



INTRODUCTION

The world is full of disasters just waiting to happen. Fires, hurricanes, power failures, network outages, processor failures, human error...the list goes on and on. It's not a question of whether disaster will strike, only when. It's estimated that more than 50% of companies never recover from such disasters. Disaster Recovery planning is the key to survival.

A major part of developing a program for Disaster Recovery is determining the potential risks to the organization, and their impact on the organization's ability to continue providing services and adhering to new government regulations. This should help you to determine if your company needs to create a disaster recovery program or upgrade what you currently have.

The following checklist, though not comprehensive, should provide you with questions that will stimulate dialogue with key stakeholders both within your organization as well as outside partners. It will help your organization prioritize your most critical databases and applications.

Look at the issues and assess where your organization rates in these areas. This will determine what actions may or may not need to be taken. To learn more about the appropriate actions to take, contact Sybase at 1 800-8-SYBASE.

DISASTER RECOVERY BASICS

- Does a major data loss put your organization at risk?
- If so, what are the critical systems, and how long can they be down without effecting business operations?
- Can you minimize the number of critical data systems for quick recovery?
- Do you need to protect your market share and reputation in case of system failure? And insure customer confidence in your company?
- Would downtime create legal or contractual issues?
- Would lack of a disaster recovery plan affect your insurance premiums?
- Do you have an off-site recovery area? If not, you need to determine if you need one and if it will be a hot, warm or cold site.

FUNDAMENTALS

- Do you currently have buy-in from senior management for a disaster recovery plan?
- If not what will it take to get that buy-in?
- Does the organization have an IT disaster recovery plan, as part of an overall recovery plan for the organization? Is it current?
- Is there a disaster recovery committee?
- Does it include members from IT, businesses and senior management?
- What are the critical points of failure?
- How critical are they to your organization's continuing business?
- Does the plan detail actions for 'disasters' that are internal as well as external?



EVALUATE THREATS – WHAT IS THE POTENTIAL FOR:

- Environmental disasters
- Organized and/or deliberate disruptions
- Loss of utilities and service
- Equipment or system failures
- Serious information security incidents
- Building risks, internal power, redundancy, network, etc.
- Human error
- Other emergency situations

IDENTIFY FINANCIAL RISKS

See detailed questionnaire in Appendix A

- What is the impact of IT system failure on the organization – cost, reputation, legal, etc.?
- Identify interdependencies for internal and external users and costs
- Have owners assign criticality of application, systems and utilities
- Develop prioritized list of applications, systems for the survival of the business
- Set the maximum recovery times for the critical applications, systems
- Set the maximum data loss for each application
- Determine cost of maintaining availability of critical systems and applications

NETWORK RISKS

- Which network assets will have a large adverse impact on the organization if they are modified without authorization?
- Which network assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which network assets will have a large adverse impact on the organization if access to them is interrupted?
- Does Local Area Networks (LAN) used in support of emergency operations have adequate protection against cyber attack?
- Does a Network diagram exist and is it kept updated?
- Is computer hardware and communications equipment identified with manufacturer, model/serial numbers?



SYSTEM RISKS

- Which system assets will have a large adverse impact on the organization if they are modified without authorization?
- Which system assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which system assets will have a large adverse impact on the organization if access to them is interrupted?
- Is the number of servers adequate to support emergency response operations?
- Is the software identified by name, description, supplier, and version number?
- Do you know the location of system software source code and/or installation diskettes, CD ROM's?
- Do you have installation and maintenance procedures, id/serial numbers?
- Are there secure system passwords?
- Is there a complete list of system software and utilities by location and owners?

STORAGE RISKS

- Which storage assets will have a large adverse impact on the organization if they are modified without authorization?
- Which storage assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which storage assets will have a large adverse impact on the organization if access to them is interrupted?
- What is the potential for infrastructure disruption by configuration changes, rogue switch or servers, data unavailability?
- What is the potential risk for modification or destruction of data in flight?
- What is the potential for Denial of Service?
- Identify all interfaces to your SAN

APPLICATION RISKS

See detailed questionnaire in Appendix B

- Which applications will have a large adverse impact on the organization if they are modified without authorization?
- Which applications will have a large adverse impact on the organization if they are lost or destroyed?
- Which applications will have a large adverse impact on the organization if access to them is interrupted?
- How long can critical applications be unavailable?
- Does the organization have backup for all critical applications?
- Can you switch to another server/site for the application, if the application is unavailable at the primary site?
- Does the organization have secure passwords for the applications?



DATABASE RISKS

- Which databases will have a large adverse impact on the organization if they are modified without authorization?
- Which databases will have a large adverse impact on the organization if they are lost or destroyed?
- Which databases will have a large adverse impact on the organization if access to them is interrupted?
- Do you test all database changes in a production-representative staging area?
- Do you collect and actively monitor internal database statistics?
- Do you monitor external database response times?
- Do you back up or replicate your databases in a timeframe for restart or switching based on their criticality?
- Are there government regulatory requirements, which dictate how long your business must maintain database data?

MESSAGING RISKS

- Which messaging assets will have a large adverse impact on the organization if they are modified without authorization?
- Which messaging assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which messaging assets will have a large adverse impact on the organization if access to them is interrupted?
- Do you have a single, centralized message store?
- How often is (are) the message store (or message stores) backed up?
- How long do you maintain the message store(s)?
- Are there government regulatory requirements that dictate how long your business must maintain message stores?
- How long can messaging queues be maintained in the event of a network outage?

SUPPORT INFRASTRUCTURE RISKS

- Which assets will have a large adverse impact on the organization if they are modified without authorization?
- Which assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which assets will have a large adverse impact on the organization if access to them is interrupted?
- Do you proactively monitor individual components of your infrastructure?
- Do you have a centralized Network Operations Center for network monitoring and support?
- Do you have a centralized Enterprise Systems Monitoring facility for systems and applications monitoring and support?
- Do you have a centralized help desk for incident reporting and tracking?



TELEPHONY RISKS

- Which telephony assets will have a large adverse impact on the organization if they are modified without authorization?
- Which telephony assets will have a large adverse impact on the organization if they are lost or destroyed?
- Which telephone assets will have a large adverse impact on the organization if access to them is interrupted?
- Do you have a secure voice capability?
- Are telephones connected to an in-house Private Branch Exchange (PBX)?
- Are telephones connected directly to a local commercial carrier?
- Is the number of facsimiles, secure and non-secure, adequate to conduct emergency response operations?

PERSONNEL

- Is staff assigned to specific duties in case of a disaster?
- Are assignments documented for everyone to be able to find in case of emergency?
- Are training programs set up for personnel tasks?
- Are all procedures reviewed on a regular basis?
- Is staff cross-trained to ensure for vacations, sick time, etc.?
- Can you easily move personnel to another site for disaster recovery, or can other personnel keep the business going after a disruption?
- Are these tasks documented and updated in the form of a plan that could be accessed remotely?

DETERMINING ALTERNATIVES FOR DISASTER RECOVERY SITES

Recovery Strategy	Pros	Cons
<i>Cold Internal Site</i>	Low Cost Fast Implementation	Long recovery times More risk – hard to test
<i>Hot Internal Site</i>	Reduced Recovery Time Service Segmentation Resource Flexibility	High Cost High Complexity
<i>Shared Services at Provider</i>	Outsource Complexity	Very expensive Shared resources Control
<i>Dedicated Hot Site at Provider</i>	Outsource Complexity Shorter Recovery times	Most expensive Control



**DETERMINING THE LEVEL OF SERVICE NEEDED PER
DATABASE/APPLICATION**

Max Recovery Time/Accepted Data Loss	Potential Solution Architecture	Cost and Complexity
<i>2Min./0</i>	Transaction Duplication	\$\$\$\$\$
<i>4H/1H</i>	Database Replication/Mirroring	\$\$\$\$
<i>12H/4H</i>	Standby Database	\$\$\$
<i>24H/1D</i>	Disk Copy Tape Backup	\$\$
<i>3D/1D</i>	Offsite Backup	\$

**TO LEARN MORE ABOUT THE APPROPRIATE ACTIONS
TO TAKE, CONTACT SYBASE AT 1 800-8-SYBASE.**



Appendix A

OVERVIEW OF THE BUSINESS FUNCTIONS

Example: Corporate functions, business functions, IT functions, etc.

1. Describe the unit location(s): _____

2. Briefly describe the unit's functions: _____

3. What is the production output of your department? _____

4. What is the average daily dollar volume processed by the business unit? _____

5. What is the average daily item or transaction volume processed by the unit? _____

6. Does the unit have any peak volume or otherwise critical times? If the unit does, please list the times as well as the average dollar and item or transaction volumes processed at those times: _____

7. What are the CRITICAL business functions performed? (Prioritize these functions)

Critical Functions	Priority
a. _____	_____
b. _____	_____
c. _____	_____
d. _____	_____
e. _____	_____
f. _____	_____

8. What are the business and applications interdependencies between departments? _____



Appendix A

9. What are the critical applications/network systems that support the above business functions performed?
Critical Applications/Network Systems

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____

10. What are the critical equipment/resources that support the above business functions performed?
Critical Equipment/Resources

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____

11. Functional Reductions: What business processes and tasks are less critical to the recovery of your department and can be delayed or postponed? Include why and the potential processing impact of each delay to your area, and impact to other areas (*if known*).

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____

12. How are the following "mission critical" items protected in your business function?

Source Documents: _____

Contract: _____

Operating Manuals: _____

Building Prints: _____

Legal Documents: _____

Personnel Records: _____

Other: _____



APPLICATION IMPACT ANALYSIS

Complete one questionnaire for each application supporting this department.

1. If the computer processing of (application name) were interrupted, which functions would be affected?

Application Name: _____

Business Function: _____

2. Do you have an alternative method for performing the business functions other than through the support of (application name)? Yes No

If yes, explain the alternative method.

If yes, explain the alternative method.

How long can you operate under these conditions?

Can you operate under these conditions with your current staff or will you need more personnel?

3. Have you ever performed this business function using the alternative? Yes No

If yes, complete the following:

a. When did you do this? *(Describe the incident, not the date.)*

b. How did the alternative method work?

c. How long did the business operate in that fashion?



Appendix B

d. What problems occurred? How did you resolve them?

4. Identify the type of impact a computer interruption would have on the business function and at what point in time it would have a significant impact on the company.

Type of impact (*check all types that apply*)

- a. A loss of business (*current*)
- b. A loss of business (*future*)
- c. A loss of dollars
- d. Problems with regulatory agencies
- e. A lawsuit filed against the company
- f. Other impacts (*explain*): _____

Impact:

a. Twenty-four hours; describe the significant impact.

b. Two or three workdays; describe the significant impact.

c. Four to five workdays; describe the significant impact.

d. Six to ten workdays; describe the significant impact.

e. Ten or more workdays; describe the significant impact.



Appendix B

5. What back-up procedures are followed, how frequently are they performed, and where are they stored?

6. If back-up tapes are stored off-site, where are they located? Are they in a safe distance such that a regional disaster would not impact tapes/optical media?

7. Are back-up tapes tested to ensure their integrity? *(For example, are back-up tapes used to load systems every year, etc.)* How do you know they function properly?

8. What are the interdependencies between computer equipment, applications, file systems, etc.
