Comprehensive Consulting Solutions, Inc. – “Business Savvy. IT Smart.”®

Disaster Recovery Planning – Process & Options

White Paper

Published: March 2001 (with revisions)

A Framework for the Disaster Recovery Planner

Contents

Preface

The process of creating, testing, and deploying a working Disaster Recovery Plan (DRP) can be daunting. This whitepaper defines, at a high level, the key steps in the creation of a DRP. It is not all-inclusive, but is intended to provide insight into the overall process utilizing a framework that we have used in the past with great success.

Disaster Recovery as part of Business Continuity

As we state in our first Business Continuity white paper, the process of Disaster Recovery Planning is usually concerned with the recovery of a key set of IT systems and infrastructure components. The process of Business Continuity Planning is concerned with the enterprise as a whole, dealing with business functions rather than application systems. Disaster Recovery (DR) can be thought of as the foundation of Business Continuity (BC); a working DRP is a core component of any Business Continuity effort.

Since both DR and BC address the same basic problem – recovery from an unforeseen event and continuation of the business, there are a number of areas with overlap between the two processes. Many companies charter their DR effort as part of their Business Continuity effort. However, just as many will first build a working DRP before taking the next logical step and constructing an overall BCP. With an understanding of the relationship between the two processes, knowledge gained in one area can be leveraged in the other. This framework proposed in this whitepaper can and has been used both for standalone DR efforts as well as integrated BC/DR efforts with success.

Defining Recovery

The first step in creating a working DRP is to define what is meant by "Recovery." This question will drive many of the decisions made as we progress towards a completed DRP, and is one of the main areas of overlap between DR and BC Planning. From the IT perspective, recovery will usually mean establishing support for the processing and communications functions considered critical by the business community, and then establishing support for ancillary systems. From the business perspective, recovery will mean being able to execute the business functions that are at the core of the business, and then being able to execute ancillary functions. It is important that issues that may affect Business Continuity be documented and addressed as part of the DR effort, even if the only action taken is to defer them to the BCP team, or to collate them as input to a future BCP effort if this is a standalone DR project.

Another key factor to consider when defining recovery is the timeframe. Is the goal to have all systems up and running within a day? A week? Is it enough to only bring up a few key systems within the first week, while taking longer to restore others? This factor is often expressed as either the "Recovery Time Objective" (RTO) or the "Service Delivery Objective" (SDO). This refers to the amount of time that can elapse from the failure to the time when the systems or services are available for use. Most often this factor can vary by system or service; for example, a company's order processing system may have a SDO of 24 hours, while the company's intranet has an SDO of 1 week.

What is the difference between RTO and SDO? It is possible to recover one or more "systems" in a short period of time, but due to an unplanned dependency (often unknown until testing the DRP) or recovery failure it is impossible to provide the full and necessary functionality to *restore service*. Hence, while having a good RTO is important, understanding SDO and planning around that goal is even more important. A single failure of a key component that other systems are dependent on can result in failures of many other systems. Because of this it is important to understand the dependencies within your environment.

How much data can you afford lose? This is expressed as the "Recovery Point Objective" or RPO. Depending on the environment, the loss of any data could have a significant impact. A rule of thumb is that the lower the RPO, the higher the overall cost of maintaining the environment for recovery. Please see our presentation on backup and recovery relative to this issue.

An RPO of 10 minutes states that it is acceptable to lose up to 10 minutes of data following an incident, while an RPO of zero effectively states that no data can be lost. Much like RTO/SDO, RPO can differ between systems and services. However, it is important that the interdependencies between systems be understood and taken into account when making this determination. Not doing so can result in inconsistencies that cause problems post-recovery for the organization at various levels (e.g., order processing, inventory management, accounting).

Finally, it is also important to have some way of tracking the various components of a recovery effort. Our approach is to use a "Critical Success Factors" spreadsheet that breaks a recovery effort down by key area, and is weighted by system criticality, downstream dependencies, RTO/SDO, RPO, and impact of failure.

As systems are recovered, the spreadsheet is updated. This provides two main benefits:

- In a DR test scenario, this spreadsheet provides a overall "score" based on the recovery test. This score can then be used as a tangible way to track progress and identify key deficiencies in the overall Disaster Recovery Plan, both for the current test and as part of a baseline metric to track improvement over time.
- In an actual recovery effort, the spreadsheet provides a "checklist" that can be reviewed with management to see the overall progress of the DR effort. It also clearly draws out the ramifications of a failed system through the weighted scoring and dependency lists, as well as to help identify timings with regards to RTO/SDO and RPO.

Disaster Recovery Planning

A Disaster Recovery Planning project cannot be completed in a week or even a month. In many ways, a DRP is never completed – the plan must be tested and updated at least once per year, if not more frequently. A Plan that does not keep pace with the changes in your organization is a disaster in itself, providing a false sense of security. Therefore, while you may have a working plan today, the project needs to be ongoing in order to ensure success if the plan is ever needed.

The primary objectives of a Disaster Recovery Plan are to guide an organization in the event of a disaster and to effectively reestablish critical business operations within the shortest possible period of time with a minimal loss of data. The goals of the planning project are to assess current and anticipated vulnerabilities, define the requirements of the business and IT communities, design and implement risk mitigation procedures, and provide the organization with a plan that will enable it to react quickly and efficiently at the time of a disaster.

It must be remembered that disaster recovery planning is not limited to the IT community. It is equally a business issue, since there may be systems or processes used that are not widely know outside the group using them. At a minimum, the DR Plan must address the processing needs of the business community; this means key members of the business community must be involved in the planning to insure that these needs are adequately documented and understood. IT personnel should not make assumptions as to what systems are critical to the business community.

Whether the DR is a stand-alone effort or is being done in conjunction with an overall BC effort, the following are some of the points which need to be addressed:

- Senior management must understand the level of effort needed to research, define, construct, and test the Plan. There needs to be support and commitment from the top!

- Management must commit to supporting the planning effort and ensure its success both on a short-term and an ongoing basis. This means allocating resources to manage tasks such as documentation and testing on an ongoing basis.

- A project team must be selected that incorporates an adequate balance between IT and business community members to ensure that the resulting Plan will cover the requirements of both the IT and business communities.

- The recovery requirements of the business and IT communities must be defined and agreed upon. Furthermore, they should be posted somewhere accessible to everyone in the organization (such as the company intranet). This type of visibility helps ensure that people realize the importance in the effort, and their role in its success.

- Solutions to fit the requirements of the business and the IT communities, including risk identification, analysis, and mitigation, must be designed. For more information on risk management as it relates to BC/DR, please see our whitepaper on Managing risk (http://www.comp-soln.com/whitepapers).

- The final Plan, which incorporates those solutions, must be easy to understand (by people unfamiliar with the systems and under stress), put into practice, and easy to maintain.

- The final Plan needs to be integrated with any other existing plans – including other DR Plans, Emergency Management Plans, Evacuation Plans, etc. This is usually part of an overall BC effort, but in the case of a standalone DR effort this should still be addressed.

- A process needs to be developed to keep the plan up to date, representing the true business and computing environments at all times. It must also be understood that disaster recovery planning is a highly complex and time-consuming activity and requires a firm commitment from management to expend the man-hours and funds necessary to achieve success. In addition, implementing solutions designed to mitigate risk often necessitates major expenditures.

Disaster Recovery Planning Project Steps

Just as every organization is unique, so too is each Disaster Recovery Planning project. As such, each plan should be tailored to the individual organization – what works for one organization will not necessarily work for another. The following are the major phases and guidelines that we use as part of our DR Planning strategy; however these are guidelines only and should be modified or supplemented as necessary and as dictated by your organizational requirements.

Step I – Project Initiation

The objectives of the disaster recovery planning project initiation are to gain an understanding of the existing and planned future IT environment of the organization, define the scope of the project, develop the project schedule, and identify risks to the project. If the DR project is to be undertaken as part of a BCP effort, this needs to be considered as part of the initiation process. By running the DR and BC efforts in parallel many of the following phases (such as risk analysis and business impact analysis) can be streamlined. Input from the BCP team will be required as part of the requirements analysis phase.

In addition, a Project Sponsor/Champion and Steering Committee should be established during this phase. The Project Sponsor/Champion should be a member of the Senior Management team with the required authority to push the project to completion – in most organizations, this will be the CEO or CFO, although with a standalone DR effort the CIO may fill this role. As with any project, the Steering Committee has the responsibility to provide guidance to the project team. The Committee should be composed of key personnel from the business and IT communities. At this time a Disaster Recovery Coordinator and/or Project Manager should be assigned and empowered to make this project a success.

Step II – Assessment of Disaster Risk

This should include, but not be limited to, an assessment of geographical location, building composition, computing environment/physical plant security, installed security devices (including automated fire extinguishers and automated shut-down devices), computing environment/physical plant access control systems and software, personnel practices, operating practices, and backup practices. This is a good time to perform an IT Assessment, Practices and Procedures Audit, and Single Points of Failure Analysis.

Step III – Business Impact Analysis

An analysis of all key business units that are supported by the IT community should be undertaken to identify which systems and functions are truly critical to the continuation of business, and to determine the length of time that those units can survive without the critical systems in operation. This analysis is essential to making decisions about how to implement disaster recovery.

Step IV – Definition of Requirements

This will be one of the most difficult and time-consuming parts of the project. All requirements of, and relating to, the Plan must be defined and detailed. These will include, but not be limited to, the recovery requirements of the business and IT communities, the requirements generated by the business impact analysis, and the requirements generated by the assessment of disaster risk and the mitigation of disaster risk.

Step V – Project Planning

It is important here to distinguish between the Project Plan and the Disaster Recovery Plan. The Project Plan in this case will define the project that is being executed and as one of its objectives will develop the Disaster Recovery Plan. An additional objective of this project is to mitigate as much disaster risk as possible. The value of professional project management cannot be overstated in an important, highly-visible project such as this.

Step VI – Project Execution

The project should proceed according to standard practices of Project Management. During the project the identified methods of mitigating risk will be executed, and the Disaster Recovery Plan will be constructed and tested.

Step VII – BCP Integration

The DR Plan needs to integrate back into the organization’s overall Business Continuity efforts. For an organization that has run the DR effort as part of an overall BC effort, this has likely already been done. However, for an organization that builds their DRP first and then creates a BCP from that foundation it is important to align the two.

Step VIII – Ongoing Maintenance and Integration

Part of the plan will include the ongoing maintenance and testing efforts required to keep the Plan up to date, as well as processes to identify and mitigate future risks as they are encountered.

Summary

Disaster Recovery Planning / Business Continuity Planning are complex and difficult processes, but can truly be a lifesaver for a company. They can be thought of as an insurance policy that you will hopefully never use. Please see our other White Papers on Disaster Recovery Planning, Business Continuity Planning, and Project Management at http://www.comp-soln.com/whitepapers/

Click here to view a slide presentation on this topic from a conference presentation.

About the Author

Chip Nickolett, MBA, PMP is the President of Comprehensive Solutions. His first disaster recovery project was in 1994 for a large insurance company, and he has been actively engaged in disaster recovery projects since then, establishing a BC/DR practice area within Comprehensive Solutions. For more information please see http://www.Comp-Soln.com/chipn.html.

Let Us Help You Succeed!

Call today to discuss ways that Comprehensive Solutions can help your organization save money and achieve better results with your IT projects. We provide the ***confidence*** that you want and deliver the ***results*** that you need.

View our Disaster Recovery Brochure

Back to White Papers

Back to Services

Comprehensive Solutions
4040 N. Calhoun Road
Suite 105
Brookfield, WI 53005
U.S.A.

Phone: (262) 544-9954
Fax: (262) 544-1236

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to Comprehensive Consulting Solutions. Comprehensive Consulting Solutions, Inc. does not provide any warranties covering and specifically disclaims any liability in connection with this document.

All product names referenced herein are trademarks of their respective companies. Use of these names should not be regarded as affecting the validity of any trademark or service mark.