

► Steps to Developing an Effective Disaster Recovery Process

Figure 18–1 lists the 13 steps required to develop an effective disaster recovery process. For the purposes of our discussion, disaster recovery is a process within a process in that we are including steps that involve contracting for outside services. We realize that, depending on the size and scope of a shop, not every disaster recovery process will require this type of service provider. We include it here in the interest in being thorough and because a sizable percentage of shops do utilize this kind of service.

Step 1: Acquire executive support. The acquisition of executive support, particularly in the form of an executive sponsor, is the first step necessary for developing a truly robust disaster recovery process. As mentioned earlier, there are many resources required to design and maintain an effective program, and these all need funding approval from senior management to initiate the effort and to see it through to completion.

-
1. Acquire executive support.

 2. Select a process owner.

 3. Assemble a cross-functional team.

 4. Conduct a business impact analysis.

 5. Identify and prioritize requirements.

 6. Assess possible business continuity strategies.

 7. Develop a request for proposal (RFP) for outside services.

 8. Evaluate proposals and select best offering.

 9. Choose participants and clarify their roles for the recovery team.

 10. Document the disaster recovery plan.

 11. Plan and execute regularly scheduled tests of the plan.

 12. Conduct a lessons-learned postmortem after each test.

 13. Continually maintain, update, and improve the plan.

Figure 18–1 Steps to Developing a Disaster Recovery Process

Another reason this support is important is that managers are typically the first to be notified when a disaster actually occurs. This sets off a chain of events involving management decisions about deploying the IT recovery team, declaring an emergency to the disaster recovery service provider, notifying facilities and physical security, and taking whatever emergency preparedness actions may be necessary. By involving management early in the design process, and by securing their emotional as well as financial buy-in, you increase the likelihood of management understanding and flawlessly executing its roles when a calamity does happen.

There are several other responsibilities of a disaster recovery executive sponsor. One is selecting a process owner. Another is acquiring support from the managers of the participants of the cross-functional team to ensure that participants are properly chosen and committed to the program. These other managers may be direct reports, peers within IT, or, in the case of facilities, outside of IT. Finally, the executive sponsor needs to demonstrate ongoing support by requesting and reviewing frequent progress reports, offering suggestions for improvement, questioning unclear elements of the plan, and resolving issues of conflict.

Step 2: Select a process owner. The process owner for disaster recovery is the most important individual involved with this process because of the many key roles this person plays. The process owner must assemble and lead the cross-functional team in such diverse activities as preparing the business impact analysis, identifying and prioritizing requirements, developing business continuity strategies, selecting an outside service provider, and conducting realistic tests of the process. This person should exhibit several key attributes and be selected very carefully. Potential candidates include an operations supervisor, the data center manager, and even the infrastructure manager.

The executive sponsor needs to identify as many of these key attributes as possible in an individual and choose the individual accordingly. Table 18–1 lists these characteristics in priority order. The finished plan needs to be well documented and kept current, making the ability to evaluate documentation highly desirable. So also is the ability to talk effectively with executives, particularly when prioritizing their critical processes and applications. A strong working knowledge of network software and components is recommended because any recovery process taking place today will rely heavily on the connectivity and compatibility of backup networks to those at the customer site.

Knowledge of backup systems is also very key since the restore process—with its numerous variables that can hamper recovery—is so critical to this activity. The last high-priority characteristic is the ability to think and act strategically. This means designing a process that keeps the strategic business priorities of the company in mind when deciding which processes need to be recovered first.

Step 3: Assemble a cross-functional team. Representatives of appropriate departments from several areas inside and outside of IT should be assembled into a cross-functional design team. The specific departments involved will vary from shop to shop, but Figure 18–2 lists a representation of typical groups normally participating in such a team. This team will work on requirements, conduct a business impact analysis, select an outside service provider, design the final overall recovery process, identify members of the recovery team, conduct tests of the recovery process, and document the plan.

Table 18–1 Prioritized Characteristics of a Disaster Recovery Process Owner

	Characteristic	Priority
1.	Ability to evaluate documentation	High
2.	Ability to talk effectively with IT executives	High
3.	Knowledge of network software and components	High
4.	Knowledge of backup systems	High
5.	Ability to think and plan strategically	High
6.	Knowledge of applications	Medium
7.	Ability to meet effectively with IT customers	Medium
8.	Knowledge of systems software and components	Medium
9.	Knowledge of software configurations	Medium
10.	Knowledge of hardware configurations	Medium
11.	Ability to work effectively with IT developers	Low
12.	Knowledge of database systems	Low
13.	Knowledge of desktop hardware and software	Low
14.	Ability to think and act tactically	Low

Step 4: Conduct a business impact analysis. Even the most thorough of disaster recovery plans will not be able to cost justify the expense of including every business process and application in the recovery. An inventory and prioritization of critical business processes should be taken representing the entire company. Key IT customers should help coordinate this effort to ensure that all critical processes are included. Processes that need to be resumed within 24 hours to prevent serious business impact, such as loss of revenue or major impact to customers, are rated as an A priority. Those processes that need to be resumed within 72 hours are rated as a B, and greater than 72 hours are rated C. These identifications and prioritizations will be used to propose business continuity strategies.

Step 5: Identify and prioritize requirements. One of the first activities of the cross-functional team is to brainstorm the identity of requirements for the process, such as business, technical, and logistical requirements. Business requirements include defining the specific criteria for declaring a disaster and determining which processes are to be recovered and in what time frames. Technical requirements include what type of platforms will be eligible as recovery devices for servers, disk, and desktops and how much bandwidth will be needed. Logistical requirements include the amount of time allowed to declare a disas-

1.	Computer operations
2.	Applications development
3.	Key customer departments
4.	Facilities
5.	Data security
6.	Physical security
7.	Network operations
8.	Server and systems administration
9.	Database administration

Figure 18–2 Potential Departments Represented on a Cross-Functional Disaster Recovery Process Design Team

ter and transportation arrangements at both the disaster site and the recovery site.

Step 6: Assess possible business continuity strategies. Based on the business impact analysis and the list of prioritized requirements, the cross-functional team should propose and assess several alternative business continuity strategies. These will likely include alternative remote sites within the company and geographic hot sites supplied by an outside provider.

Step 7: Develop an RFP for outside services. Presuming that the size and scope of the shop is sufficiently large and that the requirements involving business continuity warrant outside services, the cross-functional team develops an RFP, which is a proposal for an outside provider to supply disaster recovery services. Options should include multiple-year pricing, guaranteed minimum amount of time to become operational, costs of testing, provisions for local networking, and types of onsite support provided. Criteria should be weighted to facilitate the evaluation process.

Step 8: Evaluate proposals and select the best offering. The weighted criteria previously established by the cross-functional team is now used by them to evaluate the responses to the RFP. Visits to the bidder's facilities and testimonials from customers should be part of the evaluation process. The winning proposal should go to the bidder who provides the greatest overall benefit to the company, not simply to the lowest cost provider.

Step 9: Choose participants and clarify their roles for the recovery team. The cross-functional team chooses the individuals who will participate in the recovery activities after any declared disaster. The recovery team may be similar to the cross-functional team as suggested in Figure 18–2, but should not be identical. Additional members should include representatives from the outside service provider, key customer representatives based on the prioritized business impact analysis, and the executive sponsor. Once the recovery team is selected, it is imperative that each individual's role and responsibility be clearly defined, documented, and communicated.

Step 10: Document the disaster recovery plan. The last official activity of the cross-functional team is to document the disaster recovery plan for use by the recovery team, which will then have responsibility for maintaining its accuracy, accessibility, and distribution. Documentation of the plan must also include up-to-date configuration

diagrams of the hardware, software, and network components involved in the recovery.

Step 11: Plan and execute regularly scheduled tests of the plan. Disaster recovery plans should be tested a minimum of once per year. During the test, a checklist should be maintained to record the disposition and duration of every task that was performed for later comparison to those of the planned tasks. Infrastructures with world-class disaster recovery programs test at least twice per year. When first starting out, particularly for complex environments, consider developing a test plan that spans up to three years—every six months the tests can become progressively more involved, starting with program and data restores, followed by processing loads and print tests, then initial network connectivity tests, and eventually full network and desktop load and functionality tests.

Dry-run tests are normally thoroughly planned well in advance, widely communicated, and generally given high visibility. Shops with very robust disaster recovery plans realize that maintaining an effective plan requires testing that is as close to simulating an actual disaster as possible. One way to do this is to conduct a full-scale test in which only two or three key people are aware that it is not an actual disaster. These types of drills often flush out minor snags and communication gaps that could prevent an otherwise flawless recovery from actually occurring. Thoroughly debrief the entire team afterward, making sure to explain the necessity of the secrecy.

Step 12: Conduct a lessons-learned postmortem after each test. The intent of the lessons-learned postmortem is to review exactly how the test was executed as well as to identify what went well, what needs to be improved, and what enhancements or efficiencies could be added to improve future tests.

Step 13: Continually maintain, update, and improve the plan. An infrastructure environment is ever changing. New applications, expanded databases, additional network links, and upgraded server platforms are just some of the events that render the most thorough of disaster recovery plans inaccurate, incomplete, or obsolete. A constant vigil must be maintained to keep the plan up to date and effective. Changes in personnel affecting training, documentation, and even budgeting for tests are some additional concerns to keep in mind when maintaining a disaster recovery plan.