Disaster Recovery and Continuity Plan for Information Technology

[Your School System]

Created by Joseph Moody on Tuesday, October 23, 2018

Reviewed by: [REVIEWER]

Approved by: [APPROVER]

Table of Contents

[Disaster Recovery and Continuity Goal 3](#_Toc530058967)

[Purpose 3](#_Toc530058968)

[Examples 3](#_Toc530058969)

[Risks 4](#_Toc530058970)

[Purpose 4](#_Toc530058971)

[Examples 4](#_Toc530058972)

[Empty Risk Table 4](#_Toc530058973)

[Small Rural Organization Risk Table 4](#_Toc530058974)

[Large Urban Organization Risk Table 5](#_Toc530058975)

[High Impact/High Probability Risks 6](#_Toc530058976)

[Responses 6](#_Toc530058977)

[Purpose 6](#_Toc530058978)

[Examples 6](#_Toc530058979)

[Data Loss 7](#_Toc530058980)

[Fire 7](#_Toc530058981)

[Networking Failure 7](#_Toc530058982)

[Minimal Operational Services 7](#_Toc530058983)

[Purpose 7](#_Toc530058984)

[Examples 8](#_Toc530058985)

[Minimal Operational Infrastructure 8](#_Toc530058986)

[Purpose 8](#_Toc530058987)

[Examples 8](#_Toc530058988)

[Office 365/Exchange 8](#_Toc530058989)

[School Messenger 9](#_Toc530058990)

[Finance/HR 9](#_Toc530058991)

[Additional Documentation and Resources 9](#_Toc530058992)

[Purpose 9](#_Toc530058993)

[Contact Information 9](#_Toc530058994)

[Purpose 9](#_Toc530058995)

[Examples 10](#_Toc530058996)

[Plan Testing, Review, and Updates 10](#_Toc530058997)

[Purpose 10](#_Toc530058998)

[Examples 10](#_Toc530058999)

# Disaster Recovery and Continuity Goal

## Purpose

Define the recovery result and timeline for the technology resources supported. A recovery goal can be defined by the type of resources needing to be online for minimal operation and the time required to make these resources active.

Recovery environments can be grouped into three types.

* Near-instant recovery to a hot site
* Delayed recovery to a warm site
* Extended recovery to a cold site

A goal can utilize multiple types, as seen in the first example below. Alternatively, a goal could only include the safekeeping of mission-critical data until the original site is built again.

Note that creating the disaster recovery and continuity goal might be easier after outlining the Minimal Operational Infrastructure and Risks sections of this guide.

## Examples

In the event of a disaster, the school system will maintain authentication services through resources running in Azure AD. Authentication services, which include a domain controller, a federation server, and a web application proxy, allow access to communication programs (email and mass text/voice notifications).

Depending on the condition of the disaster, mission-critical software will either be quickly available from the high school hot site or recovered to a warm site at the middle school. Initial recovery will focus on financial, human resources, and support software.

Our school system recognizes that threats could exist that may damage or destroy the ability to continue normal business operations following a serious unexpected disruptive incident. The organization has a high level of dependency upon its automated systems and processes, and this creates risks that need to be mitigated.

This Information Systems (IS) Continuity Plan has been prepared to assist the organization to manage a problem that affects our information systems in a controlled and structured manner. It contains information on emergency contact details, strategies to mitigate impact, procedures to be implemented, and communication processes to be followed in response to an emergency.

# Risks

## Purpose

Copy and fill in the generic risk table. Decide on the likelihood and impact of each risk. Try to imagine any potential systematic threat to IT that is not listed and add it to the table. Remove any risk that is not applicable to your area. If possible, complete this risk table by yourself and then have at least one other person complete it as well. Compare results and decide on a final risk score.

The risk table is divided into disasters that are mainly natural and those that are not. Both Probability and Impact are rated on a five-point scale.

Probability Scale: 1 = very unlikely, 2 = unlikely, 3 = neutral chance; 4 = likely, and 5 = very likely.

Impact Scale: 1 = very low, 2 = low, 3= moderate, 4 = high, and 5 = very high.

## Examples

### Empty Risk Table

|  |  |  |
| --- | --- | --- |
| **Risk** | **Probability** | **Impact** |
| Earthquake |  |  |
| Fire |  |  |
| Flooding |  |  |
| Hurricane |  |  |
| Lightning |  |  |
| Tornado |  |  |
| Water damage (natural) |  |  |
|  |  |  |
| Communications Failure |  |  |
| Cooling Failure |  |  |
| Data Exposure |  |  |
| Data Loss |  |  |
| Human (external actor) |  |  |
| Human (internal actor) |  |  |
| IT Employee Loss |  |  |
| Networking Failure |  |  |
| Power Failure |  |  |
| Theft |  |  |
| Water damage (mechanical) |  |  |

### Small Rural Organization Risk Table

|  |  |  |
| --- | --- | --- |
| **Risk** | **Probability** | **Impact** |
| Earthquake | 1 | 4 |
| Fire | 2 | 5 |
| Flooding | 4 | 3 |
| Hurricane | 4 | 4 |
| Lightning | 2 | 4 |
| Tornado | 2 | 5 |
| Water damage (natural) | 3 | 4 |
|  |  |  |
| Communications Failure | 2 | 2 |
| Cooling Failure | 1 | 3 |
| Data Exposure | 2 | 4 |
| Data Loss | 2 | 5 |
| Human (external actor) | 3 | 4 |
| Human (internal actor) | 2 | 4 |
| IT Employee Loss | 1 | 3 |
| Networking Failure | 2 | 5 |
| Power Failure | 1 | 4 |
| Theft | 2 | 3 |
| Water damage (mechanical) | 1 | 3 |

Probability Scale: 1 = very unlikely, 2 = unlikely, 3 = neutral chance; 4 = likely, and 5 = very likely.

Impact Scale: 1 = very low, 2 = low, 3= moderate, 4 = high, and 5 = very high.

### Large Urban Organization Risk Table

|  |  |  |
| --- | --- | --- |
| **Risk** | **Probability** | **Impact** |
| Earthquake | 3 | 5 |
| Fire | 3 | 3 |
| Flooding | 2 | 4 |
| Hurricane | 2 | 4 |
| Lightning | 2 | 2 |
| Tornado | 4 | 5 |
| Water damage (natural) | 1 | 3 |
|  |  |  |
| Communications Failure | 2 | 3 |
| Cooling Failure | 1 | 2 |
| Data Exposure | 3 | 5 |
| Data Loss | 1 | 5 |
| Human (external actor) | 3 | 4 |
| Human (internal actor) | 2 | 4 |
| IT Employee Loss | 1 | 2 |
| Networking Failure | 2 | 4 |
| Power Failure | 1 | 3 |
| Theft | 1 | 2 |
| Water damage (mechanical) | 2 | 2 |

Probability Scale: 1 = very unlikely, 2 = unlikely, 3 = neutral chance; 4 = likely, and 5 = very likely.

Impact Scale: 1 = very low, 2 = low, 3= moderate, 4 = high, and 5 = very high.

### High Impact/High Probability Risks

After your risk table is complete, go back and highlight any row that has an impact and probability score greater than or equal to seven. These are the high impact and high probability risks for your organization and will be used in the next section.

|  |  |  |
| --- | --- | --- |
| **Risk** | **Probability** | **Impact** |
| Earthquake | 1 | 4 |
| Fire | 2 | 5 |
| Flooding | 4 | 3 |
| Hurricane | 4 | 4 |
| Lightning | 2 | 4 |
| Tornado | 2 | 5 |
| Water damage (natural) | 3 | 4 |
|  |  |  |
| Communications Failure | 2 | 2 |
| Cooling Failure | 1 | 3 |
| Data Exposure | 2 | 4 |
| Data Loss | 2 | 5 |
| Human (external actor) | 3 | 4 |
| Human (internal actor) | 2 | 4 |
| IT Employee Loss | 1 | 3 |
| Networking Failure | 2 | 5 |
| Power Failure | 1 | 4 |
| Theft | 2 | 3 |
| Water damage (mechanical) | 1 | 3 |

# Responses

## Purpose

For each high impact/high probability risk, write out a response that addresses the disaster. This section should not be very technical. Specific recovery steps will be listed in the Minimal Operational Infrastructure Section Templates, which should be customized for your organization, are provided in the examples below.

As you expand this section, you will see ways to minimize risks before of an emergency. For example, you might notice that a fire extinguisher is mounted outside a locked data room but there is not one located inside for working personnel. When you find these issues, make the changes, reevaluate the risk and edit the risk response. Your final generic disaster response should be a series of short steps because many of the compounding risk factors have already been addressed.

## Examples

### Data Loss

A disaster involving data loss includes loss of a critical server, loss of a SAN, or loss of a backup location. Data loss also includes ransomware related disasters.

* Loss of a critical server: restore with backup software.
* Loss of a SAN: restore data to alternative storage. Contact SAN support (see Contact Information).
* Loss of a backup location: repurpose secondary clusters as a temporary backup location until the original data can be restored.

### Fire

* Immediately call 911.
* Use the wall-mounted fire extinguisher if near a small fire.
* If applicable while evacuating the building, set off the fire alarm, pull the emergency power disconnect for infrastructure locations, and close any unlocked doors.

### Networking Failure

* School:
  + If cause is hardware, replace uplink switch with district spare. Copy last week’s configuration to switch.
  + If cause is connection to district, call Fiber support (see Contact Information).
  + Alert school staff through mass text service.
* Core:
  + If cause is hardware, replace core modules or move connections to secondary switch.
  + If cause is connections to schools, call Fiber support (see Contact Information).
  + Alert staff through mass text service.

# Minimal Operational Services

## Purpose

Define the applications and services that must be available during a disaster to facilitate recovery. Optionally, include services that would be needed directly after a disaster to resume normal operations.

Here are a few near universal services.

* Communications will be a priority. Multiple communication methods might be necessary to contact internal and external parties.
* Financial and human resource applications might also be considered a minimal operational service.
* Depending on the disaster, access to inventory, auditing, and previous digital records might need to be available immediately for insurance-related purposes.
* Backup and restoration processes might also be considered a minimal operational service.

## Examples

To recover from a disaster, the School System would need the following service categories and applications available:

|  |  |  |
| --- | --- | --- |
| **Service Category** | **Application** | **Purpose** |
| Communications | Office 365/Exchange | Contacting staff and students |
| Communications | School Messenger | Contacting staff and parents through text/mass calling |
| Financial/HR | Finance Works Suite | Payroll and purchasing |
| Inventory | Destiny Follett | Insurance |
| Restoration | Backup Exec (Restore Extra) | Resuming services |

# Minimal Operational Infrastructure

## Purpose

Thoroughly explain the individual pieces that are required to keep or bring minimal operational services online. The level of detail should be sufficient enough that a knowledgeable external party could complete the recovery efforts. Step-by-step instructions are not required unless a specific service is complicated and critical enough to warrant it.

Individual services can be broken down into sub-headings. Supplemental information, like network charts or hardware inventory, can be added to the Additional Documentation section that is at the end of this document.

Establishing a detailed minimal operational infrastructure guide should involve input from the departments that use the service as this can build a complete picture of the components that need to operate. For example, a plan might include failover plans for financial software but no plans for check printers.

## Examples

### Office 365/Exchange

Relies on an Active Directory Federation Services farm. This setup includes two ADFS instances, two Web application proxies, and access to domain controllers. The O365 environment is configured in a hybrid structure with an on-premise Exchange server.

Syncing between on-premise and O365 is handled by the Azure AD Sync clients, which are installed on both ADFS servers. A component of this process is password synchronization. This enables O365 to be transitioned to a standalone environment if the on-premise infrastructure is unavailable.

### School Messenger

Relies on an Active Directory Federation Services farm. This setup includes two ADFS instances, two Web application proxies, and access to domain controllers. If the on-premise infrastructure is unavailable, local School Messenger users will be used for district messages.

### Finance/HR

The financial and HR applications reside on three internal virtualized servers (Finance-01, Finance-02, and Finance-03). Each VM sites on one of the three Hyper-V clusters at the network core. See the Additional Documentation section for hardware and software inventories.

Incremental backups of each VM are created each weeknight. Full backups are created each Saturday and retained for six weeks.

If one of the three VMs were unavailable, a restoration would occur on the physical cluster or another available cluster. If primary core clusters were unavailable, VMs would be restored on the secondary site cluster.

# Additional Documentation and Resources

## Purpose

Items within this portion should assist in the recovery process. If internal IT employees are not available, any item that would be useful to an external consultant should be added. These items might include:

* Network maps
* Server and domain documentation
* Pictures of rooms/layouts
* Secondary access to department knowledge bases
* Instructions for accessing resources, including secured password databases
* Offline Multi-factor authentication codes
* Location of spare room keys/badges or network chassis keys

# Contact Information

## Purpose

Using the table below, fill in all internal and external contact and support information. For internal resources, include multiple means of communication that do not rely on company resources. For example, an external email column could be added to the sample table below. Warranty and support information for minimal operational services / minimal operational infrastructure can also be included here, even if this information is recorded in previous sections.

## Examples

|  |  |  |
| --- | --- | --- |
| **Name** | **Support Role** | **Phone** |
| Joseph Moody | Network/Server |  |
| Dell EMC | SANs |  |
| Finance Works | Financial/HR Software |  |
| Robert Jones | Secondary contact for Joseph |  |

# Plan Testing, Review, and Updates

## Purpose

Ideally, this plan and the contained resources are updated following changes made in the environment. At least once a year, this document should still be tested, reviewed, and updated. There are two separate steps to completing a review.

The first step is to update resources to reflect undocumented changes. When completing the review, it may be helpful to start from the end of the document and work toward the beginning. Update contact information and the additional documentation section. Use items, like your inventory, to update the Minimal Operational Services and Minimal Operational Infrastructure sections. Finally, evaluate the risks to your environment and the general responses to those risks.

The second step is to test these changes and these resources. Pick a response and the related risk; then implement the response as thoroughly as you can. Below are several disaster scenarios that can be used:

* Practice a response to data loss due to ransomware that was introduced accidentally by IT staff.
* Prepare for a major hurricane that is expected in three days.
* If possible, do a practice fire drill for a fire in a data room.
* Have a junior IT staff member ensure normal IT operations due to primary staff being unavailable.

Hopefully, these tests will highlight gaps in this plan before an actual disaster strikes. Changes to the plan should be added to a table in this section. If possible, previous versions of this document and the additional resources should be saved.

## Examples

|  |  |
| --- | --- |
| **Date** | **Changes** |
| 2016-08-02 | Creation of DR Plan |
| 2016-10-14 | Added completed server inventories |
| 2017-06-05 | Lowered fire risk due to suppression system. Updated fire response section. |
| 2017-12-01 | Included new KeePass database in the Additional Documentation section. |
| 2018-06-20 | Updated contact information. |