).
* Contact information for vendors and other personnel such as database administrators and application owners.]

#### Service Classification

[Specify the classification of this service (critical, vital, necessary or desired) as determined in step 2.4 – Classify and Prioritize of the *IT Disaster Recovery Planning Guide*.]

#### Recovery Strategy and Location

[Specify the overall strategy for recovering this service as well as where the service will be recovered.]

#### Assumptions

[Specify any assumptions required to follow the recovery procedure, such as the ability to restore from backups, etc.]

#### Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

[Specify the recovery time objective and recovery point objective for this service as determined in step 2.2 – Assess Impact of Service Outages of the *IT Disaster Recovery Planning Guide*.]

#### Recovery Platform

[Specify the technology platform required to restore this service. For example, virtualized Windows servers configured similar to the current production environment.]

#### Recovery Procedure

[Consider providing an overview of the major steps of recovery before providing detailed recovery procedures. Select the minimum level of documentation possible that reduces risk to an acceptable level as more detailed documentation requires more time to create and maintain. See page 28-29 of the *IT Disaster Recovery Planning Guide* for more information.]

#### Test Procedure

[Specify how the service can be tested to ensure that it’s working correctly.]

#### Resume Procedure

[Specify how to resume the service after the event has been addressed.]

# Appendix D – Sample Voice Communications Service Recovery Plan

[Instructions: This appendix contains sample content for a Voice Communications Service Recovery Plan.]

#### Responsibility

* John Smith, IT Manager, Communications
* Backup: Jim Beauchamp

#### Priority

Critical [specify Critical, Vital, or Necessary]

#### Recovery Strategy and Location

* The updated procedure will be available when the standby arrangement with the third-party technology partners is determined. The current solution requires a disaster recovery team member to contact Bell to switch the main phone line to a standby line with a pre-recorded message.
* Acquisition of systems necessary for telephone communications. Contact Avaya to prepare for the recovery.
* Tape restoration of configuration data.
* Telephone system will be restored at the data centre. Future strategy may change if the telephone system (partially or as a whole) will be migrated to the XXX location for daily operations.

#### Assumptions

* Necessary servers will be set up on a **best effort basis**.
* A standby arrangement with third party technology partners will be established in the future.
* A critical escalation support arrangement with third party technology is available.
* The configuration information can be restored from tape.
* Four telephone lines are readily available. Three for customer broadcast and one for internal communication.

#### Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

* RTO: Best effort.
* RPO: Best effort.

#### Recovery Platform

Windows servers with similar configuration as in production environment.

#### Recovery Procedure

* The procedure will be updated when the standby arrangement with the third-party technology partners is determined. The following steps will be implemented:
  + Contact Avaya to arrange technical support. When the recovered server is available, arrange Avaya technician to install the phone system.
* As a short-term solution, voice mailboxes can be arranged in advanced and pre-recorded messages can be implemented to keep customers and business partners aware of the incident status. The following phone lines will be addressed by the following procedure:
  + Reception phone number xxx-xxx-xxxx and line xxx-xxx-xxxx will share the standby line.
  + Other lines.
* During an incident, our designated member(s) will contact Bell using the contact information documented in VMC Vendor Escalation Contact List to activate the re-route. Use the passcode documented in the password file as indicated to update the broadcast message and collect voice messages to distribute to the proper BCP/DRP members. RTO can be revised once this solution is established.
* For fax services, our designated member(s) will contact Myfax to start archiving our fax to a special email account. The designated member will follow the procedure documented in IT Operations Manual to retrieve the fax emails.

#### Test Procedure

* Logon to Avaya server as administrator. Connect to Avaya Console and retrieve historical data to confirm connectivity.

#### Resume Procedure

* Contact Avaya to arrange technical support. When the production server is available, arrange Avaya technician to be on-site and transfer the configuration and user data from recovery system.
* Contact Bell to switch the main line back to the phone system.
* Contact Myfax to redirect the fax emails back to our email.

# Appendix E – Local Area Network Recovery Plan

[Instructions: This appendix contains sample content for a Local Area Network Service Recovery Plan.]

#### Responsibility

* John Smith, IT Manager, Communications
* [identify backup if available]

#### Priority

Critical [specify Critical, Vital, or Necessary]

#### Recovery Strategy and Location

….

#### Assumptions

* Racks and power are available
* Other

#### Network Diagram



#### Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

* RTO: 6 hours.
* RPO: 6 hours.

#### Recovery Platform

….

#### Recovery Procedure

Overview of major steps:

1. Rack Gear
2. Patch to switches
3. Configure Router

Details for each step:

1. Rack Gear

* Mount Gear
* Confirm power
* Patch to Servers
* Connect to WAN
* Login and update switch
* Configure rules
* …

Configure the following rules for the core and edge router:

**Core**

| **Rule** | **Source** | **Destination address & port** | **Complete** |
| --- | --- | --- | --- |
| Explicit Traffic only | Internal | Deny All |  |
| Permit HTTPS |  |  |  |
| Permit Mail Traffic |  |  |  |
| Permit WebApp1 |  |  |  |
| … |  |  |  |

**Edge**

| **Rule** | **Source** | **Destination address & port** | **Complete** |
| --- | --- | --- | --- |
| Explicit Traffic only | Internal | Deny All |  |
| Explicit Traffic only | Internet | Deny All |  |
| Permit HTTPS | Internet | Server : 443 |  |
| Permit Mail Traffic | Internal SMTP Server : 25 | All Internet SMTP: 25 |  |
| Permit DNS |  |  |  |
| … |  |  |  |

# Appendix F – Glossary

## Applications and Services

Identify any IT applications or IT services required for the completion of the identified processes. Consider applications that are both supported internally and through third party vendors or are located in the cloud.

## Business Impact

A business disruption can impact an organization in several ways. There are five main categories that are used to measure impact:

* safety/human life;
* financial;
* reputation;
* operations; and
* regulatory/legal/contractual.

### Impact Rating

In order to effectively assess the impact of a disruption throughout the organization, it is necessary to use a common metric to assess impacts across the various business services and their individual processes. For each of the identified processes, identify the impact in each of the applicable categories based on the values found in the table below. Note that it may be prudent to give dollar figures for the financial and regulatory/legal/contractual categories where the loss exposure (the amount of potential monetary losses) is a known amount.

The timeframe for the impact should be based on the time-sensitivity values previously identified.

| **Rating** | **Description / Example** |
| --- | --- |
| Catastrophic | The consequences would threaten the provision of essential school authority processes, causing major problems for clients and require immediate executive involvement and action.   Disruption would have extreme consequences for school authority (e.g., major damage or destruction, imminent threat to human safety, loss of life or major/multiple injuries, extreme monetary losses to school authority). |
| Major | The consequences would threaten continued effective provision of school authority processes and require executive involvement.   Disruption would have very high consequences for school authority (e.g., significant damage or destruction, some minor injuries or threat to human safety with no loss of life, high monetary losses to processes). |
| Moderate | The consequences would not threaten the provision of school authority processes, but would mean the business operations and administration could be subject to significant review or changed ways of operating. Executive involvement would likely be required.   Disruption would have medium consequences (e.g., no loss of life or injuries, moderate monetary losses to school authority). |
| Minor | The consequences would threaten the efficiency or effectiveness of some school authority processes but would be dealt with at the business unit or department level.   Disruption would be of low consequence to school authority (e.g., no loss of life or injuries, low monetary losses to school authority). |

## Criticality Period

|  |
| --- |
| A criticality period is any point during which the identified process is critical and may affect the recovery time objective (RTO). |
| It is possible that a process may have multiple criticality periods or none at all; this is highly dependent on the nature of the process. Criticality periods may be cyclical or one-offs and may range from months to hours in length. |
| Examples of criticality periods include:   * year-end processing; * regulatory deadlines; * payroll processing; and * scheduled events. |
| A manual workaround is a non-IT dependent action undertaken to circumvent the loss of IT systems in order to complete a process. Manual workarounds are usually short-term stopgaps and are not intended to be implemented indefinitely. |
| Identify any manual workarounds that may exist for each of your processes. |

## Known Risk

A known risk is anything that may negatively impact business as usual. Identify any concerns or threats you have identified or feel may affect your normal operations.

## Process

A process is a service the business unit carries out in the course of normal day-to-day operations. It is essential to account for all processes when conducting a business impact analysis in order to assign categories of time-sensitivity and tailor contingency plans accordingly.

|  |
| --- |
| 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)1. 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. |

## 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)[[1]](#footnote-1). 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.

## Service Classification

| **Classification** | **Maximum Recovery Time** |
| --- | --- |
| 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 |

## Service Tier

The logical grouping of services to be recovered such as Tier 0, Tier 1, etc.

Core infrastructure services need to be recovered first and would be included in Tier 0. Lower numbered tiers are recovered first as they are either more critical or higher numbered tiers depend on them in order to function.

1. 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> [↑](#footnote-ref-1)