Assignment-5

Kartik Velede

8672807

Collaborative Environment Processes 1 – INFO8930

Doug Ferrier

June-19-2020

June-29-2020

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| Security Level: | Public | Version #: | 1.0.1 |
| Author: | Kartik Velede | Version Date: | June 29, 2020 |
| Owner/Approver: | Doug Ferrier | Document Status: | For Review |
| Comments: |  | | |

Contents

[1 Introduction 4](#_Toc451267388)

[1.1 Purpose 4](#_Toc451267389)

[1.2 Scope 5](#_Toc451267390)

[2 Define 5](#_Toc451267391)

[2.1 Asset Management 5](#_Toc451267392)

[**2.1.1 Hardware Assets 5**](#_Toc451267393)

[**2.1.2 Software Assets 5**](#_Toc451267394)

[**2.1.3 System Configuration 6**](#_Toc451267395)

[**2.1.4 Configuration Management Database 6**](#_Toc451267396)

[**2.1.5 Asset Management Policies and Processes 6**](#_Toc451267397)

[2.2 Business Impact Analysis (BIA) 6](#_Toc451267398)

[**2.2.1 Impact of Downtime Criteria 6**](#_Toc451267399)

[**2.2.2 Failover RTO and RPO Summary for Tier 1, 2, and 3 Applications 7**](#_Toc451267400)

[**2.2.3 Failback RTO and RPO Summary for Tier 1, 2, and 3 Applications 7**](#_Toc451267401)

[**2.2.4 List of Tier 1, 2, and 3 Applications 7**](#_Toc451267402)

[**2.2.4.1 Tier 1 (Mission-Critical) 7**](#_Toc451267403)

[**2.2.4.2 Tier 2 7**](#_Toc451267404)

[**2.2.4.3 Tier 3 7**](#_Toc451267405)

[2.3 Risk Assessment and Risk Management 7](#_Toc451267406)

[2.4 DR Duration Considerations 8](#_Toc451267407)

[3 Implement 8](#_Toc451267408)

[3.1 Disaster Recovery Procedures 8](#_Toc451267409)

[**3.1.1 Notification and Escalation Procedures (Communications During a Disaster) 8**](#_Toc451267410)

[**3.1.2 Damage Assessment and Disaster Declaration 8**](#_Toc451267411)

[**3.1.3 System Recovery Procedures 9**](#_Toc451267412)

[3.2 DR Solution 9](#_Toc451267413)

[**3.2.1 Backup Strategy 10**](#_Toc451267414)

[**3.2.2 DR Solution 10**](#_Toc451267415)

[3.3 Procedures for IT Operations While Operating in DR Mode 11](#_Toc451267416)

[3.4 DR Awareness and Training 11](#_Toc451267417)

[**3.4.1 Roles and Responsibilities 11**](#_Toc451267418)

[4 Maintain 12](#_Toc451267419)

[4.1 DR Testing 12](#_Toc451267420)

[**4.1.1 Test Plan Summary 12**](#_Toc451267421)

[**4.1.2 Passive Testing Handbook 12**](#_Toc451267422)

[**4.1.3 Active Testing Handbook 12**](#_Toc451267423)

[4.2 DR Documentation Management 13](#_Toc451267424)

* 1. [DR Change Management 13](#_Toc451267425)

**4.3.1** [**DRP Maintenance Log 13**](#_Toc451267426)

# 1 Introduction

This section helps position the disaster recovery plan (DRP), detailing what is included in the plan and what areas are addressed. Lists and paragraphs should be made relevant to your Business.

This Disaster Recovery Plan Summary captures all the information that describes VSN’s ability to withstand a disaster. It should also describe the processes to achieve disaster recovery. Organized into the following categories:

* **Define:** Summarize asset management, Business Impact Analysis (BIA), and risk management.
* **Implement:** Summarize the DR strategy and recovery procedures.
* **Maintain:** Summarize the DRP testing and maintenance strategy.

## Purpose

Establishes the procedures for properly recovering from a disaster affecting IT services.

An IT disaster is defined as the interruption of the process due to the IT components that help the business to work properly such as hardware and software. Disasters may arise from Hardware/Software glitch, Security breaches, Natural Disaster.

A disaster is properly recovered when:

* The affected IT services are rectified within the Recovery Time Objective (RTO)
* The affected data is retrieved than the Restore Point Objective (RPO)
* The end users affected by the outage can resume their work
* The business and IT agree that the recovery plan was successful, and the business can run their process as normal.
* The DR owner is responsible for designing the all the goals and objectives of Recovery time Objective (RTO) and Recovery Point Objective (RPO)

## Scope

This document applies to all IT infrastructure of VSN company

|  |  |  |
| --- | --- | --- |
| Hardware & Network | | |
| Network Equipment (Switches, Routers, DMZ, WAP, Phone) | Networked Storage | Firewall |
| Enterprise Servers | Anti-Malware | ISP Routers |
| Workstations | LAN Closet Coolers | UPS |
| A/V Equipment | Security Server | Check Printer |

|  |  |  |
| --- | --- | --- |
| **Applications and Data** | | |
| Team Files (HR DB, LP DB, Legal DB) | Email | File Server (V Drive, Finance) |
| Financial Reporting Software | Thin Client | Help Desk Software |
| Third-Party SaaS Solutions | Bulk Email Software | SQL Server |
| Windows Server (incl. Print) | Data Backup | Email/Messaging |
| Fax Server | AD/Domain Controllers | Wireless Platform |
| Virtualization Management | Network Storage Management | Network Management |
| FTP Server | Access Control Software |  |

# Define

Analyzes and creates the foundational documents which the rest of the DRP phases will reference. The key outputs of the define phase are asset management documents, the business impact analysis, and risk management components.

## Asset Management

VSN’s Asset Management Strategy will:

* Clearly identify the IT glitches in the software, hardware, datacenter of the company
* Document and track all the detailed information about the IT components that is being used in the company
* Document the current state of IT components. Also include what actions the [Business Name] must take to implement the Asset Management Strategy, including resource requirements, timeframes, and accountabilities.

### Hardware Assets

Inventory of all Hardware Assets can be found: [www.vsn.com/documnets/assets/hardwareassets](http://www.vsn.com/documnets/assets/hardwareassets)

### Software Assets

Inventory of all Software Assets can be found: [www.vsn.com/documnets/assets/hardwaressets](http://www.vsn.com/documnets/assets/hardwaressets)

### Asset Management Policies and Processes

Asset Management policies and processes can be found in the following links.

For detailed documentation, please refer to the following links:

* Policies –[www.vsn.com/documnets/policies](http://www.vsn.com/documnets/policies)
* Processes – [www.vsn.com/documnets/processes](http://www.vsn.com/documnets/processes)
* Action plan roadmap – [www.vsn.com/documnets/roadmap](http://www.vsn.com/documnets/roadmap)
* Revision and change history – [www.vsn.com/documnets/revison and change history](http://www.vsn.com/documnets/revison%20and%20change%20history%20)
* Audit record – [www.vsn.com/documnets/auditrecord](http://www.vsn.com/documnets/auditrecord)

## Business Impact Analysis (BIA)

IT applications and systems at VSN have been analyzed using a Business Impact Analysis. The BIA provides guidance regarding the criticality of each application and their respective RTOs and RPOs.

For the comprehensive Business Impact Analysis, please reference: [www.vsn.com/documnets/impactanalysis](http://www.vsn.com/documnets/impactanalysis)

### Impact of Downtime Criteria

The criteria to evaluate the impact of downtime in the BIA are as follows:

* Evaluating the the internal and external threats
* Evaluating the issue in the datacenter
* Build the plans such that recovery from disaster can be easy

### Failover RTO and RPO Summary for Tier 1, 2, and 3 Applications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application Tier | Failover Desired RTO | Failover Desired RPO | Failover Achievable RTO | Failover Achievable RPO |
| Tier 1 | 4:00 | 02:00 | 24:00 | 12:00 |
| Tier 2 | 24:00 | 12:00 | 48:00 | 12:00 |
| Tier 3 | 72:00 | 24:00 | 72:00 | 12:00 |

### Failback RTO and RPO Summary for Tier 1, 2, and 3 Applications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application Tier | Failover Desired RTO | Failover Desired RPO | Failover Achievable RTO | Failover Achievable RPO |
| Tier 1 | 08:00 | 02:00 | 24:00 | 12:00 |
| Tier 2 | 24:00 | 12:00 | 48:00 | 12:00 |
| Tier 3 | 72:00 | 24:00 | 72:00 | 12:00 |

### List of Tier 1, 2, and 3 Applications

Below is a summary list of Tier 1, 2, and 3 applications.

#### Tier 1 (Mission-Critical)

* Tier-1 is considered as the Mission-critical application and RPO and RTO of less than 15 minutes is required.

#### Tier 2

* Tier-2 is considered as the Business-critical application and RTO of 2 hours and RPO of 4 hours is required.

#### Tier 3

* Tier-3 is considered as the Non-critical application and RPO of 24 hours and RTO of 2 hours is required.

## Risk Assessment and Risk Management

VSN has conducted a risk assessment which focused on identifying the risk considerations.

This includes:

* **Areas of low risk tolerance**
* **Areas of existing or potential risk**
* **Location-based risks**

In addition to the risk assessment, each identified risk has been mapped to a mitigation plan which is included in the Risk Mitigation Roadmap. For the complete risk assessment and risk management strategy, please reference:

[www.vsn.com/documnets/riskmanagemment](http://www.vsn.com/documnets/riskmanagemment)

## DR Duration Considerations

VSN has made provisions for when a disaster causes extended periods of downtime. To accommodate DR requirements, VSN has decided with Vendor 123 to switch to their DR environment during extended downtime.

For more information on accommodating extended downtimes, please reference:

[www.vsn.com/documnets/downtime-extension](http://www.vsn.com/documnets/downtime-extension)

# Implement

The implementation phase of the DRP focuses on developing the pre-planned steps to be taken to get back to normal phase from disaster.

## Disaster Recovery Procedures

If a disaster occurs, and there is a health and safety risk (e.g. the disaster is a fire), the priority is to ensure that all employees are safe. After this, recovery consists of the following steps:

* Notification and escalation procedures
* Damage disaster and disaster declaration
* System recovery procedure

### Notification and Escalation Procedures (Communications During a Disaster)

In the event of a disaster, VSN will need to communicate with manager of the core disaster recovery team to inform them of disaster that has occurred. The Core Disaster Recovery Team will be responsible for contacting all of VSN’s stakeholders.

The disaster communication plan highlights the following key areas:

* Collecting the customer feedback and analyzing it.
* Escalating the issue to resolve the it quickly
* A system that controls the disaster needs to be developed.
* Ask the spokesperson to let the stakeholders know about the occurrence of the disaster.

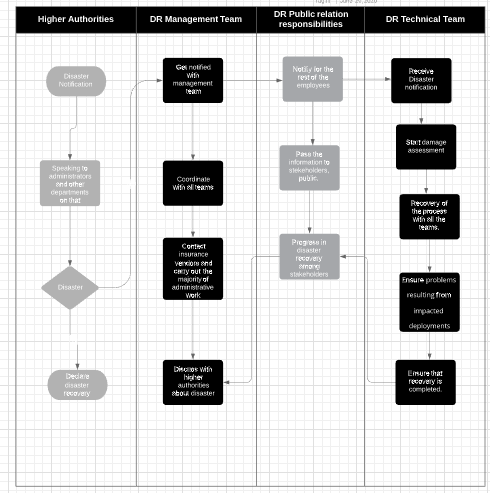
### Damage Assessment and Disaster Declaration

VSN has defined and documented severity definitions and escalation rules which will determine when DR takes over from service management. Summary of the process is as follows:

* For an obvious disaster (severity 0 in this example), DR procedures take over immediately. For critical or urgent issues (severity 1 or 2), attempt to resolve within time allowed before escalating to DR procedures.
* After the incident is resolved, or DR completed, file a problem ticket to resolve the root cause (e.g. replace faulty primary hardware, address process issues, etc.) and document lessons learned.
* After the problem ticket is resolved, return to normal (i.e. initiate repatriation planning).

For additional information on Damage Assessment, please reference:

[www.vsn.com/damageassessment](http://www.vsn.com/damageassessment)



### System Recovery Procedures

System recovery procedures are outlined for all applications and infrastructure dependencies. These procedures are stored in the following location and are accessible during a disaster: [www.vsn.com/recovery-procedure](http://www.vsn.com/recovery-procedure)

## DR Solution

The current DR Solution for VSN relies on an in-house DR site. The decision for the DR solution was made with the following considerations:

* RTO and RPO Requirements
* Budget
* Number of IT employees
* Components that are currently in working conditions

### Backup Strategy

The current backup schedule for VSN is as follows:

|  |  |  |
| --- | --- | --- |
| Type of Data | Backup Frequency | Length of Retention |
| Operating Systems | 48 hours | 30 days |
| Tier 1 application data | Incremental backup every 1 hour and full back up every 23 hours | 30 days |
| Tier 2 and 3 application data | 24 hours | 15 days |
| End-user data | 23 hours | 2 days |

Data is backed up to date and stored in the Organization data server. The location of the backup is local host

Please reference the detailed Backup Strategy document for additional information.

See: [www.vsn.com/databackup](http://www.vsn.com/databackup)

### DR Solution

In the event of a disaster, VSN is prepared to failover to the DR site located at 3A-33 queen street south, Kitchener. 3A-33 queen street south, Kitchener will act as the Emergency Operations Center as well as the primary meeting place for VSN staff when communications are not available.

The current DR solution for VSN is designed as such:

DR Solution Documentation for VSN includes the following:

* List of mandatory resources available at the DR site.
* How to access the DR site.
* Directions to DR site.
* Transportation and access to the DR site.
* Executing day-to-day IT operations at the DR site.

For the comprehensive DR Solution Document, please reference:

[www.vsn.com/DR-Solution](http://www.vsn.com/DR-Solution)

## Procedures for IT Operations While Operating in DR Mode

During a disaster, VSN has made provisions for IT operations at a reduced scope. The services below will be supported by IT staff during a disaster:

* Help in finding out the issue
* Plan the disaster recovery model
* Present all the available issues

For further clarification on the types of services that will be supported during DR to repatriation, please reference: www.vsn.company/support-it

## DR Awareness and Training

The Core DR Team is responsible for supervising and ensuring that the entire DR team is aware and trained to execute the relevant DR procedures. DR awareness and training will include:

* Prepare the material for DR awareness and training
* A website that provides the practical training videos on DR awareness.
* Periodically conducting scrum meetings
* An assessment to be conducted to improvise the knowledge

### Roles and Responsibilities

In the event of a disaster, the Core DR team will refer to the DRP Workbook for information pertaining to roles and responsibilities. The key elements of the Workbook include:

* DR Roles and Responsibilities
* Contact Information

During a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of VSN. The groups that are responsible for responding and resolving a disaster are as follows:

* Maintenance department
* Work-force department
* Network department
* Security management department
* IT department
* Process Department

Please reference the DRP Workbook for detailed information:

[www.vsn.com/drp-workbook](http://www.vsn.com/drp-workbook)

# Maintain

The maintenance phase of the DRP provides the Business with the opportunity to review, maintain, and optimize the DRP. The key outputs of the Maintenance phase are problem identification, problem analysis, design ,implementation, system test and acceptance test.

## DR Testing

DR Testing at VSN follows a cyclical testing schedule and includes the following core components.

* Test Planning
* Executing the plan
* Outcome analysis

For the comprehensive DR Test Plan, please reference: www.vsn.com/dr-testplan

### Test Plan Summary

The DR Test Plan Summary is a high-level plan that summarizes the more detailed planning documents. Core components of the Test Plan Summary include:

* Hardware testing
* Software testing
* Security testing

For the comprehensive Test Plan Summary, reference: [www.vsn.com/test-plan](http://www.vsn.com/test-plan)

### Passive Testing Handbook

The Passive Testing Handbook outlines how VSN prepares and plans tabletop planning exercises. Components of the Passive Testing Handbook include:

* How to deal the with disaster
* Steps to be taken to resolve the disaster
* Plans that include to control the disaster

For the complete Passive Testing Handbook, reference: [www.vsn.com/passive-testing](http://www.vsn.com/passive-testing)

### Active Testing Handbook

The Active Testing Handbook outlines how [Business Name] prepares, documents, schedules, and collects results for each active DR Test. Components of the Active Testing Handbook include:

* Identify the scope
* All the resources are documented
* All the risks and mitigation need to be identified

For the complete Active Testing Handbook, reference: www.vsn.company/active-testing

## DR Documentation Management

DR documentation will ensure that all the necessary information that is needed during the time of disaster is written properly. Everyone on the DR team will be responsible for preparing the document.

The DR documentation resides in these locations:

* IT file share is typically mapped as Drive “I:” and is located at [www.vsn.com/dr-document](http://www.vsn.com/dr-document)
* Main DRP folder: [www.vsn.com/drp-folder](http://www.vsn.com/drp-folder)
* System Recovery Documentation: [www.vsn.com/recovery-documenattion](http://www.vsn.com/recovery-documenattion)
* Direct link to OneNote: [www.vsn.com/document/one-time](http://www.vsn.com/document/one-time)

## DR Change Management

DR is incorporated into the change management process to ensure that changes in the business and technology environment are consistently reflected in DR procedures. To ensure relevance, usability, and maintainability, the DRP will be updated using the following guidelines:

* Plan for the change
* Identify the changes that can be improved
* Identify the problem if any before changing the DR management

# References

*Baseline Data sheet*. (n.d.). Retrieved from https://baseline-data.com/blog/high-availability/5-steps-analyze-downtime-impact-downtime-impact-cheat-sheet/

*Common practice html*. (n.d.). Retrieved from https://www.veeam.com/blog/rto-rpo-definitions-values-common-practice.html

*Communication plan*. (n.d.). Retrieved from https://blog.hubspot.com/service/crisis-communication-plan

*Recovery plan*. (n.d.). Retrieved from https://nuummite.consulting/getting-started-with-your-it-disaster-recovery-plan-drp-implementation-part-1/

*Testing handbook*. (n.d.). Retrieved from https://www.infotech.com/research/dr-test-plan-active-testing-handbook