Blue Saffron
Disaster Recovery Primer

Blue Saffron

more than just IT

Table of Contents

06/05/2016

1   Introduction

1.1   Purpose and Objectives

This document is intended to act as a basic primer on disaster recovery (DR) planning.-

1.2   Document Revisions

Revision No.	Date	Summary of changes	Made By
V1.0		Initial draft	

1.3   Disclaimer

This document contains proprietary information that relates to BSL Limited and must not be disclosed in whole or part to any third party. The party to whom this response is addressed may copy the same for the purpose of enabling due consideration of the response. All trademarks are hereby acknowledged. This document is a formal submission and neither party shall have any right or obligation as a result of the preparation or transmittal of this document or otherwise, on account of the subject nature thereof.

2   Disaster Recovery Background

2.1   Background

Although many organizations have a DR plan in place, many are not mature or extensive enough. The following should help start an evaluation of your DR program's maturity level.

2.2   What is Disaster Recovery (DR) Program ?

A disaster recovery (DR) program describes the overall process or planning for DR. And most DR planners will agree that a disaster recovery plan is not complete until it has been tested, identifying gaps in the plan or areas that need improvement. Unfortunately, many companies adopt a "good enough" attitude after a few successful tests and move on to the next IT challenge or more prominent issue. Only a small percentage of companies will seek continued improvement in their disaster recovery program until it reaches a point where the level of recovery capability becomes predictable and highly reliable. These various degrees of this evolution can be described as the disaster recovery planning maturity level.

Disaster recovery is an area where most of the best practices and knowledge focus on the development of the plan itself. In many companies, DR lacks in the area of assessing the quality of the process and how well integrated it is with daily operations. This can be noted by the scarcity of models available to describe the different levels of maturity of a DR plan. A maturity model that comes to mind, although it is aimed at IT services, is the ITIL Process Maturity Framework. ITIL can be used in this context as an example of how to illustrate different levels of maturity. The table below is an example of an ITIL DR rating process, and suggests a way to rate process maturity.

Maturity	ITIL qualifier	Disaster recovery context
Level 1	Initial	A disaster recovery strategy exists and technology is in place.
Level 2	Repeatable	The technology supporting DR has been successfully tested numerous times.
Level 3	Defined	The DR plan is documented in detail.
Level 4	Managed	Alignment of IT with the business -- DR requirements are understood and met.
Level 5	Optimized	Seamless integration with the business and adaptable to meet growth and change.

An example of an ITIL disaster recovery rating process

There could also be a Level 0 in this table, representing the absence of maturity, but the absence of a DR plan or strategy implies on DR maturity, making its evaluation pointless. The above examples are not arbitrary and are only meant to illustrate the actual evolution of a DR program. The real measure lies in evaluating the various aspects of DR planning that differentiate a mature process from one that is only in its infancy. The following is an outline of some key elements that should be evaluated to determine the maturity level of a DR program.

2.3 Areas where your disaster recovery program can be improved

As a self-evaluation exercise, companies can easily rate each of the elements outlined below and assign a value from 1 (lowest) to 5 (highest) based on an honest assessment. Individual values can then be added up to establish an overall score indicating a higher process maturity level (similar to ITIL's Optimized Maturity Level) the closer it gets to its maximum score. And although this approach is not intended to be a failsafe or absolute model, it does provide a self-evaluation mechanism that will help identify areas where your DR program can be improved.

2.3.1 Executive support

Executive support is listed first because without it, the chances of the disaster recovery process reaching maturity in an organization are little to none. Strong executive support for DR beyond simply meeting contractual or regulatory requirements is an indication of good risk management.

2.3.2 Scope

A disaster recovery plan initially focuses on the recovery of critical infrastructure components. As the plan is further refined, other elements are added until eventually, all IT components are within scope.

2.3.3 DR testing

The frequency and quality of DR tests are a good metric to determine maturity of a DR program. Early testing is often limited to tabletop exercises complemented by some partial data restore or isolated system failover. A well-established disaster recovery program tests the alert and notification mechanism, follows DR procedures documentation, includes role playing elements and covers all aspects of IT over a test cycle (i.e., annual or semi-annual).

2.3.4 Documentation quality

Comprehensive and well-documented disaster recovery procedures are always an indication of experience and DR maturity. Companies that are serious about improving their recoverability quickly learn that relying on knowledgeable IT staff member who "*know the environment inside out*" is a bad idea, as employees are not always available when needed.

2.3.5 Maintenance

Maintenance of a disaster recovery plan is directly tied to the documentation quality previously mentioned. Poorly managed disaster recovery programs typically lead to a plan becoming obsolete shortly after its creation. Companies that have done this for a while learn to protect the effort invested in creating the DR plan and develop a mechanism through which the plan is regularly maintained. DR test results are often leveraged for that purpose, but change management and integration with systems design are also leveraged as DR programs are refined.

2.3.6 Change management and disaster recovery planning

Integration of disaster recovery planning with the change management process is a definite sign of a more mature program. Changes that may affect configuration, recoverability, or the recovery procedures are captured as they are implemented and trigger an automatic DR strategy and documentation revision. The main reason DR plans become obsolete is because changes in the environment were not documented; best of class DR programs are fully integrated with change management.

2.3.7   Integration with systems design
IT organizations that include DR requirements and strategy as part of the systems design process are definitely demonstrating DR planning and overall IT maturity. For many organizations, DR planning is an afterthought, and a disaster recovery strategy is often developed after new systems have already been implemented rather than in parallel with the development or design phase. As a result, the disaster recovery strategy is often compromised, incomplete or postponed due to lack of time or funding.

2.3.8   Awareness
Disaster recovery awareness is frequently overlooked in many organizations. DR tends to be the responsibility of a small group or IT staff members. In order to reach a higher level of maturity with many of the disciplines discussed in this article, widespread support is required. Your IT department's ability to create general awareness around the IT recovery goals and objectives is a good DR maturity metric.

2.3.9   Disaster recovery program ownership
Companywide DR awareness is a good thing, but it can also lead to the assumption that "someone is taking care of it." Ownership of the DR program must be assigned to ensure success and constant improvement. Shortfalls and gaps tend to remain unaddressed unless they become someone's responsibility.

2.3.10 Monitoring and measuring
The simple fact that an IT organization seeks to evaluate and monitor its own recovery capabilities and the quality of the DR program in place is a sign of higher maturity. Obtaining a DR performance baseline, leveraging DR test results to increase recoverability and looking at ways to improve the reliability of processes in place are all traits of a maturing DR program.

Obviously and as always, there is no one-size-fits-all approach; the quality of your disaster recovery program must be aligned with your business recovery requirements and budget.