How do YOU Spell Disaster Relief?
C-O-N-T-I-N-G-E-N-C-Y P-L-A-N-N-I-N-G
(Business Resumption Planning)

A. Perry Sellars Jr.
Lead Operational Assessor
Hewlett Packard Company
545 North Pleasantburg Dr.
Suite 100
Greenville, SC 29607
(864) 241-2057
(864) 241-2061 fax
perry_sellars@hp.com

How do YOU Spell Disaster Relief?
C-O-N-T-I-N-G-E-N-C-Y P-L-A-N-N-I-N-G
(Business Resumption Planning)

The ABC Company expanded an existing facility to house the manufacturing of their latest product line. The site chosen had proven very reliable in the past and seemed protected from the usual weather related disasters, which plagued their current facility. Additionally, ABC had a reciprocal agreement with another company located two miles away to provide contingency systems should their facility experience a disaster. In the course of two years, ABC had not needed to exercise this agreement.

Roberta, MIS Director for ABC, ensured a Business Resumption Plan for the company had been created and tested. Each test had been successful. Her team of very experienced System Administrators and DBAs verified the systems were fully recovered with the database being accessible during each test. The required recovery time had been effectively reduced after each test with the latest requiring only 24 hours of downtime.

UNFORTUNATELY, over the holidays at the end of 1998, an ice storm hit the area where ABC is located, leaving over 11,000 residents without power. The Help Desk paged the on-call System Administrator 15 minutes after the power went out. Stan, having just been promoted from the Operations Group, was familiar with the Business Resumption Plan but had not yet participated in a test as an administrator. He decided to call his mentor, the System Administrator who had a major part in documenting the BRP.

UNFORTUNATELY, he and his family were still out of town for the holidays. Using his phone list, Stan paged the on-call DBA. Janice responded very quickly and she and Stan agreed to meet at the office.

When they arrived at the office, Stan and Janice found the systems were still up and running. The UPS had done its job. Stan brought up his laptop to retrieve his copy of the BRP. The next step, according to the plan was to contact the neighboring company and request the use of their systems during the disaster.

UNFORTUNATELY, the power was out at the alternate facility as well. What was Stan to do? He knew ABC had recently installed a generator to ensure power was available for the facility. He checked his copy of the BRP. “Hummm, uh-oh, no reference to the generator”. Stan then signed onto the documentation server maintained for his group. He found a current copy of the BRP. “Whew, glad THAT system is still up and running. I better print a copy of the BRP”, but remembering the new escalation plan ABC had recently put in place, he decided to call the Help Desk and have Roberta paged instead.

UNFORTUNATELY, while he was talking with the Help Desk, the UPS shut down due to the batteries having been drained, killing power to the computer room. Due to no power source, the documentation server also failed. The generator failed to start. Stan did not know about the generator or who to contact. He knew the Facilities Manager or one of his people should be involved but he didn't know how to contact them. "Well, I AM talking with the Help Desk, they should know how to do that", Stan thought.

Stan was told Facilities had been contacted when the power failure began and the responding individual had said he would get to the plant as soon as possible.

UNFORTUNATELY, neither the Help Desk nor Stan knew about the major automobile accident, which involved the Facilities Management person.

"Janice has a copy", thought Stan.

UNFORTUNATELY, Janice only stored the database recovery and start-up information on her laptop. Stan started to feel major strains of panic. This situation is getting out of hand. "Why hasn't Roberta called back?"

UNFORTUNATELY, Roberta was out of town due to a family emergency and would not be back until the next day. Of course that is IF the airport is open. She will do her best to stay in touch by phone until she does get back in town. The Help Desk takes down this information on paper and then sends an analyst to pass it along to Stan.

By this time Stan has called all the System Administrators for the environment. Only one is at home and she will come in. Fortunately, Cathy is very experienced, but…

UNFORTUNATELY, she doesn't have an up to date copy of the BRP either. Her laptop had been upgraded and she had not finished restoring all of her files.

The above scenario could go on and on, but fortunately, I won't bore you with all the details. Notice how often the word UNFORTUNATELY has been used? Have you, as the System Administrator or MIS Director had to use this term during a similar disaster situation? If so, I would like to share some practical information with you that may help in this unfortunate situation.

Business Resumption planning is asking and answering "what if…?" questions. Once the questions stop, so will the on-going effectiveness of your Business Resumption Plan.

Planning

Ownership

To ensure success, there must be a clear owner responsible for Business Resumption planning for the environment. Without assigned ownership, processes will generally fall out of repair.

Responsibilities for this individual include:

- being aware of all changes to the infrastructure
- communicating and documenting those changes in the BRP
- scheduling and auditing all tests of the plan
- updating procedures and processes found to be at fault during testing
- maintaining the sense of urgency and focus required for successful planning in the environment

Assign ownership high enough in the organization to ensure adequate visibility within the company. In many cases Business Resumption is an add-on responsibility to a senior System Administrator that already has more on their plate than they can handle. This approach leaves the Business Resumption process as either an orphaned process or the person may not have the authority to completely handle the assignment.

Awareness

Each level in the organization has to be aware of the need for, and the continuity gained by diligent Business Resumption Planning.

Mount an awareness and education campaign that includes all levels in the organization. During the campaign, use examples of risk that are relevant to your business and geography. A little research during this step will go a long way at the Director's meeting.

Scenario-based risk analysis

An effective way to define your company's exposure is to perform a scenario-based risk analysis. A scenario can be a synopsis of events or conditions leading to an accidental loss. There are many parties involved in identifying these areas of possibility. Engineers and actuaries use their expert judgement and the parameters that you provide to accomplish this task. However, many organizations can perform this type of analysis on their own.

By using brainstorming sessions, your planning team can identify many risks the company may be exposed too. The more scenarios you can come up with, the more accurate your assessment of the risk factors. Additionally, each scenario should be constructed from the department all the way to the corporate level in the organization.

Ensure all scenarios are as accurate as is feasible. Make certain that all "unknowns" are documented and communicated. If not, the final outcome of the analysis can be skewed and decisions made from this data could be costly. Additionally, the credibility of the analysis will be questioned.

Another method for risk analysis is CRAMM. The Information Technology Infrastructure Library (ITIL) recommends the CCTA Risk Analysis and Management Methodology or CRAMM. As described by CRAMM, risk analysis involves:

- identification and valuation of assets (physical and data)
- identification and determination of the levels of threats (accident and deliberate)
- identification and determination of the levels of vulnerabilities

Using asset values, threat and vulnerability levels, you should calculate the levels of risk to the assets. Risk management is reducing the vulnerability of assets by understanding and applying different countermeasures, i.e., contingencies.

CRAMM is not a Business Impact Analysis. This methodology is concerned with the priority value of data assets, not the monetary or cost of downtime. From a qualitative point of view, CRAMM identifies and values, assesses the threats and vulnerabilities and the risk associated with the asset.

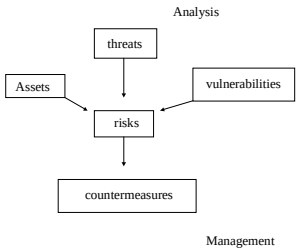

Figure 1 CRAMM

Risk analysis and management is more concerned with the physical and data assets of a company. An additional point of interest is the actual impact to the business should a disaster strike. How will the business processes continue? How long can the business be down? These questions and more are better answered using a Business Impact Analysis. A complete end-to-end view of the business processes must be maintained. In calculating the cost associated with creating the Business Resumption Plan, be sure to include a Business Impact Analysis.

Business Impact Analysis

A Business Impact Analysis will highlight areas such as:

- How does each component affect the end-to-end business process?
- How long will current inventories hold?

- How deep are your retained earnings and how long before they are depleted?
- What business processes depend solely on your information systems?

A BIA is not an inexpensive process. However, spending the correct amount on business resumption can offset this cost.

An additional outcome of a BIA will be the categorization of your data. Not all data is created equal. I recommend that your company divide your systems and data into three categories:

- business or mission critical (Tier I)
- business or mission sensitive (Tier II)
- non critical (Tier III)

Each data or systems category should have a restoration commitment reflected in the Service Level Agreement. For example, Tier I data and systems will be restored and operational within 6 hours. Restoration commitments should reflect what your IT infrastructure can actually meet. In many cases, IT departments will make a restoration commitment based solely on what the user community wants, not what the department is actually capable of doing.

Without proper categorization, all data becomes critical, resulting in a "fire fight" mode restore event, resulting in an over-all delay in business resumption.

By knowing what risks your company is exposed to, the impact to the business should a disaster occur, you are better equipped to gain management commitment to create and maintain an effective Business Resumption Plan.

Contingency Options

Contingency Planning is a key component in effective Business Resumption. This portion of the BRP deals with how your company's IT infrastructure will operate during and after a disaster. A contingency plan will have a cost associated with it alone. Let's look at concepts used in designing a contingency plan for your company.

The company in my introduction, ABC Company has daily sales revenue of $80,000.00. Their normal day-to-day expenses are $50,000.00.

	Disaster Exp.:	Under Normal	-8,000.00
	Activate BRP:	Conditions	
	Profits:		$22,000.00
Revenue:		$80,000.00	
Expenses:		-50,000.00	

Disaster w/o CP	Disaster w/ CP
$ 0.00	$80,000.00
-50,000.00	-50,000.00
- 8,000.00	- 8,000.00
	- 4,000.00
-58,000.00	$18,000.00

The simple table above demonstrates the effect to ABC Company's bottom line should a disaster occur.

The contingency planning portion of a Business Resumption Plan is not a popular subject to management due to cost. Why pay for something we may never use? When making a proposal to gain commitment from executive level management, you have to be prepared to deliver your message in a quick and powerful way. Use definitive information, such as your company's revenue and expense information coupled with calculated risk and vulnerability, and the positive effect of business continuity. This approach should succeed in gaining executive level commitment for Business Resumption Planning.

In theater, opening night is the most critical performance. This one performance can often make or break a show. Business Resumption is the same for most companies. The failure or success of your company will depend on how quickly and effectively you respond to disaster.

Any company WILL lose money in case of a disaster. With or without a contingency plan that works and including the cost associated with that plan. An effective contingency plan can provide continuity of incoming revenue, lessening the loss typically felt during a disaster. We must first look at the different contingency options available to most companies.

The different contingency options defined by ITIL are:

- do nothing
- clerical backup procedures
- reciprocal arrangement
- the "fortress" approach
- "cold" start fixed center (cold site)
- "cold" start portable center
- "hot" start- external (hot site)
- "hot" start – internal
- mobile hot start or "computer on a truck" (portable site)

Do nothing

The “do nothing” approach may be a legitimate choice for some companies. However, many questions have to be answered before choosing this option. For example:

- How will the business continue to operate?
- How long will our cash and other financial reserves last?
- Will our company permanently lose customers?

The “do nothing” option means exactly what it states, to do nothing except wait until the problem is resolved.

Clerical backup procedure

The clerical option is defined by going to a manual, paper-driven process. Think of it as going back to your company’s pre-computer time. In most cases this is not a feasible option. To staff and train a complete organization to perform the services your IT group and all of your IT equipment can perform is very expensive and prone to error.

Reciprocal agreement

This option is certainly viable but is less popular in today’s environment. If both companies are batch oriented and do not have a 24 hour 7 day a week service requirement, a reciprocal agreement approach can work. The agreement should be formally documented. Additionally, both companies change management processes have to communicate together to ensure long-term system compatibility.

Fortress approach

This approach is spending money on making the single site as disaster-proof as possible. In the fortress you will find redundancy for all systems, components, and the physical environment. This is a very costly approach, yet can succeed for the most part. However, it is very difficult to eliminate all risk of disaster. Additionally, data corruption is still a major risk for any approach.

Cold start – fixed center (cold site)

The cold start fixed center or cold site is an environment that is void of computer hardware. The environment will be equipped with the proper environmental controls, power requirements, and network connections. Generally, this is a service that is contracted for and only used for a specified period of time. One drawback to this arrangement is getting sufficient system hardware located and installed quickly. Many companies use this approach as an interim solution between the Hot-start external and return to their original or newly built site.

Cold start – portable center

Portability is the difference between this approach and the fixed center environment. The environment is built at a pre-arranged site for temporary use, situated close to the original location. The name, cold start implies the absence of equipment. As with the fixed center, equipment must be shipped in and installed.

Hot start – external

This approach provides an environment, including hardware suitable to meet your company's need for a specified period of time. A service provider often supplies this approach. The main advantage to this approach is the speed in which a business can be back in operation. The main disadvantage is the cost. Access to the facility can also be a concern. In some cases a hot start facility is provided on a "first come, first served" basis. Without a solid guarantee, your company may be left out in the cold.

Hot start – internal

Many companies today are utilizing their own hot start facility. In most cases, these facilities are either at the same site or may be a short distance away. Typically these sites are used for development or other types of activity under normal conditions and become a contingency site should a disaster occur. This approach, while effective has several drawbacks. Whatever is running on the "backup" environment may have to stop during a contingency, i.e., development. In many organizations development can be just as important as the production environment. Should the hot start internal be your company's choice, ensure adequate capacity and resources to continue both the primary and secondary functions during a disaster.

Mobile hot start

This option provides for a portable environment, complete with hardware to be shipped to your site. This approach has many advantages such as quick response. However, there are several disadvantages such as duplicating a very large environment.

The first steps of ownership, awareness, risk and business impact analysis and management, and deciding which contingency choice to use takes time to complete. Do not rush through these steps. An effective Business Resumption Plan will be the result. Through proper planning and determination, the goal of business continuity will be realized with great results to your company's bottom-line should a disaster occur.

Recovery

Recovery needs

Just like your favorite ice cream, disaster comes in many different flavors. Additionally, there are different types of recovery. For this paper I will concentrate on Operational and Full environment recovery.

Operational Recovery

In my position at Hewlett-Packard Company I have had the opportunity to see many different types of recovery plans. Many Business Resumption Plans only deal with the major geographical type disaster, i.e., what is going to happen if the entire facility is lost? While this is a necessary procedure, it only represents the worst case scenario most companies' face.

The term "Operational Recovery" deals more with the day-to-day type of disaster. While the problem may be confined to a particular system or environment, it still represents a disaster of sorts.

Data corruption is a disaster in many cases. Your business may or may not be able to operate until the corruption has been removed and the data recovered. Additionally, a user-error can be viewed in the same way.

Operational recovery deals with these and similar types of disasters. The procedures and processes required to quickly recover from an error such as this have to be properly documented and maintained. In most cases, the senior DBA or System Administrator deals with this type of problem. The recovery procedures are in their head. What if this person is not present during an event of this type? How long will it take to "re-invent the wheel"?

Operational Recovery procedures should exist for all day-to-day administration functions such as:

- recovering a file, fileset, or database
- retrieving backup tape sets from off-site storage facilities
- rebuilding a system from scratch should it be necessary

Operational recovery includes anything from single disk recovery to an entire system recovery and generally occurs on a more frequent basis than a large-scale disaster. Additionally, operational recovery is an excellent method to ensure the processes documented in the BRP are correct.

System and Database Recovery

I realize system and database recovery may appear very similar. However, we all know there are vast differences in the approach and time involved.

Speaking of time, I think this is a good point to start with. I have often encountered the idea that recovery or restore time for a database will be the same as the time it takes to back it up. This often is NOT the case. The only way to know how long a restore event will take is to actually perform the recovery!

In many environments terabyte-sized databases are not uncommon. There are many contributing factors as to why store and restore time may differ. Areas such as:

- hardware and software data compression
- file system structure is only rebuilt during a restore
- full and partial store events

If possible, always practice a full recovery of your database.

Database recovery can take many forms and requires much expertise. Therefore, the procedures to complete a partial or full recovery should be well documented and tested. Ensure the most in-experienced person on your staff can complete the procedures with minimal instruction.

System recovery requires different skill sets. In-depth knowledge of the configuration is required to efficiently recover the environment. In the UNIX environment this also includes:

- volume configuration data
- file system information
- network and kernel parameters

In many HA environments, the configuration of a system is very complex. Without current back-plane layout diagrams, detailed volume configuration information, etc., re-building a system can be almost impossible. The act of restoring the data becomes secondary if the system is not configured properly. As well, once restored, an incorrectly configured system can have a disastrous effect on the overall environment in areas such as capacity and performance.

Ensure your company maintains up-to-date procedures and configuration information to quickly recover from operational and full environment disasters.

The recommendation is to maintain up-to-date back-plane layouts, kernel parameters, and network and disc configuration in printed form. The documents should be updated anytime there is a configuration change. While difficult, discipline in this area will have a very high pay-off during recovery.

Documenting the Plan

The next step is to document your plan. It may surprise you how often this step remains incomplete. Like other documentation, the BRP is often the last item to be created or updated. Use the following information when documenting your plan.

ITIL recommends the following sections when documenting the BRP:

- Administration
  Information on how and when to invoke the plan the people, management involved where the emergency control center is located.

- IT Infrastructure
  The hardware, telecommunications, and software for the contingency systems or how to reorder if necessary along with contracts and agreements to support the recovery or reorder effort.

- IT Infrastructure Management & Operating Procedures
  Instructions for the operation of IT functions during a disaster, including SLA requirements and the possible lessening of service requirements, resulting from a disaster.

- Personnel
  The particulars regarding the people, logistics, etc. for the people required while in disaster mode.

- Security
  Fire and bomb instructions for the home site, and information about items in remote storage.

- Contingency Site
  All the information, i.e. location, people, facilities, security, etc. regarding the contingency site.

- Return to Normal
  How to return to the original, rebuilt, or new facility once recovery from the disaster is complete.

The more detailed each of the above sections are, the higher your success rate when activating your BRP.

All of the sections are important. However, I would like to point out some specific areas of concern with regard to personnel and returning to normal.

Personnel

As pointed out by one of my co-workers, emotions can run very high during a disaster. Often, the most simple of tasks become almost impossible to complete. The human factor during a disaster is generally not tested during rehearsals, leaving an unknown gap, which can easily wreck a BRP.

The following areas need special attention in your plan:

- logistical information for non-travel status employee
- funds, i.e., cash, credit cards to be used by employee's at the contingency site
- "personal" crisis resulting from a disaster

Ensure your BRP contains instructions and provisions for the non-travel status employee. During a crisis event, booking hotel, travel, and other arrangements can become difficult. Especially for persons who do not travel on a regular basis. The time spent working through this exercise can often delay recovery time.

Your BRP should include:

- travel agent contact information
- preferred airline, hotel, and rental car information
- step by step procedures for completing travel arrangements

During a disaster, especially a large-scale geographical event, removing funds from personal accounts may not be in the best interest of the employee. Rather than require this choice, provide a company credit card, included in the BRP package, to be used for all expenses during the event. A current list of valid signatures should be maintained at all times at the lending institution. Additionally, you might consider this account be monitored to ensure its use only in case of an emergency.

In the case of geographical disasters, personal homes and families will often take priority over the interest of the company. Consider personnel alternatives at the contingency site. As an example, many contingency sites can offer the expertise and personnel required to manage the infrastructure on a temporary basis.

Remember, during a crisis, emotions will run high. Inter-personal conflict is almost guaranteed. The simplest task becomes difficult to execute. By properly documenting the plan, rehearsing on a regular basis, and ensuring its applicability, the personal factor can be reduced.

Return to Normal

Another area that is often over-looked in many plans is the return to normal section. Returning to the original or a newly renovated site can be as stressful as the original disaster. Remember, your company has just experienced a disaster, requiring the IT Infrastructure be re-located to an alternate facility. When returning the environment

must be shut down again, data moved, and the systems brought back on-line. Doesn't this represent a disaster of sorts? The only difference being the knowledge as to when this disaster will occur.

The cost of new equipment, facilities, networking and other infrastructure related items should be documented in the plan. What if your company has to relocate as a result of the disaster? Has this scenario been planned for?

Your BRP rehearsals should always include the return event. If not, your plan will likely fail during a real crisis.

Maintenance and rehearsal

When should you revise your plan? I realize this may appear a simple question, yet, I have been asked this numerous times. Many Business Resumption Specialists recommend a yearly basis. I would suggest this as a minimum and recommend a more frequent schedule.

Most companies experience change throughout the year. Many of these changes will affect the plan. For example:

- organizational change
- change to the infrastructure
- Service Level Requirement change

The plan should, at a minimum, be reviewed as a result of one of the above changes. For instance, organizational change usually means new or different personnel involvement in the BRP. New persons need to understand the resumption plans and what their role is. Additionally, existing personnel will need to know how their roles may have changed. An organizational change is an excellent time to dust off, review, and update the plan.

Infrastructure change will generally have an immediate impact on the plan. For example, your company may have introduced clustering or redundant networking. While redundancy is an excellent High Availability practice, it does not take the place of an effective Business Resumption Plan.

Many organizations today are moving from a mainframe-centric to an open or distributed systems approach, with pieces of client/server applications dependent on numerous components in the IT infrastructure. This type of infrastructure change will have a dramatic effect on Business Resumption planning. I have seen numerous companies that have not updated their BRP after a change of this nature. How effective do you think their BRP will be should a disaster occur?

Like documentation, the BRP is often the last process to reflect change. Don't let this "gotcha" get you!

Rehearsal

Even though the following statement is not grammatically correct, I still like it, and feel it is appropriate in Business Resumption Planning. "Like theater, life ain't a dress rehearsal, it is "opening night" every day!" I have yet to hear of disaster announcing its presence in advance!

Without rehearsal, your plan is not complete. Worse yet, it will probably fail, resulting in even more damage to your company's bottom line. Business Resumption Plan rehearsals should be:

- frequent (at least once a year, I recommend twice)
- honest in their evaluation
- audited by someone other than the IT staff
- revised to improve noted problems
- involve inexperienced personnel when possible

Type and frequency of rehearsal

The popular choice for many companies is a yearly rehearsal. The experienced personnel plan for the test months in advance. They ensure the plan is printed off (if it exists), update the contact information, i.e., phone and pager numbers, and current backup tapes are retrieved. If the company has an agreement with a contingency site, (hot-start – external), travel arrangements are made using normal procedures, and off they go, to do the deed!

Once at the contingency site, the alternate systems are restored using the current backup tape set, the applications are brought up, maybe a few transactions are completed, and the rehearsal is noted a success. "Congratulations to everyone involved in our annual Disaster Recovery Test!"

As previously stated, how often have you heard of a disaster announcing its arrival months, weeks, or days in advance? During a major catastrophe, can your company rely on normal procedures for travel arrangements? What if the disaster is not the major geographical event planned for? Instead, it is data corruption on the primary database server? Is your BRP equipped to handle this type of operational recovery?

My recommendation is to rehearse your BRP on a semi-annual basis. One of the rehearsals should be the normal, publicized event. The second should be an unpublicized event to test the actual readiness of the plan and personnel involved in the recovery.

Using a risk scenario discovered during CRAMM, rehearse your plan. This rehearsal should not disrupt on-going business. Follow the following steps:

- Plan scenario
- Clear proposed date with contingency site
- Schedule auditors
- Notify executive level management with the actual date of the impending BR test
- Provide a possible time frame, i.e., a month to all other personnel
- Document scenario, including who will be involved, what each role will be, i.e., available, disabled, on vacation, etc. on note cards to distribute at beginning of test

On the date of the test:

- Present note cards to participants and begin test
- Audit entire process from notification to completion
- Honestly evaluate test
- Modify plan
- Hold post-mortem to ensure all persons involved know results, modifications to plan, and any changes to their roles

If your plan can not be located, activated, and successfully completed by the least experienced member of your staff, I suggest the plan will fail when called upon in a real disaster.

The experienced System Administrator and DBA know the special quirks of your environment. What if they aren't available during a recovery event? Your company can no more be guaranteed of their availability than it can be assured a disaster will never occur.

Your current Business Resumption Plan may not be ready for unpublicized rehearsals. This should not stop you from striving toward this goal. Additionally, include junior personnel whenever possible in all phases of business resumption planning to ensure competence during a disaster.

Key to Success

Maintenance is the key to successful business resumption. Be wary if anyone in your organization tells you the plan is complete. An effective BRP is never complete. Due to the ever-changing business climate and frequent operational disasters, this type of planning is as on going as a daily back-up process. Ensure you have a regular schedule established for updating and rehearsing your plan. Include business resumption in project management, change and problem management process, and SLA creation and reporting. Integration of Business Resumption with tactical and support processes is imperative to ensure success when disaster strikes.

Summary

The purpose of this paper is to highlight some of the processes, pitfalls, and other best practices to assist you in complete Business Resumption Planning. Of course it is not exhaustive, but contains much that I feel will help you to successfully plan, document, rehearse, and maintain an effective plan.