



## *Disaster Recovery Plan*

*Version 1.0, Created by*

---

## Overview

Use this section to give a brief executive overview of the DR plan and what you are trying to achieve with it. The key to success is to keep it as simple as possible.

Break your plan into sections to allow the reader to understand the logical flow of the plan. The sections below are suggestions and may be included or excluded depending on the company requirements.

The DR plan is not designed to be a static document. In order to be successful it needs regular reviews, testing and feedback in order to assist you when you need it.

1. **Contact details** - This section identifies personnel that are key to the successful planning, testing and execution of the disaster recover plan. Contacts will be referenced throughout the plan at appropriate parts of the execution or testing.
2. **Key IT Processes** - This section lists the key IT processes relevant to the normal operation of the business. The items are in order of importance; each item has a brief description of the process and lists any processes that it depends on for normal operation.
3. **Important information** – This section details other important information that needs is relevant to the disaster recovery plan such as insurance details, health and safety issues etc.
4. **Execution plan** - This section is best written as a flow diagram. This will give the reader a visual aid to follow the appropriate course of action in the event of a disaster or a test. It will aid them in identifying the particular processes that need attention.
5. **Process Recovery** - This section details the process that needs to be followed in order to get the identified process up and running again.
6. **Testing the DR plan** - This section details the results of any DR testing that has been done against the plan. The plan version number will be incremented by 0.01 each time a test is added.

IT IS ESSENTIAL THAT YOU SCHEDULE REGULAR TESTS OF THE DR PLAN

7. **Lessons Learned** - This section lists any results that are ascertained from the tests that are of relevance to future tests or executions of the plan. Depending on the severity of the lesson, it may be included in section seven, **Plan Amendments**.
8. **Plan Amendments** – This section details any amendments to the plan that might occur from changes in the IT infrastructure or as a result of lessons learned from testing or actual execution of the plan.

## Contact Details

The following individuals have a vested interest in one or more of the key IT processes for Finance Cornwall and maybe required for the testing or execution of the plan.

## Key IT Processes

The following should be a descriptive list of the organisations key it functions in order of importance to the business together with a brief description of the business process and any dependencies associated with it.

The process owner is also an important element and should refer to a key contact listed in the contacts section of the plan.

Key IT Areas <i>In order of importance</i>	Brief description of process	Process Owner	Process Dependencies
1			
2			
3			
4			
5			
6			
7			
8			
8			
9			
9			

## Important Information

This section should detail any information key to successful implementation and testing of the plan. The bullet points should give you some indication of the points to consider

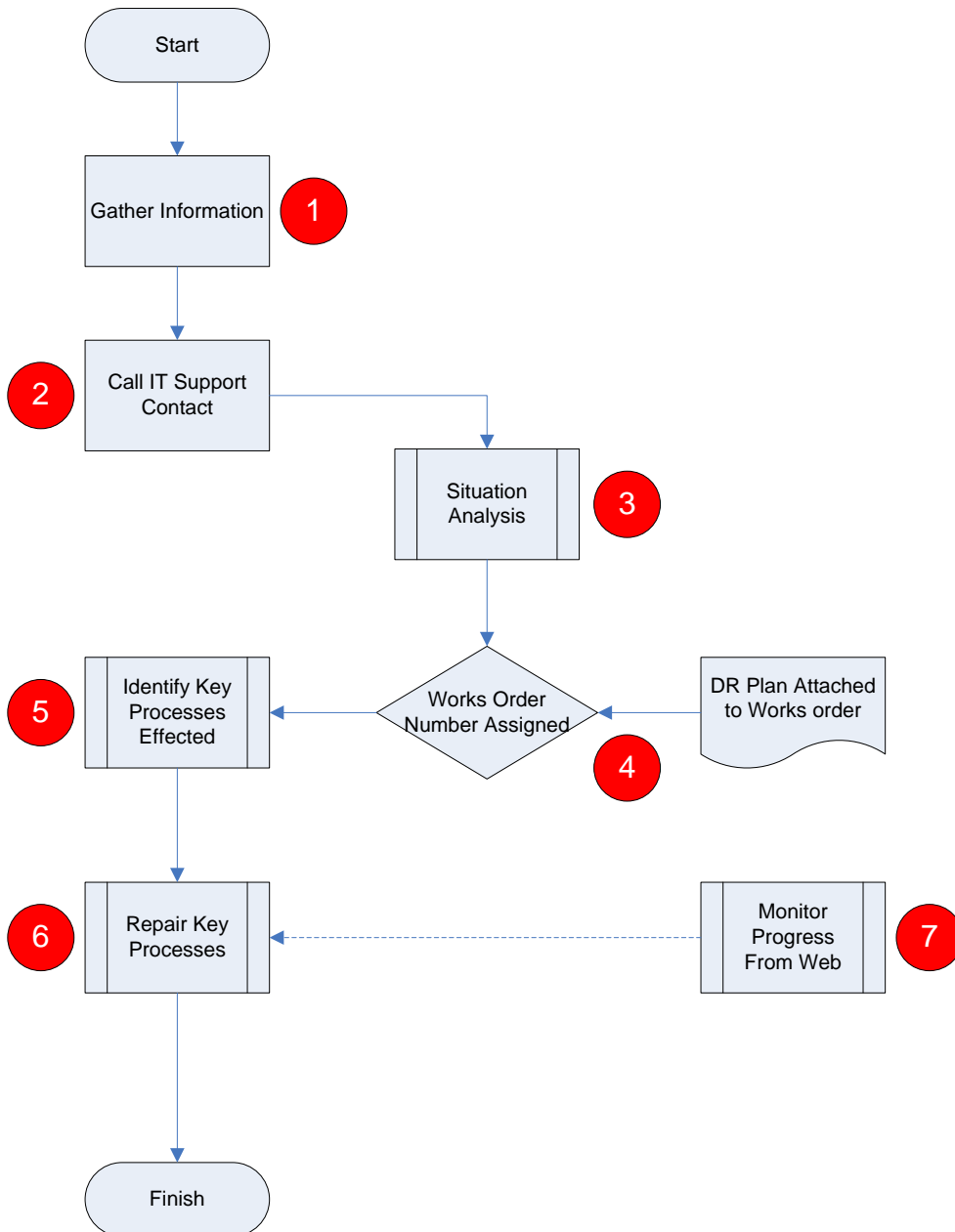
- Off site server
- Off site router
- Backup routines and storage
- Server configurations
- Internet connectivity
- Network schematics
- Insurance details

# Execution Plan

The execution plan should clearly indicate the flow of the plan to analyse the extent of the disaster and the steps required to bring the business back to a normal or contingent level of operation.

Each of the steps should be numbered and clear works instructions for the process listed after the flow diagram.

The suggested flow diagram assumes a call management and tracking system is used to register and record any activity surrounding the DR plan. This is not essential but provides a great deal of traceability which is useful when reviewing the DR plan.



1. Gather Information

During this stage the on-site contact will gather as much information about the disaster as possible, bearing in mind the key processes defined in the DR plan.

2. Call IT support contact

The IT support contact listed in the DR plan will be called and informed of the disaster. All relevant information will be passed to the IT support contact.

3. Situation analysis

The IT support contact and the on-site contact will agree the extent of the situation at present and use the information to construct a works order. There may be a requirement for the IT contact to attend the site to complete this.

4. Works order and DR plan

The IT contact will give the on-site contact a works order so that the progress of the disaster can be tracked. The works order will also contain an attached copy of the DR plan in order that any technician may be able to inform on-site contacts of the progress.

5. Identification

Key processes affected will be identified and listed in the resolution of the works order. They will be listed in the order that they need to be addressed in accordance with the DR plan.

6. Repair

The IT support contact will set about reparations of the key processes as defined in the DR plan

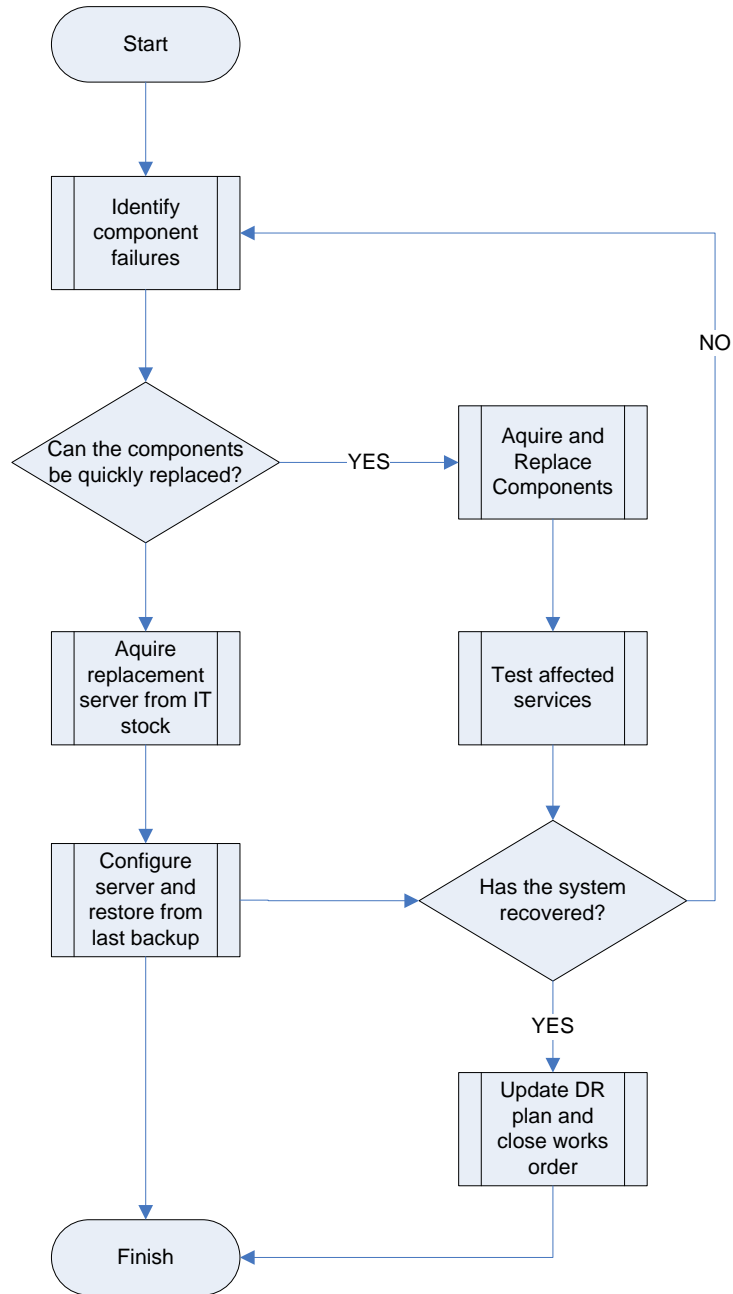
7. Monitor

Once the above is completed, the on-site contact and interested stakeholders will be able to monitor progress of the recovery from the web if possible.

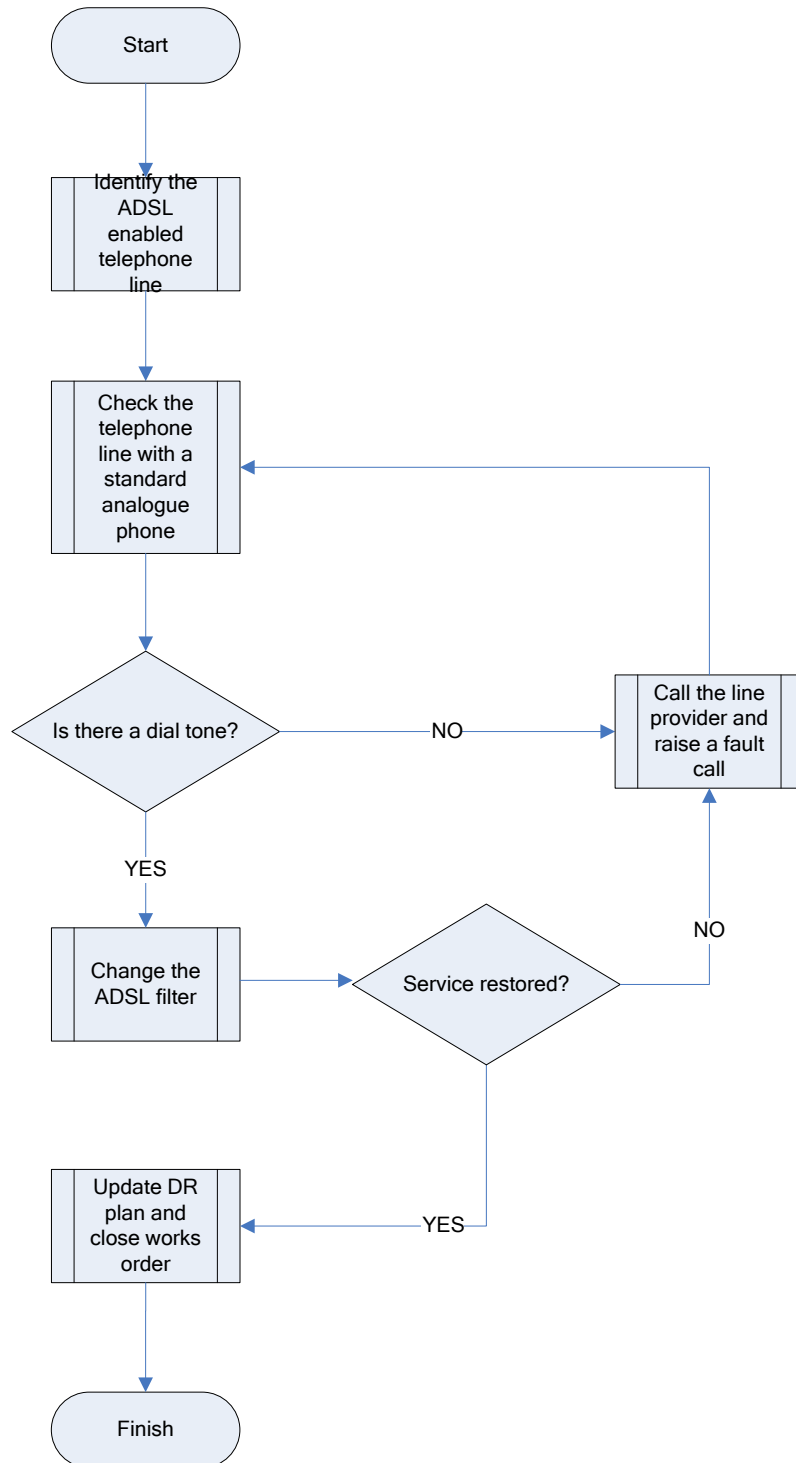
# Key IT Processes - Recovery

The recovery process is very specific to the individual business and depends on a number of variables such as number of users, number of sites, hardware and network configuration. The details below give you an example of the basic idea. This is where you need to involve a specialist Computer Services company to assist. Hopefully, this will be [Piran Technologies!](#)

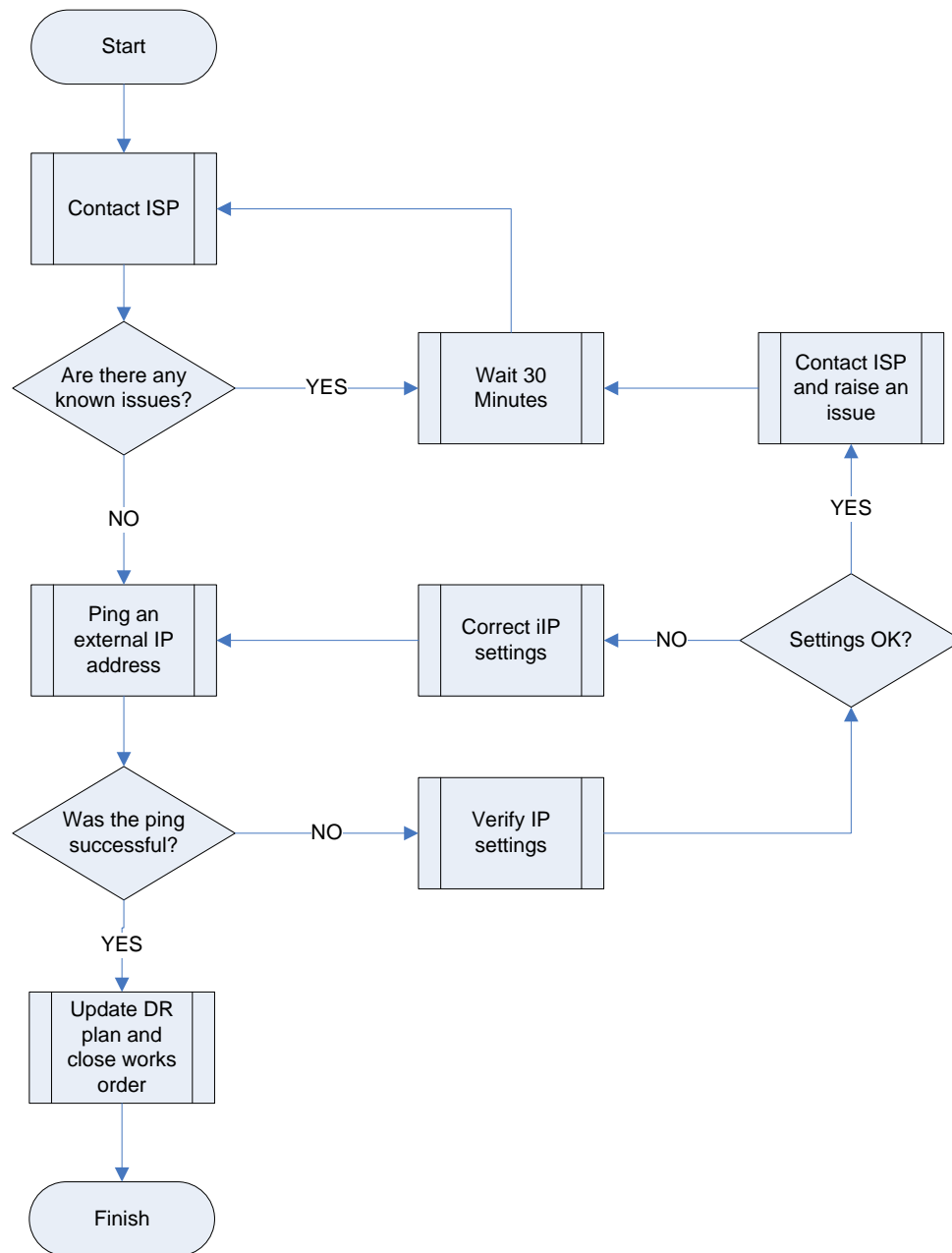
## 1. Network server



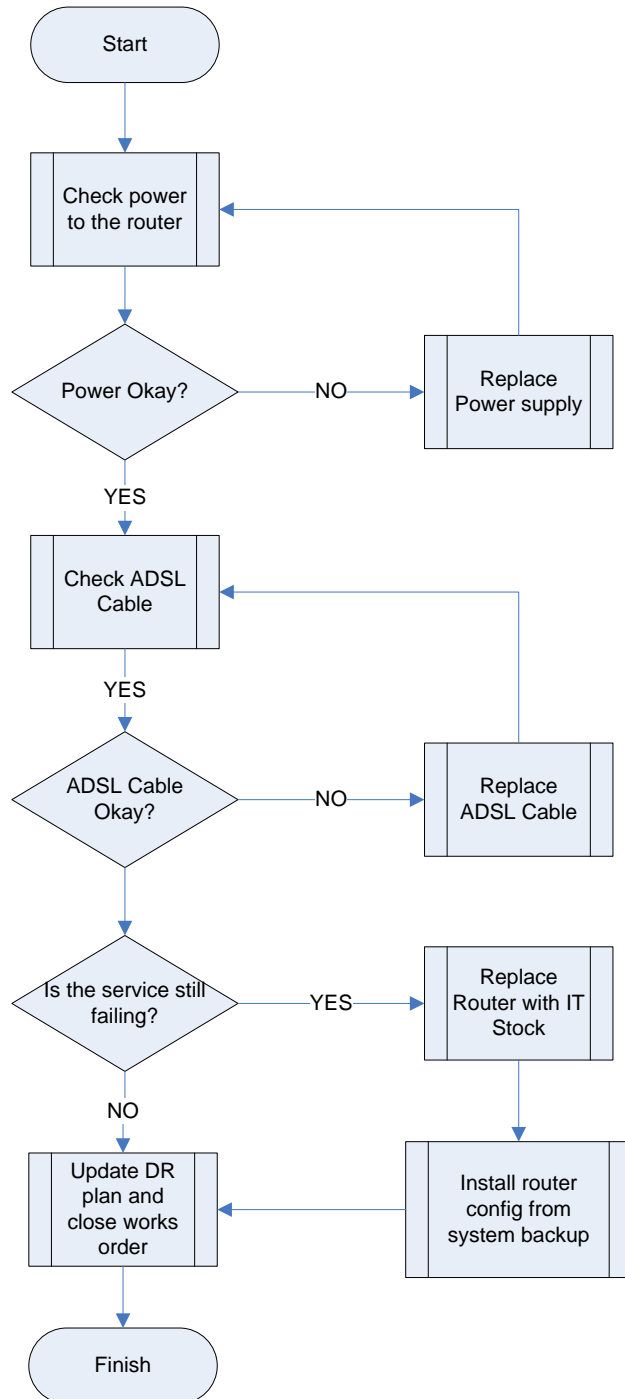
## 2. ADSL enabled telephone line



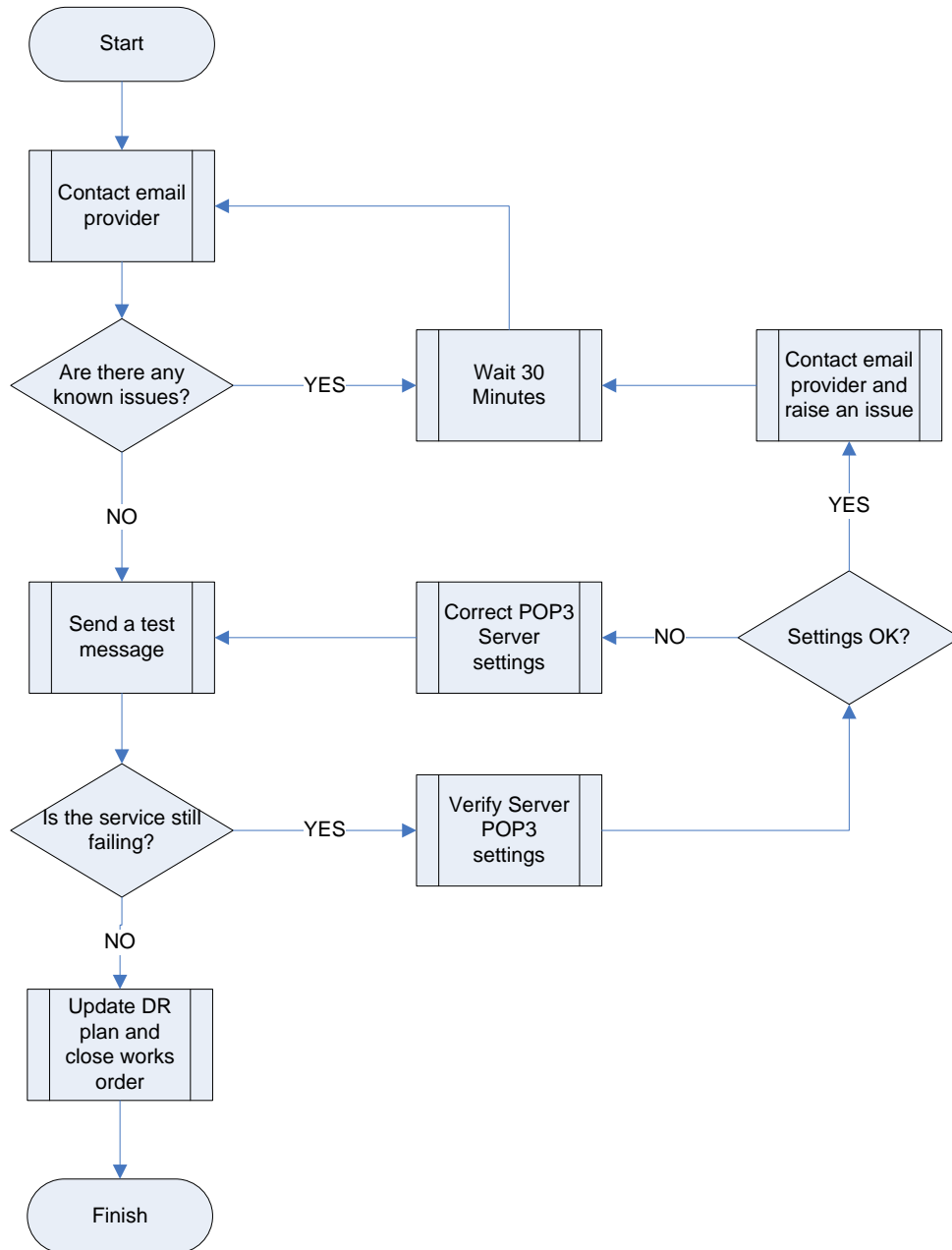
### 3. Internet Access



## 4. Internet Router



## 5. Email – Provider



## 6. Data Backup

A harder one to do a sample flow for as there are many different ways to backup and restore data

### Testing the DR plan

A full test recovery of the DR plan should be scheduled in accordance with the requirements of the business. The optimum time to do this will be during replacement of hardware.

Scheduled tests should address the different parts of the DR plan to ensure each area is covered and tested during the test cycle.

Use a table like the one below to schedule and record tests, their outcome and any amendments made to the plan.

<b><i>Entry number</i></b>	<b><i>Description of test</i></b>	<b><i>Date of test</i></b>	<b><i>Lessons learned reference</i></b>	<b><i>Plan amendments reference</i></b>

## Lessons Learned

This section records details of any events during the testing or application of the DR plan that the users feel would benefit future execution.

If there is a need to amend the plan there will be a reference to the amendment entry in the following section

<b><i>Entry number</i></b>	<b><i>Description of test</i></b>	<b><i>Date of entry</i></b>	<b><i>Plan amendments reference</i></b>

## Plan Amendments

This section details any amendments that have been made to the DR plan over the course of time. These may be amendments from changes in hardware or software systems, service or support providers or recommended changes highlighted through testing or execution of the plan.

Each time an amendment is made, the version of the DR plan will be incremented by the plan owner.

<b><i>Entry number</i></b>	<b><i>Description of amendment</i></b>	<b><i>Date of entry</i></b>	<b><i>Last version number</i></b>