



**“Before any disaster plan can be implemented, it is absolutely critical to establish the recovery requirements. This involves a thorough understanding of your applications and the way they relate to everyday business”<sup>1</sup>**

**How much data can you afford to lose?**

#### **Recovery Point Objective (RPO)**

The maximum possible length of time for which data could be irretrievably lost if a disaster occurs – usually equivalent to the time interval between backups

**How long can I afford to be down?**

#### **Recovery Time Objective (RTO)**

The maximum length of time for which service could be down after a disaster is declared (Note: The point in time when a disaster is declared is not necessarily coincidental with time that a disaster actually strikes)

<sup>1</sup>CIO News, “Disaster Recovery Planning: Special Report”, May 31, 2006, Stephen J. Bigelow

## Executive Brief: Disaster Recovery Planning

The demand for information is increasing exponentially, and the tolerance for being without information – by customers, employees, suppliers, and especially, by regulators – is decreasing at an even faster rate. Organizations need to be prepared by having solutions in place to ensure that stakeholders are always connected to mission-critical information.

#### **Business Continuity Requirements**

Business Continuity involves more recovering an organization’s IT environment in the event of a disaster. Business Continuity ensures that an organization can restore its IT systems, business processes and that its people can be back in operation despite disruptions to the business that may be beyond its control.

Today’s Business Continuity solutions must keep organizations up and running despite unplanned interruptions. Service availability and recovery strategies should extend beyond the data center to the entire enterprise and value chain. A comprehensive Business Continuity solution should also include a networking plan that addresses specific needs for redundancy, diversity and recoverability.

#### **Disaster Recovery - Striking the Balance**

The Chief Financial Officer and Chief Information Officer typically have the responsibility to plan for Disaster Recovery (DR), that is Data Protection and Service Restoration for IT systems. Their initial focus should be on determining the probability for unanticipated disruption and the resultant business impact. Next, prudent executives consider the magnitude of the financial impact for this probable event versus the real costs, in today’s dollars, of preparing for, mitigating or avoiding this undesirable financial impact. Further complicating the analysis is the difficulty of quantifying and factoring in the damage to a company’s reputation, brand equity and the real possibility of a significant loss in valuation. These strategic decisions require due diligence to strike the right balance.

Many executives consider Disaster Recovery decisions to be similar to the evaluation process used when buying insurance. The decision variables for Disaster Recovery include the Recovery Time Objective (RTO), the Recovery Point Objective (RPO), and the level of system and operating capacity that is absolutely necessary restore business-critical operations. A reputable vendor who understands an organization’s business processes, information technology and application software is well positioned to help executives make good choices in these areas.



### Disaster Recovery Terms

#### Data Protection

Restoration of an organization's critical data, subject to the RTO and RPO service levels

#### Service Recovery

Restoration of required level of service to continue mission-critical operations, usually at an alternative site

#### Capacity

The level of service restoration (e.g. Restoring customer service operations to 80% of normal level)

#### Electronic Vaulting

Electronic transmission of data to a remote site (called a data vault).  
Electronic Vaulting is an alternative to tape backup, usually with improved RPO (less data lost)

### Data Protection and Service Recovery

Most companies have some amount of business-critical information and getting this data and the associated information systems up and running should be their first priority. Recovery of the information systems and recovery of business-critical information are unique to each organization; to one it is a call center database, to another it is their payroll system, and to another, it is their shipping records. Although critical information is unique, the way to protect and restore this information need not be.

Even the most secure primary locations have the potential for catastrophic loss, as has been demonstrated by the tragic events of September 11, the Northeast Blackout, and Hurricanes Rita and Katrina. Simple on-site redundancy is a good start, but what if a disaster occurs that impacts your place of business?

A good Disaster Recovery plan should be comprehensive, considering data and service recovery, data and record management, network, infrastructure, security and regulatory compliance. Forward-thinking businesses often incorporate data replication or electronic vaulting to a secure remote location to protect their critical information. A remote location ensures that any catastrophic loss to a company's facility or infrastructure will not result in the loss of mission critical information as well.

To provide a level of service, or capacity to resume mission critical operations, a service provider can "share" capacity among many customers, and can usually provide this protection more cost effectively than an individual customer could on their own.

### Plan for the Worst, Hope for the Best

It's never been more important to ensure that people and information are always connected. When employees, customer, suppliers or partners can't gain access to the information they need, business suffers. Organizations that utilize a remote location for data backup and service recovery as part of a well conceived plan that is tested periodically will greatly increase the probability of getting their information restored within a reasonable timeframe following a disaster.

The time to begin to develop or to re-evaluate your Disaster Recovery plan is now. Lost information and unplanned downtime can cost your company its revenue, productivity, and customer confidence. Contact your Oracle representative to help you develop a Business Continuity plan that balances risk and cost; a plan that is well designed to ensure the survival of your business.

### CONTACT US

To learn more, visit us at [oracle.com/ondemand](http://oracle.com/ondemand) or call 888-264-5909 to speak with an Oracle representative