Skillmine Technology Consulting

Business Continuity Plan / Disaster Recovery

Approach Paper

Contents

1 Purpose

Information Technology (IT) and systems are vital to supporting seamless business processes. It is critical that the services provided by these systems are able to operate effectively without excessive interruption. Disaster Recovery Planning (DRP) supports this requirement by establishing thorough plans, procedures and technical measures that can enable a system to be recovered appropriately following a disaster.

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) and from a variety of sources such as natural disasters to acts of terrorism. While much vulnerability may be minimized or eliminated through technical, management or operational solutions as part of risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the direct control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective disaster recovery planning, testing, and execution are essential to mitigate the risk of system and service unavailability.

IT disaster recovery plans aim to provide a clear recovery path in the event of losing a critical technology component such as an application or piece of technology infrastructure. They should be detailed to a level which assists staff in recovery of systems. These plans should be action and outcome oriented as they establish:

- management and staff responsibilities;
- key action steps to be followed and the strategic options and information required;
- activation, management and escalation processes;
- internal and external communication protocols;
- dependencies for all in-scope components;
- critical resources and contact numbers for key staff and external service providers;
- recovery instructions for all in-scope components which may include failover capabilities, build procedures, software loading and configuration procedures, connectivity, data restoration; and
- testing and maintenance requirements.

The IT Disaster Recovery Program should be developed in accordance to the overall Business Continuity Management Policy of the Organization.

1.1. Objectives

Top executive commitment is required to ensure effective recovery processes operate across all parts of the IT that provide a critical system, either internally or externally. This commitment involves the design & implementation of end-to-end IT Disaster Recovery Plan (DRP).

In order to achieve alignment and consistency of the recovery plans, as well as to understand the interdependencies, this document offers an IT disaster recovery approach to start discussions and panning around the IT DR.

Additionally, the framework also provides guidance on achieving the following:

- Identifying and classifying applications for each Business Unit
- Continuing the operation of critical applications in the event of a disruptive incident
- Understanding the criteria and triggers for invoking the IT DRP

- Ensuring that all staff understand their roles and responsibilities when a disruption occurs;
- Ensuring that there is a clear understanding throughout the Organization of what accountabilities and responsibilities are in place during an interruption to 'business as usual';
- Understanding the necessary documentation and procedures needed for IT disaster recovery planning and the Customer's expectation around these;
- Educating and training staff on IT disaster recovery and exercising the IT disaster recovery plans.

1.2. Scope

IT disaster recovery planning should be one part of the larger process associated with managing a disaster or incident. The scope of the IT Disaster Recovery Program described in this framework is limited to the Information Technology Services (ITS) division.

This framework does not cover emergency response procedures or business continuity management procedures. These need to be developed by individual Business Units for their own business continuity and emergency response plans as per the BCM policy.

1.3. Triggers and Invocation Procedures

If a disruptive IT incident intensifies it can become a disaster, escalating the IT disaster recovery effort to a higher level within the Organization.

IT Incident Management processes should be used as a first response to an IT incident. If the incident cannot be resolved within a suitable timeframe, or the magnitude of the incident is much greater than expected, then IT Disaster Recovery should be activated.

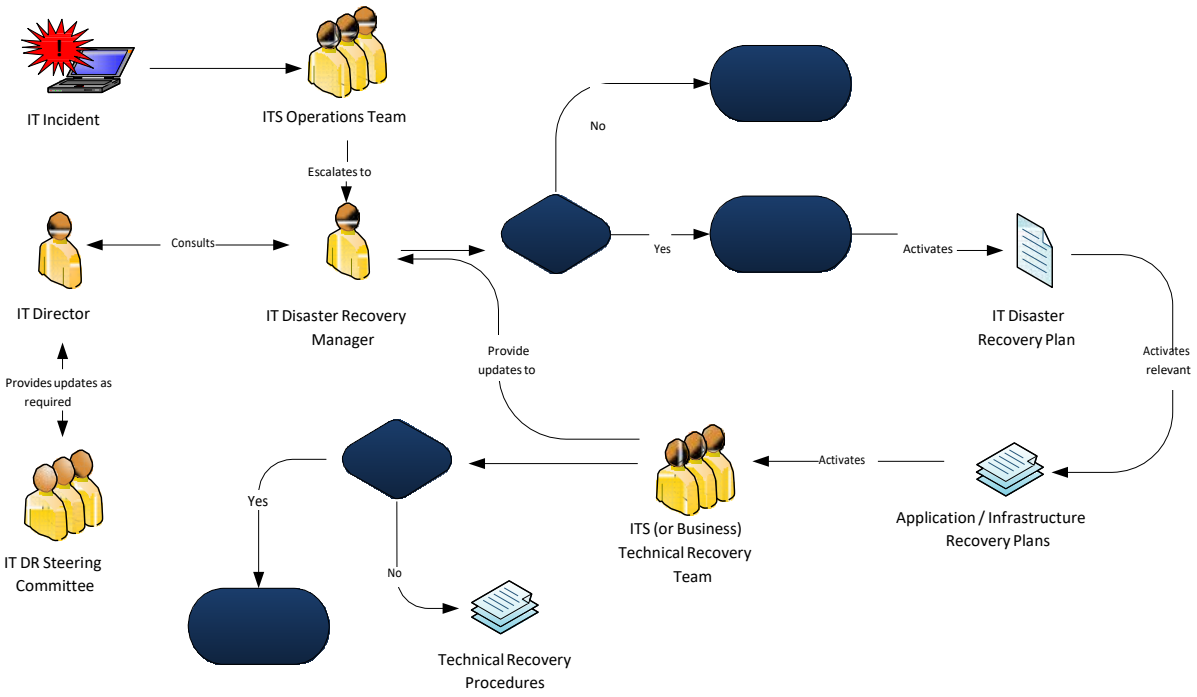

Figure 1 - High Level IT DR Escalation

1.4. Consider Assumptions

The Organization should consider the assumptions that are being made during the IT disaster recovery planning process. These assumptions should be clearly stated in the IT Disaster Recovery Plan so as to recognize the limitations of the plan. Assumptions should be communicated and agreed by all stake holders.

For example, an assumption might be 'this plan assumes that no more than 2 critical systems within the region are affected by the incident'.

Individuals should also consider the following possibilities when assessing the impact of an incident:

- the maximum Recovery Time Objective (RTO) of a critical system may be exceeded.
- the incident has the potential to involve multiple departments across the Organization.
- remote sites may also be involved.
- there may be a prolonged impact on downstream dependencies.
- there may be increased public attention (including media) of the areas affected.

2 The IT Disaster Recovery Lifecycle

The IT Disaster Recovery Lifecycle is shown below highlighting the key steps that should be taken in order to develop an effective IT Disaster Recovery Plan:

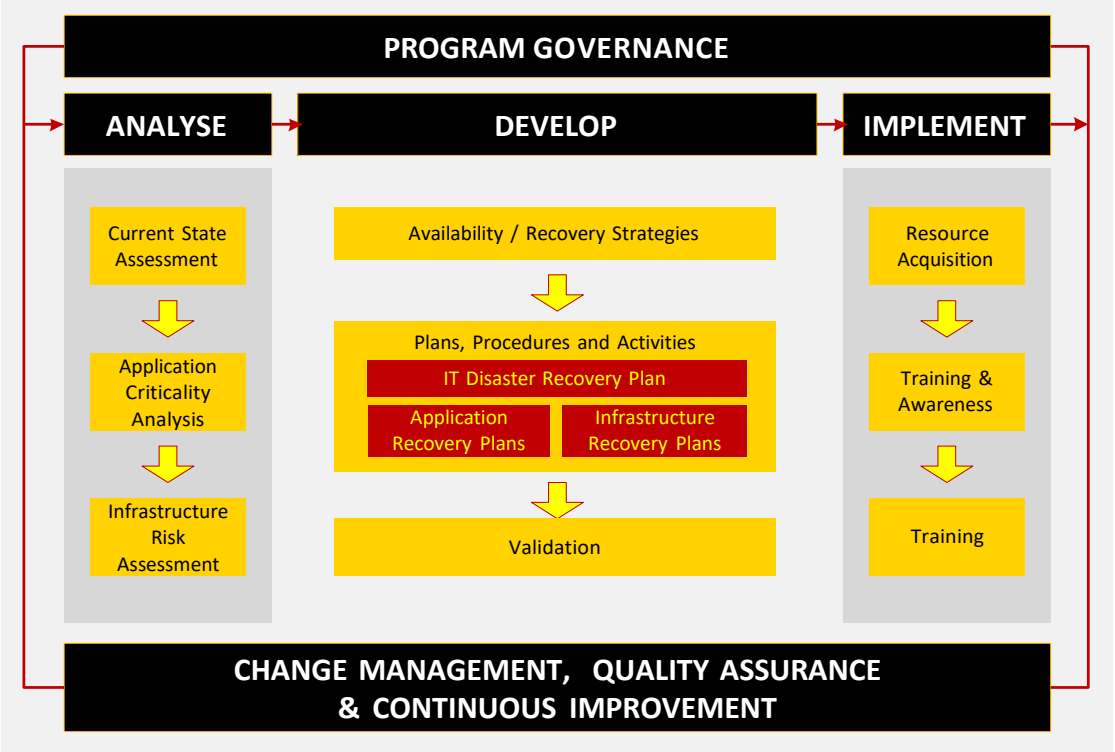

Figure 2 - IT Disaster Recovery Lifecycle Diagram

The remainder of this section will aim to explain each of the phases described in the lifecycle diagram above.

2.1. Program Governance

Provides structure and consistency to the management of the disaster recovery plan and influences how the Organization will:

- set and achieve recovery objectives;
- assess and manage risks;
- control critical documents and align them with the broader Governance framework;
- allocate roles and responsibilities and align the Organization recovery initiatives;
- achieve optimal performance.

This framework will serve as the driver for governance as it largely would combine many elements of the IT disaster recovery policy. The IT disaster recovery governance should articulate and communicate the Organization's strategic approach toward such planning.

Good governance should also be embedded within system recovery thinking and approaches within each level of the Organization. Disaster recovery governance should be aligned with their wider corporate governance initiatives.

Formalizing and communicating the roles and responsibilities of key IT disaster recovery stakeholders is a critical component of effective IT disaster recovery governance. Success of this framework therefore hinges on the wide recognition and acceptance of allocated IT disaster recovery roles and responsibilities. Section 3 defines the roles and responsibilities which should be allocated within the Organization and recommends the appropriate level of training, engagement and exercising that those positions should undertake.

2.2. Analyse

2.2.1 Objectives

The objective of the analysis phase is to:

- Analyse and understand the current state of disaster recovery plans in place across the Organization;
- identify and quantify the exposure levels of the Organization to key and prioritized risks;
- identify critical systems that are used to support the Organization's functions;
- identify manual workarounds or alternate working arrangements that are already in place in the event of a loss of a key system.

2.2.2 Current State Assessment

A current state assessment should be performed across the IT application environment to determine the level of IT DR maturity. The current state assessment should occur in conjunction with the Application Criticality Assessment, described in the next section. Where gaps are identified, these should be highlighted for remediation.

2.2.3 Application Criticality Analysis

In order to ensure IT disaster recovery requirements are met, the business needs to identify and classify the key systems that support the business operations by completing a Business Impact analysis (BIA) annually or where significant change has occurred. This will form the basis of developing and maintaining a disaster recovery strategy that will encompass the critical applications and services across the Organization.

System Identification

A discovery exercise must be conducted with the different Business Units in order to establish a prioritized list of systems and services that are being used. Meetings and workshops should be conducted with key representatives from each faculty or division, who have a good working knowledge of the day to day operations of their business area. A toolkit has been provided to help capture the information required, which includes the following information:

- Application / service name;
- Business Impact of an outage to the application over a period of time (RTO);
- Threshold of acceptable data loss (RPO);
- Known and approved manual workarounds;
- Internal and external application support arrangements.

While only the application name is required for identification purposes, the remaining information helps with classification, which is covered in the next section.

If this exercise has already been performed, then the existing list of key systems should be used as a starting point in discussions with the Business Units, with a view to validate the list of key systems and capturing any new systems that have been implemented.

System Classification (Application Criticality Analysis)

Once the list of key systems has been established, these systems must be classified according to their criticality. As part of the system identification exercise, the Business Units should be stepped through a series of questions, including:

- Determining the impact-over-time caused by an outage. This will enable the capture of the magnitude of the impact to the Organization and the escalating impact caused by a prolonged outage of the application. This will provide the information necessary to determine the Recovery Time Objective (RTO) for each application.
- Determining the data loss acceptable as a result of an outage. This information should be used to determine the Recovery Point Objective (RPO) for each application.

The Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) form the basis of the 'business recovery requirements' for the application in terms of its recoverability and availability. Applications outages that have the potential to cause a significant impact to the Organization as a result of a system outage need to be identified and appropriately planned for. Using the business requirements, the applications should be classified using the following model:

Classification	Definition	* Conditions Met
Tier 1	Critical applications • services must be restored as a high priority	Causes at least a 'serious' impact to the Organization after an outage that lasts for a period of **4 hours**.
Tier 2	Important applications • services must be restored as soon as Tier 1 applications have been restored	Causes at least a 'serious' impact to the Organization after an outage that lasts for a period of **1 - 2 days**.
Tier 3	Convenient applications • services can be stood down temporarily • services must be restored as soon as Tier 2 applications have been restored	Causes at least a 'serious' impact to the Organization after an outage that lasts for a period of **3 - 7 days**.

Tier 4	Non-essential applications • services can be stood down for extended periods without significant impact • lowest priority in restoration order	All other applications, that either: • only cause a 'serious' impact after an outage lasting greater than 3 – 7 days • never cause a 'serious' impact

Table 1 - Application Criticality Classification

2.2.4 Infrastructure Risk Assessment

Once the key systems have been classified according to their criticality, it is important to identify what the key supporting infrastructure services they depend on. The potential hazards and threats that can cause an application outage due to a disruption in these infrastructure services should also be identified. There are a number of threats that can cause an outage, ranging from human error, sabotage or natural disasters. In order to determine what risks can potentially cause an outage to the supporting IT infrastructure, the following steps must be performed:

1. Develop an application topology map;
2. Perform a Single-Point-of-Failure analysis.

Application Topology Maps

In order to develop effective system continuity and recovery strategies, each system should be assessed to determine what critical IT infrastructure is used to support its operation.

An application topology map helps to provide an end-to-end view of the critical infrastructure that is required by a system to operate. The following information should be determined in order to build a suitable application topology map:

- Determine the hardware that is used to support the system, including:
  - Physical and / or virtual servers, including application server(s), database server(s), web server(s), etc. that are used to run the application;
  - Network links, including switches, cable / fiber capacity and pathways and any redundancies;
- Determine if there are any critical upstream dependencies (data feeds from other systems);
- Determine the location of the data centre(s) or server room(s) that house the basic hardware described above;
- Determine the support arrangements (including any third-party support) available for the hardware. Where third parties are responsible for the support of any hardware, obtain any Service Level Agreements (SLA) that exist.

Single-Point-of-Failure (SPoF) Analysis

Once the application topology has been constructed, it can be used to establish any high level weaknesses in the application design (not including any technical functionality weaknesses such as logical coding errors or business functional requirements).

Of particular importance from the context of availability is the existence of redundant hardware and redundant network pathways to provide continued system uptime in the event of an outage affecting one component of the hardware.

2.3. Develop

2.3.1 Objectives

The objectives of the Development phase of the IT Disaster Recovery Framework are to:

- select acceptable continuity and recovery strategies to address the key risks identified;
- minimize the impact and duration of disruptions to services that critical systems and their key dependencies deliver;
- document recovery plans for key systems;
- provide the suitable mechanism to re-establish normal BAU operations;
- ensure that all personnel are aware of their roles and responsibilities both during and after an incident.

2.3.2 Availability / Recovery Strategies

The availability and recovery strategies should be developed based on the business requirements established in the Analysis phase. Specifically, the RTO and the RPO should be assessed in the context of the existing or proposed strategy and determine whether it is achievable.

The RTO is the timeframe that the business has agreed with ITS, establishes the recovery time required following an outage. If any of the individual components of the application (servers, databases, and network components) cannot be recovered within this period, then new strategies should be developed.

The backup strategy employed for each application should be determined by the RPO established by the business and ITS. The amount of data loss that can be afforded should drive the type and frequency of data backups required.

It is important to note that when formulating these strategies, consideration should be given to the suitability (financially and practically) of the proposed strategies. It is therefore important for each strategy to be endorsed and signed off by an executive within the Organization. Presenting the executive with a number of strategies from which they select the chosen option, is another method which can be employed by the Organization. This method is recommended when strategies result in high exposure (financial, legal, reputation, etc.) to the Organization or to the industry as a whole.

A number of recovery strategies can be selected for each application, including the following examples to recover from virtual infrastructure, recover from tape backups, rebuild the infrastructure and reinstall the application, etc. In some cases it may be most effective to do nothing, and wait for the disaster event to pass. These decisions will need to be made by the IT DR Team at the time.

2.3.3 IT Disaster Recovery Plan

The IT Disaster Recovery Plan (IT DRP) will provide a holistic view of the IT environment and how it supports the critical applications used by the Organization. It will provide strategies and guidance for the recovery of the underlying infrastructure, including the data centres, servers, data storage and network links and infrastructure applications (e.g. Active Directory, LDAP), based on the business' recovery requirements.

The following information should be provided within the IT DRP:

- definition of a disaster and triggers for consideration of when the IT DRP should be invoked;
- activation and escalation procedures;
- roles and responsibilities during the recovery;
- communication and escalation processes when a plan is invoked;
- internal and external communication strategies (usually sourced from a communications plan);
- short term workarounds and alternate working procedures;
- key contact details for, emergency services, all relevant staff involved in the recovery of IT and external parties involved in the recovery of IT;
- Critical dependencies;
- Recovery Assumptions;

The IT DRP will serve as a 'master plan run book' encompassing the key services and components of the IT environment at the Organization. However, should an outage only affect a single application, there will be a suite of application specific recovery plans accompanying the IT DRP for all applications deemed critical to the Organization. These are covered in the next section.

2.3.4 Application Recovery Plans

While the IT Disaster Recovery Plan coordinates the overall recovery process, a major component of recovering the Organization's critical operational ability lies with the successful recovery of individual applications. Each application that has been identified as critical must have an Application Recovery Plan (ARP) that will include the necessary steps needed to successfully recover the application. The ARP should also include:

- recovery of specific hardware / infrastructure (some may be referred onto a dedicated Infrastructure Recovery Plan);
- recovery of software files;
- recovery of application specific data (from databases or other storage means), using the available backup strategies;
- roles and responsibilities for recovery;
- short term workarounds and alternate working procedures;

- key contact details for all relevant staff involved in the recovery of IT and external parties involved in the recovery of IT.

2.3.5 Infrastructure Recovery Plans

The critical infrastructure services identified will have a dedicated Infrastructure Recovery Plan (IRP) to plan and coordinate the recovery of the service. The IRP should also include:

- recovery of specific hardware / infrastructure (some may be referred onto another Infrastructure Recovery Plan);
- recovery of software files;
- recovery of service specific data, using the available backup strategies;
- roles and responsibilities for recovery;
- short term workarounds and alternate working procedures;
- key contact details for all relevant staff involved in the recovery of IT and external parties involved in the recovery of IT.

2.4. Implement

2.4.1 Objectives

The objectives of the Implementation phase of the IT Disaster Recovery Framework are to implement:

- the IT Disaster Recovery plan, including potential acquisitions and site rollouts;
- IT Disaster Recovery training for all staff through a comprehensive training plan and schedule;
- an exercising plan for the IT Disaster Recovery plans on a regular basis, and should be based on an existing exercising plan and schedule.

2.4.2 Implementation

This section is focused on rolling out the IT Disaster Recovery Plan and associated Application Recovery Plans that have been developed.

The information and strategies contained within each plan must first be validated by its associated recovery team to ensure they are realistic, factually accurate and fit for purpose. A business representative must also validate the plan to ensure that it meets their recovery requirements.

Once plans have been validated, they must be ratified by the Organization and the IT Disaster Recovery Owner (Information Technology Director). Following official sign-off, copies of the plans must be provided to the following people and groups:

- IT Disaster Recovery Steering Committee
- IT Disaster Recovery Manager
- IT Disaster Recovery Team(s) and Technical Recovery Teams

- IT DR Owner
- Other key stakeholders, as determined by the IT DR Owner and Steering Committee

The final version of the IT DRP must also be stored securely and visible widely to all of relevant Organization personnel.

2.4.3 Training

Appropriate IT disaster recovery training programs should be developed and implemented to ensure that each staff member with roles and responsibilities assigned during a disaster response have the required knowledge and capability.

The development of a continuity verification process is essential to ensure that employees are familiar with the measures implemented and that they are confident and competent in their use. A training and testing regime also ensures that the dependent resources and faculties / divisions that support the business recovery strategies and are aligned with the plans in place.

Training can be categorized into the following areas:

- awareness - aimed at providing a cross-section of staff with a general understanding of the subject;
- team training - aimed at providing key team appointments with targeted training for their respective roles and responsibilities at providing greater level of understanding for individuals who have a team role;
- coaching - Aimed at providing key team appointments with targeted training for their respective roles and responsibilities including media handling.

A training schedule should be established to provide initial training to all staff who may be called upon during a disaster or be involved in continuity planning. Training may involve participation in components of IT DRP testing.

2.4.4 Testing and Exercising

The development of an effective testing process is essential to ensure that staff are familiar with the recovery measures implemented and that procedures are update and relevant. The IT DRP should be tested on an annual basis or after any major updates to the technical environment. IT Disaster Recovery testing can consist of the following of approaches:

- Table Top - This exercise involves the owner and a subset of users of the plan to read over the plan in detail, and ensure that the information contained remains factually accurate and should theoretically continue to provide effective recovery.
- Walkthrough – This exercise chronologically steps the recovery team through the process for responding to and managing a crisis using the plans and tools specific for the Organization. It is aimed at increasing confidence in the use of the plans and the operation of the team during a crisis.
- Isolated simulation – This exercise involves the live activation of the teams and plans using a realistic, hypothetical scenario limited to a specific application and / or

associated infrastructure. Exercise participants respond to and manage the incident using the IT DRP and any relevant ARPs.

- Integrated Simulation – This exercise involves the live activation of teams and plans using a realistic, hypothetical scenario involving multiple applications and / or associated infrastructure, to test the ability to restore each application within its business requirements when there is an outage involving multiple applications. Exercise participants respond to and manage the incident using the IT DRP and any relevant ARPs.
- Full Simulation - This exercise is the most robust examination of the team and plans. It involves the live activation of teams across more than one level of the organization using a realistic, hypothetical scenario covering all critical applications. Teams are activated to manage the incident using the plan and tools specific to the organization. This exercise is usually incorporated with a Business Continuity or Crisis Management exercise.

Testing Schedule

A testing schedule should be developed and consist of a mixture of the types of testing as outlined above. The following table describes the minimum standard for the frequency for tests.

	Frequency of Testing Across Application Tiers			
Test Type	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Table Top	After initial plan development; when significant changes to the content occur; when changes to the Organization's response or organisational structure occur			
Walkthrough	Twice a year		Annual	Annual
Isolated Simulation	Annual		Annual	No minimum standard
Integrated Simulation	Once every 2 years	No minimum standard		
Full Simulation	At the discretion of the Executive			

Table 2 - Disaster Recovery Test Types & Frequency

Note that when an integrated or full simulation is performed over an application, an isolated simulation need not be performed in the same year as that application's ARP will have been tested already.

It is important to be aware of the costs an interruption to the Organization can have and careful strategizing and consideration must to be undertaken when planning for each test exercise.

Test Document Requirements

The following documents should be maintained as part of each disaster recovery test:

1. Test Notification – Communication to notify appropriate staff of DR testing, including Organization faculties, divisions or staff involved, date, type, locations and applications involved.
2. Test Scope – Provide the background, objectives, application and / or infrastructure scope, risks, issues, assumptions and reporting guidelines.
3. Test Script – This is the actual test plan for the test containing, test objectives, test steps, expected results, actual results, testing staff involved, business owner validation and sign-off.
4. Test Debrief Report – Immediately following each test, a written debrief report should be produced, outlining the overall outcomes of the test, the lessons learnt, the areas for improvement and action items resulting from the test.

Templates for the above documents are provided with the IT DRP.

2.5. Continuous Improvement

The primary goal of the Continuous Improvement phase is to make the IT Disaster Recovery Program at the Organization self-sufficient and sustainable. A formalized continuous-renewal and review feedback cycle should be developed to help ingrain the processes within the Organization and ensure it adapts and grows with the organization.

Continuous Improvement can be achieved by implementing rigorous processes around the management of the program, such as:

- change management of the IT Disaster Recovery program and plans;
- effective testing and update schedules for plans;
- ensuring compliance with industry better practice by performing external reviews of the IT Disaster Recovery program.

As iterations over the lifecycle of the IT Disaster Recovery program are made, areas of improvements will become clear. It is essential that these improvements are captured and explored sufficiently.

If changes are required to the program and / or the IT DRP, they should be validated to ensure the IT DRP remains effective and meets or exceeds the business recovery requirements

3 Roles and Responsibilities

Formalizing the roles and responsibilities of key stakeholders throughout each level of the Organization is a critical component to achieve effective IT disaster recovery. Therefore the entire IT disaster recovery strategy relies on clear definition, allocation and acceptance of individual roles and responsibilities. The following roles could be examples of good practice for a medium to large organization. It is mandatory that these are adopted in a consistent manner across the Organization.

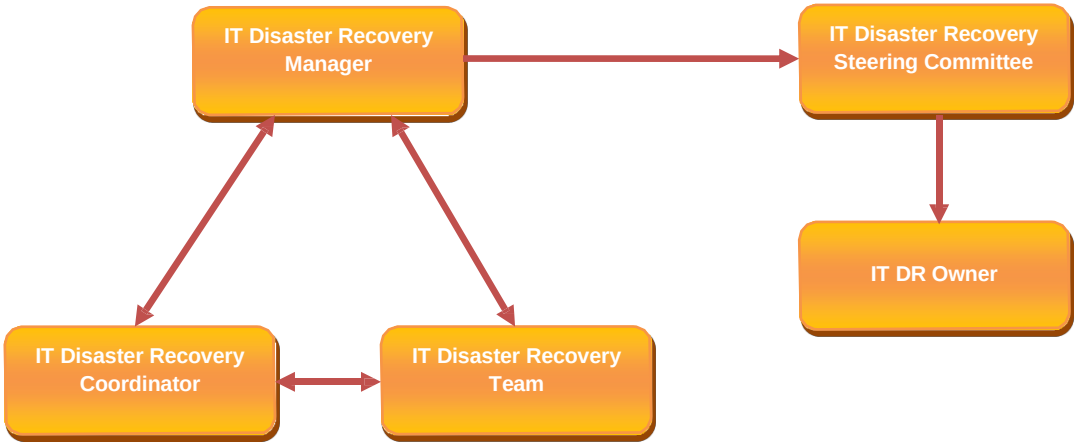

Table 3 - Role Relationships

Role Descriptions can be developed in detail as part of the project