

Disaster Recovery Plan

A **disaster recovery plan** is a written plan describing the steps a company would take to restore computer operations in the event of a disaster. Every company and each department or division within an enterprise usually has its own disaster recovery plans. A disaster recovery plan contains four major components: the emergency plan, the backup plan, the recovery plan, and the test plan.

The Emergency Plan An *emergency plan* specifies the steps to be taken immediately after a disaster strikes. The emergency plan usually is organized by type of disaster, such as fire, flood, or earthquake. Depending on the nature and extent of the disaster, the procedures that are followed in an emergency will differ. All emergency plans should contain the following information:

1. Names and telephone numbers of people and organizations to notify (e.g., management, fire department, police department)

2. Procedures to follow with the computer equipment (e.g., equipment shutdown, power shutoff, file removal)
3. Employee evacuation procedures
4. Return procedures; that is, who can reenter the facility and what actions they are to perform

The Backup Plan Once the procedures in the emergency plan have been executed, the next step is to follow the backup plan. The *backup plan* specifies how an organization uses backup files and equipment to resume information processing. The backup plan should specify the location of an alternate computer facility in the event the organization's normal location is destroyed or unusable.

When operations are so important that an organization cannot afford to lose the operations to a disaster, the organization often maintains a *hot site*, which is a separate facility that mirrors the systems and operations of the critical site. The hot site always operates concurrently with the main site, so that if either site

becomes unavailable, the other site continues to meet the organization's needs. The process of one system automatically taking the place of a failed system is called *failover*. A *cold site* is a site that mirrors the critical site, but does not become operational until the critical site becomes unavailable. When using a cold site, some time elapses between the disaster and when the cold site becomes functional.

The backup plan identifies these items:

1. The location of backup data, supplies, and equipment
2. The personnel responsible for gathering backup resources and transporting them to the alternate computer facility
3. A schedule indicating the order in which, and approximate time by which, each application should be up and running

For a backup plan to be successful, the organization must back up all critical resources. Also, additional people, including possibly nonemployees, must be trained in the backup and recovery procedures because organization personnel could be injured in a disaster.

The location of the alternate computer facility is important. It should be close enough to be convenient, yet not so close that a single disaster, such as an earthquake, could destroy both the main and alternate computer facilities. Some organizations preinstall all the necessary hardware, software, and communications devices at the alternate computer facility. These facilities immediately are ready in the event of a disaster. In other cases, the alternate computer facility is simply an empty facility that can accommodate the necessary computer resources, if needed. One more alternative is to enter into a *reciprocal backup relationship* with another firm, where one firm provides space and sometimes equipment to the other in case of a disaster.

The Recovery Plan The *recovery plan* specifies the actions to be taken to restore full information processing operations. As with the emergency plan, the recovery plan differs for each type of disaster. To prepare for disaster recovery, an organization should establish planning committees, with each one responsible for different forms of recovery.

For example, one committee is in charge of hardware replacement. Another is responsible for software replacement.

The Test Plan To provide assurance that the disaster plan is complete, it should be tested. A disaster recovery *test plan* contains information for simulating various levels of disasters and recording an organization's ability to recover. In a simulation, all personnel follow the steps in the disaster recovery plan. Any needed recovery actions that are not specified in the plan should be added. Although simulations can be scheduled, the best test of the plan is to simulate a disaster without advance notice. Read Innovative Computing 14-2 to find an example of another type of simulation.



INNOVATIVE COMPUTING 14-2

PS3s Perform Rocket Science

Sony's PlayStation 3 has won the hearts of some gamers, but it also is finding a home in scientific labs. Astrophysicists at the University of Massachusetts networked 15 PS3s, installed Linux, and programmed the supercomputer to simulate black hole activity.


Their PS3 Gravity Grid outperforms the best desktop computers available and is powered by a Cell processor, which has six special computing engines that can perform multiple mathematical operations in a single step. The researchers claim this speed, combined with the PS3's relatively low cost, give their Gravity Grid the least expensive raw computing power per dollar of any computer available today.

The PS3s are being used for several projects. The Binary Black Hole Coalescence study estimates the properties of gravitational waves generated when two enormous black holes collide. Albert Einstein predicted these traveling ripples in his general relativity theory. Another project, called AstroPulse, searches for high-power broadband signals being sent from possible black holes, pulsars, and civilizations on distant planets.



Disaster Recovery Plan

For more information, visit scs.site.com/dc2011/ch14/ weblink and then click Disaster Recovery Plan.

 For more information, visit scs.site.com/dc2011/ch14/innovative and then click PS3.