

Request for participation in the ISW-2002 workshop
Ronald M. LaPedis, CBCP, CISSP
Sr. Product Manager, Business Continuity, Security, I18N
Compaq Computer Corporation, NonStop Division
408-285-5987 (voice) 408-285-9570 (fax)
Ron LaPedis@compaq.com

Unfortunately I will be in Shanghai for the 2001 conference acting as a visiting scholar for security and business continuity issues. However, a paper is attached for consideration.

Business Continuity Planning Strategy Brief

Ensuring survival

With the shift to a 24 x 7 business model, companies require continuous availability

In the business world, computer disaster recovery planning is evolving toward business continuity planning. In recognition of this trend, in 1995, DRI International, an organization founded in 1988 to provide a base of common knowledge in continuity planning, replaced the designation for Certified Disaster Recovery Planner (CDRP) with Certified Business Continuity Planner (CBCP).

What is the difference between disaster recovery and continuity planning? In theory, a disaster recovery plan is reactive and usually focuses on the computing environment. Although work is done to harden the computing infrastructure to prevent a disaster, the plan's main purpose is to recover from damage to the infrastructure. In contrast, a business continuity or contingency plan is not only proactive, but it is also targeted at keeping the *business* running, not just recovering the computers.

Continuity planning should not be limited solely to the computing infrastructure. Each company also needs to review continuity or recovery of manufacturing, packaging, warehousing, shipping, customer support, and any other facilities or operations that are critical to the company's survival.

Many companies today do not have a working continuity plan. Of those companies that do develop a plan, many proceed without sufficient knowledge or input from end users. Because end users are not involved in developing the continuity plan, their manual procedures,

physical facilities, hard-copy records, and other special needs are often overlooked. Thus hardware and applications are being recovered, but not the business processes that use them.

In a business continuity planning program, individual business functions identify their critical business processes and develop separate (but coordinated) continuity plans for each of them. The benefits of this distributed approach are many:

- > Business processes that are not critical do not hinder those that are, so limited resources can be used effectively.
- > Infrastructure that supports noncritical business processes does not get recovered.
- > Multiple critical business processes or applications can be recovered in parallel.
- > Applications that normally run on different systems can be recovered on the same system, if necessary.

The survival of your business after a disaster depends on having a continuity plan in place. This brief is intended to help you develop and deploy one.

Directed at a hypothetical employee, a corporate continuity planner, it details the procedures for launching a continuity planning program.

Contents

1	Beginning the continuity planning process	11	Tips for successful continuity planning
1	Where do I start?	11	Contact an amateur (ham) radio organization
2	Risk assessment and business impact analysis	11	Assess application availability requirements
3	Recovery time and recovery point objectives	11	Refine your backup/restore process
4	Disaster tolerance: Closing the freshness window	12	Enhance your plan with everyday procedures
5	Alternative plans and controls	12	Work with local authorities
6	Documentation and standards	13	Conclusion
6	Required documentation	13	For further information
7	Developing standards: A “cookbook”	14	Appendix A: Compaq Remote Database Facility software
9	Writing the continuity plan	15	Appendix B: Compaq Reliable Transaction Router software
9	Corporate continuity planner responsibilities	16	Appendix C: Compaq StorageWorks Data Replication Manager software
10	Exercising the plan		
10	Pitfalls of a continuity planning program	18	Appendix D: Compaq Disaster Tolerant Cluster Services

Beginning the continuity planning process

Developing a corporate continuity plan involves a number of steps as well as some basic concepts.

Where do I start?

Suppose you are beginning a corporate continuity planning process for the Absolutely Best Company (ABC), a manufacturer of top-quality widgets (an imaginary company and product). There are several steps involved, as detailed in the following paragraphs.

Obtain management commitment

For the continuity plan to be successful, management must be committed at the highest level. The plan must be part of the strategic business plan, and the company must budget appropriately and separately for the continuity planning program. A top-level policy statement should be issued that

- > Affirms the value of business continuity
- > Acknowledges and accepts the associated costs
- > Documents management responsibilities
- > Includes the goals and expectations of the plan, as well as any organizational assumptions or parameters

Identify critical business functions

Assuming that you have management support, the next step is to identify how the company obtains its revenue in terms of business functions. For example, ABC first takes orders for widgets and then builds the widgets to meet those orders. Next, the widgets are installed, and the customers are billed. Finally, the employees are paid so that the process will continue. Other revenue comes from service and support, but because those are distributed functions, an event that has an impact on the corporate site should not affect them adversely.

There also are numerous ancillary business functions within ABC, such as ordering parts from suppliers and paying them. Because parts are usually ordered months in advance and payables probably could be postponed until normal processing resumes, these business functions are usually not a critical concern. Note that a just-in-time supply chain would require substantially more complicated planning, which is beyond the scope of this paper. Compaq Global Services consultants can assist you with this planning.

Once you have defined the gross critical business functions (not the infrastructure, such as computer applications, that supports them), a risk assessment and a business impact analysis should be performed for each of the business functions and then, if appropriate, for the infrastructure supporting them. Remember to analyze dependencies because a business function that appears noncritical could be supporting one that is critical.

This information should be communicated to the responsible senior managers so that they can confirm, and then rank, the criticality of each business function. The executive staff or office of the CEO should have final approval of the list because those individuals are in a better position to understand the company in its entirety.

After you have determined what the critical business functions are, it is time to contact the people who will write the plan to ensure the function continues or is recovered. Following a distributed planning methodology, you will not actually write any continuity plans—you will be acting as a consultant and a facilitator. The daily users know best the tasks involved in the business functions.

Build business process core teams

You start by building business process core teams consisting of information technology (IT) operations management, end-user management, applications support staff for each critical business function, and the records management department. This team technique is called the *Delphi method*, and hence the team is called the Delphi team.

Through the Delphi teams, you develop a clearer view of the infrastructure (for example, processes, records, IT applications) the teams believe is critical to performing their business functions.

Build a corporate team

You should also build a corporate team, consisting of members from the accounting, auditing, information technology, facilities, human resources, legal, public relations, investor relations, purchasing, postal services, records management, risk management, safety, security, shipping/receiving, and telecommunications departments. In a disaster, not only will these departments be required to continue their support roles, but also they may have to implement major infrastructure changes to support the affected areas. The legal, public relations, and investor relations departments need to keep the public and stockholders informed of the company's operational status after an event has occurred.

Risk assessment and business impact analysis

The purpose of a risk assessment and a business impact analysis is to answer the following questions:

- > What am I trying to protect? (system inventory and definition)
- > What am I trying to protect them from? (vulnerability and threat assessment)
- > What controls are currently in place or needed to prevent or minimize the effects of potential loss? (evaluation of controls)
- > How much am I willing to spend on those controls? (decision)
- > Is the money I am spending effective? (communication and monitoring)

The continuity planner (or planning coordinator) helps each Delphi team answer these questions as depicted in figure 1.

The risk assessment involves identifying threats, vulnerabilities, risks, and the business impact of a disruption for each entity. *Threats* are events that could disrupt an entity. Some examples are natural disasters (wildfire, flood, earthquake), man-made disasters (burst pipe, fire from an electrical short), disgruntled employees, and mistakes. *Vulnerability* is the susceptibility to the threat (chances that an entity can be affected by a threat). For example, the closer a building is to an earthquake fault, the more vulnerable it is to an earthquake. The *business impact* from these risks can be loss of revenue, customers defecting to the competition, damaged reputation, or disgruntled employees if the company cannot pay them.

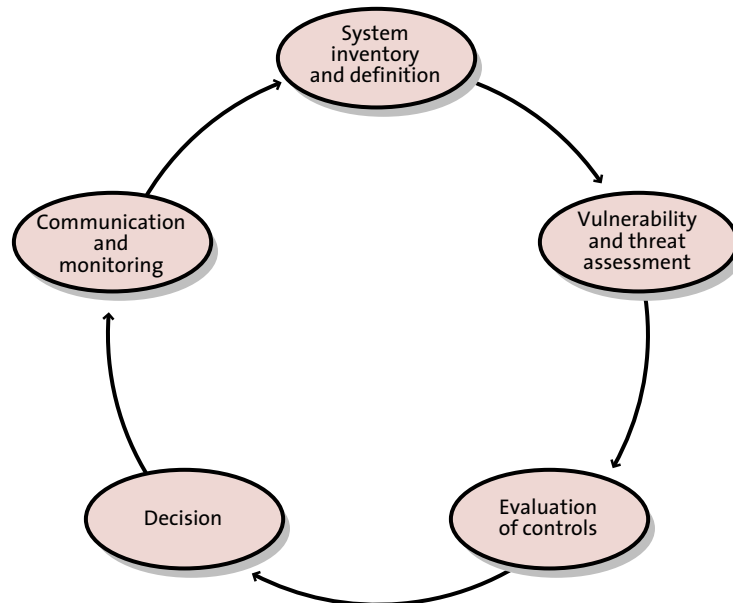


Figure 1. Disaster risk assessment.

A risk assessment can show that an entity thought to be critical is not or vice versa. It is pointless to perform a formal risk analysis if the informal analysis shows that there is little vulnerability to the risk (for example, a snowstorm in New Delhi or a typhoon in London).

Before you begin the ranking process, determine what criteria to use. Generally, they are split between quantitative and qualitative. Quantitative losses can be expressed as a number, such as an annualized loss exposure (ALE). Calculating an ALE is outside the scope of this paper, but it is a standard part of any insurance company's activities. Compaq Global Services can assist with ranking risks, or you can use any of several well-defined methodologies (see the "Conclusion" section).

At this time, ABC is interested in

- > *Monetary exposure:* Would it cost ABC money if the function could not be performed?
- > *Customer exposure:* Could ABC lose market share if the function were suspended?
- > *Legal and regulatory exposure:* Is ABC required to perform the function?
- > *Intracompany dependencies:* Would suspension of the function affect the critical activities of another area?

To start the risk assessment, rank all of the entities whose loss could negatively affect ABC's business, gain consensus from each Delphi team, and then merge the results for presentation to and concurrence by upper management. Note that some threats have a time component as well. For example, a power failure that lasts a few minutes may not be a disaster, but one that lasts hours could well be.

Recovery time and recovery point objectives

As part of the risk assessment, the Delphi teams estimate how long an entity can be unavailable, how old the information supplied by the entity can be, and how much of it can reasonably be lost when it is made available again. That is, they determine the recovery time objective (RTO) and recovery point objective (RPO).

Recovery time objective refers to the time from when the event occurs until the business process (for example, the accounting department, the accounting application, or manual procedures used by accounting) must become active again (recovered). This can also be called the *recovery window*.

Recovery point objective describes the point in time to which the data must be recovered—stale (old or obsolete) information no longer

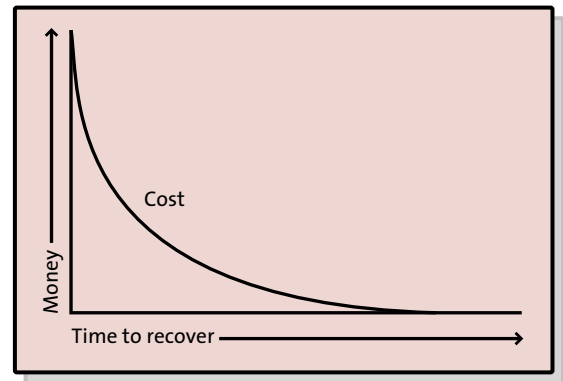


Figure 2. Cost of recovery.

reflects the state of the company. This can also be thought of as the *freshness window*. The teams consult with management to confirm their decisions.

The longer the RTO for a particular entity, the less the cost will probably be to recover it (figure 2). Unfortunately, at the same time, the losses from the entity that is unavailable are escalating (figure 3).

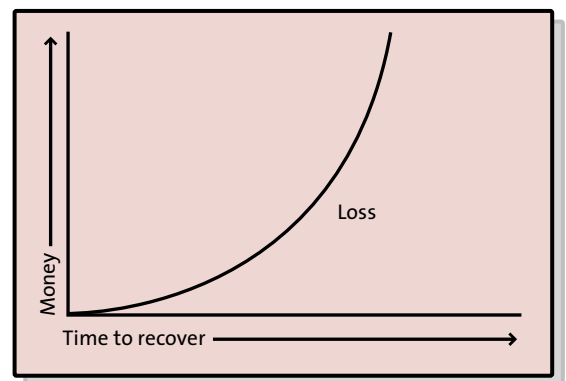


Figure 3. Loss due to the time an entity is unavailable.

RTO and RPO are not necessarily linked to each other; that is, a short RTO does not imply a short RPO. For example, a database might need to be recreated from backup tapes in less than a day (RTO), but while the online

data must be current, it is acceptable for the batch data to be one week old (RPO). Consider what the difference would be if the database could be recreated in two hours, or if the batch data were only one day old.

The hardware, software, and backup/restore methodology supporting the recovery need to be carefully evaluated and addressed. For example, if your RTO is a couple of hours, do you have enough tape drives to load the data in that time, or do you need to recover using a different method? Some companies have spent hundreds of hours practicing and refining how their databases are backed up to decrease recovery time.

RTO varies greatly, depending on the application. For example, if an online company's website is not available in a period of time measured in seconds or minutes, customers will simply click to another site. On the other hand, it may be acceptable for the company's warehouse application to stay down for as long as a week or more because the functionality can be replaced by manual methods.

By overlaying the curves in figures 2 and 3, you can see that there is a point at which the potential loss equals the cost of recovery (see figure 4). This represents the starting point of the maximum cost of the business continuity plan for each entity. With this viewpoint, you can determine how long the function will be

allowed to be unavailable and how much to spend on your plan. Note that this is only a starting point—remember to include qualitative losses as well.

Looking at RPO again, assume that a bank has recovered its automated teller application but that the backup tapes are two days old. Even though the automated tellers are running, customers may still defect to the competition because the data is stale. ATMs maintain audit logs so that lost data can be reconciled—eventually, but that may occur too late to retain customer loyalty.

In contrast, if a week's worth of payables is lost, the next billing cycle from each vendor will allow you to recreate the correct payables state. The worst that might happen is that an interest penalty could be incurred for missing a payment.

Disaster tolerance: Closing the freshness window

Real-time technologies, such as online data replication or vaulting, can practically close the freshness window (see figure 5). They are more expensive than routine backups but could be deemed necessary in some situations, such as Web transactions, wire transfers, and supply chain applications. Replication or vaulting duplicates data onto an off-site location as it is manipulated on the primary system. The semantic difference between these two terms usually is that vaulted

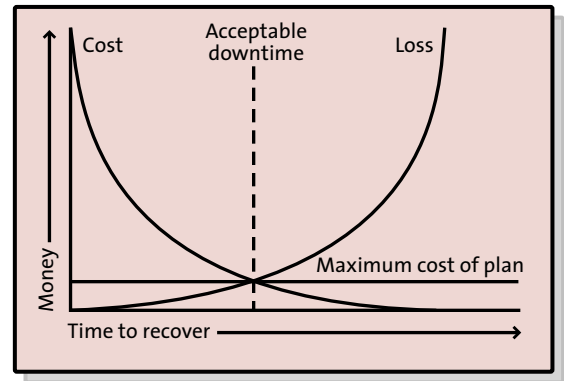


Figure 4. Maximum justifiable cost of plan.

data is batched and/or stored offline and needs to be moved to the backup hardware, while replicated data is sent in near real time, possibly directly to the backup hardware, and is ready to run.

If your company is already geographically dispersed and application uptime is imperative, you can create *application domains* at more than one site and distribute the load. With load balancing routers, redundant communication lines, or other methods, transactions can be split between multiple servers running in multiple sites.

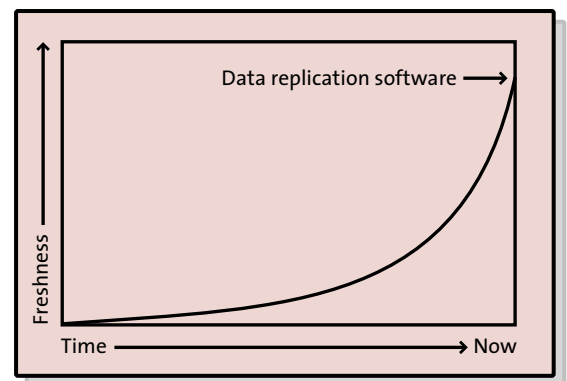


Figure 5. The freshness window.

When the load is being shared in this manner, you do not actually have primary and secondary systems or sites. What you do have are the beginnings of indestructible, scalable computing. New servers can be added at any time, and applications and database files can be migrated between the servers and sites as needed, so that any server or any site can be taken offline for testing, maintenance, or upgrades. In a properly designed application domain, a failure is undetectable, except perhaps for application slowdown.

An overview of Compaq's disaster-tolerant and data replication products appears in the appendixes. Compaq has several partners that provide data replication products as well.

Alternative plans and controls

Once risks are assessed and recovery windows are determined, the planner can ask the Delphi teams to begin outlining possible continuity plans for their business functions, starting with the most critical. The baseline is the *before* risk or ALE (no plan or controls in place). For each alternative plan or control, the Delphi teams need to calculate the *after* risk or ALE (plan and controls in place) along with the cost of the plan and controls.

The plan execution time is important. If the entity can be unavailable for only a few hours, but the execution time is two days, reevaluate either the acceptable recovery time objective or the plan itself.

Because computer resources can be at a premium in a disaster, replacing computer-based processes with manual processes is an option that should be explored. Besides computing costs, the planner should also address such matters as alternative sites, temporary personnel, hotel and meal costs, off-site records and forms storage, and installation of new phone lines. The purpose of this step is to calculate the cost/benefit ratio of plans and controls for different recovery objectives.

At some point, the potential loss reduction (savings) will be less than the expenditures required to develop and implement the continuity plan (see figure 6). Here is where the executive staff comes into play again. They need to determine which controls and recovery window each plan should address based on cost versus savings and time to deploy. Remember that some risks, such as loss of customers or reputation, can cause unforeseeable losses in the future. Possibly a continuity plan that costs more than the expected loss should still be implemented, based on potential loss of future revenue and corporate image.

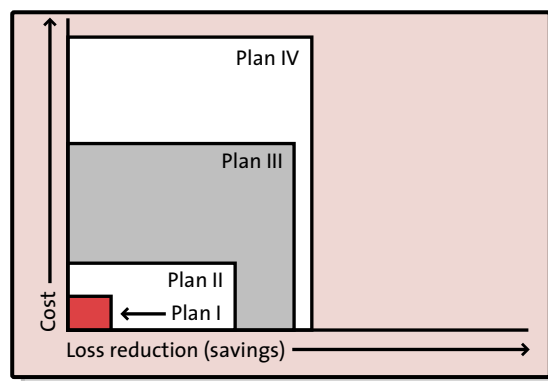


Figure 6. Plans I and III would break even (at different levels). Plan II would generate savings in excess of its implementation cost, and Plan IV would cost more than it would save.

When an actual crisis occurs, a crisis response team—composed of executive staff members and guided by one or more emergency response teams consisting of Delphi team members—determines if a disaster should be declared. The team considers the estimated time the affected entity will be unavailable, the recovery window, and the time it will take to execute the plan. If, for example, the recovery window is two days and the entity will be unavailable for only one day, it may not make sense to declare a disaster.

Declaration of a disaster needs to be reevaluated if the entity is down longer than initially expected, based on the time remaining before the entity can be made available again and the time required to execute the continuity plan.

Documentation and standards

As a continuity planner, you assess current documentation.

Required documentation

Before developing a continuity plan identifying activities to be performed during a disaster scenario, you need to understand how those same activities work every day. This means that you need access to some basic documentation for each business process. Determine if the following exist:

- > Change control process
- > Standard operating procedures (SOPs) for end users
- > Run books
- > Special forms requirements and special peripheral requirements for the operations staff
- > Data flow diagrams and problem isolation procedures (for the business functions as well as the computer applications)
- > Tape backup/rotation schedule for records management

You also need to gather more specific information about your company's business functions. For example, find out if sufficient application downtime is scheduled to

back up the databases used by the business functions, or, if the software allows it, if the databases are being backed up online. (If your company runs 24 x 7, you don't have time to take your system down for backups.) Determine if there is an archival process to remove inactive records from hard-copy files and databases so that they are kept at a manageable size. Also, identify where critical records are being stored: on site, off site, or out of the regional area.

If any of this information is missing, a continuity plan can be started, but it may not be effective. Without knowing how the business functions run and what is required for normal processing, no one can guess the requirements for exception processing. Actually, the bulk of the work of developing a continuity plan lies in ensuring that standard business practices are documented and followed.

For a plan to be effective, you also need a commitment to gather or create the necessary documents and to begin a consistent backup program, if one does not exist. If you encounter opposition by pointing out that commitments are lacking, you can call in a consultant to identify the deficiencies so that you retain cooperation for developing a plan. You can also

point out that by having these documents and processes in place the company will be more competitive in the long run due to

- > Faster isolation of application bugs
- > Fewer operational mistakes
- > Reduced support requirements
- > Faster training of new staff
- > Easier maintenance and enhancement
- > Fulfillment of industry and legal regulations
- > Easier auditing

The Delphi teams must be especially aware of any non-IT-related infrastructure required to keep each of their functions running, for example, if they need special paper, printers, or inks. Some questions to be answered include those relating to the storage and accessibility of important phone numbers, PC hard drives, and removable media.

The continuity planner develops a standard set of forms and procedures to be used by each function: a continuity plan “cookbook.”

Developing standards: A “cookbook”

The continuity planner either develops or purchases a standard set of forms and procedures to be used by each function: a continuity plan “cookbook.” Without standards, each business function’s plan will look different, making coordination difficult.

Different practitioners divide and name the phases of the continuity planning program differently. The Disaster Recovery Institute defines seven phases of a continuity planning program as follows:

- > Phase 1: Project initiation
- > Phase 2: Functional requirements
- > Phase 3: Design and development
- > Phase 4: Implementation
- > Phase 5: Testing and exercise
- > Phase 6: Maintenance and update
- > Phase 7: Execution

Your cookbook should be developed or software selected during phase 3 to be used by the business function teams during phase 4. At a minimum, it should contain the following:

- > Step-by-step approach for each group to follow in writing the continuity plan
- > Corporate team description, stating which corporate resources will be available to assist each business function in developing its plan
- > Notification process
- > Plan considerations
- > Responsibility list

As discussed previously, the corporate team performs the centralized tasks common to all business functions. By building the corporate team, you eliminate duplication of effort among the business functions while the plans are being written, as well as ease resource contention during an actual disaster. The corporate team should consist of a primary and secondary contact from each department involved.

The corporate team maintains an overall list of resources required for each business function’s plan and resolves conflicts. Resource requirements are submitted via *corporate support forms*. Corporate support forms provide a standard way to list the resources that will be required of the corporate team members should a disaster occur. Each sheet is forwarded to the appropriate corporate team member, who then coordinates the requirements necessary for all business functions. If you have chosen a PC-based disaster recovery package, the forms can and should be modified to fit the format of the software. It is important that you find software that fits your planning program, rather than attempting to fit your planning program to some arbitrary product.

Although the planner maintains the first-level response part of the plan, including lists of important phone numbers, at the corporate level, the security department probably should start the actual notification process in the event of a disaster.

The plan considerations section identifies the issues that must be addressed by business functions as they write their plans. This section consists of details that might be overlooked by people who have not previously written a continuity plan.

A responsibility list is a script or checklist, by job function (not by name, since you don't know who will be available in a disaster situation), of what each person will be required to do during the seven phases of plan execution:

- > *Evaluation and declaration:* Using information about the situation as well as the criteria for declaring a disaster, determine if a disaster should be declared and what parts of the plan to deploy.
- > *Notification:* Deploy the notification process detailed in the plan.

- > *Emergency response:* Deploy the parts of the plan that activate your hot site, relocate people and equipment, pull supplies from storage, hire temporary personnel, notify the media, stop trading in your stock, and so forth.

- > *Interim processing:* Continue running your business as effectively as possible.

- > *Salvage:* The damage assessment team works to salvage as much as possible from your primary site after pictures are taken and insurance issues are handled. Remember that equipment, microfilm, paper, and magnetic media degrade rapidly if not properly removed, stored, and recovered. This team also estimates the cost and time required to restore the primary site. It may be decided that restoring the site is not feasible, so the company should relocate to another primary facility.

- > *Relocation/reentry:* Your company needs to move out of the emergency site to its previous facility or to new facilities. Enter any manually generated information into your automated systems.

- > *Resumption of normal processing:* At the end of plan execution, your company's business functions return to normal. Remember to debrief everyone involved in plan execution and update and test the plan as necessary.

It is much easier to divide and assign the tasks necessary for recovery while the plan is being written, rather than in the middle of a disaster. The cookbook should contain sample responsibility lists and layout hints. Note that tasks should be assigned by teams or by job titles and not to individuals.

Writing the continuity plan

Finally, you are ready to facilitate the development of a written continuity plan.

If employees within each business function write the plan for that function, you achieve multiple goals:

- > Employees know what the day-to-day activities are.
- > Numerous functions can be generating plans at the same time.
- > You gain buy-in of the business function employees.

You or your staff should be available to answer questions as each group writes its continuity plan. Not only does each business function need to generate a plan, but also each department represented on the corporate team needs to have a plan, in case those departments are also affected by the disaster.

Although the plan can be written online, it must also be stored on paper to help ensure accessibility. Some continuity planning software vendors sell Web-based services that make your plan available from any PC. The drawback to these services, however, is that if you do not have access to a PC, or the disaster also makes the vendor's site inaccessible, you may not be able to access the plan.

Corporate continuity planner responsibilities

As the corporate continuity planner, you supply each business function's continuity planner and each corporate team member with a continuity plan binder containing plan dividers and a basic phone list. The phone list contains the direct phone numbers for police, fire, ambulance, hospital, toxic spill, FBI, and utilities. The binders given to the corporate team members also contain the office, home, car, and pager phone numbers for each corporate team member, backup, and manager. These binders are used for storing each business function's continuity plans after you and the corporate auditors have approved the plans.

Each executive staff member is given a small packet for his or her briefcase, containing an emergency phone list, an executive staff phone list, and a plan execution "quick start" document.

Corporate team members keep a copy of the binder, with their own continuity plan and the requirements sheets from each business function appended, at home and in their offices. The various business functions select a primary and backup contact to care for their own plans, which should also be stored at home, locally, and if applicable, at the backup site.

The corporate continuity planner has copies of each corporate team member's and business function's continuity plan. As keeper of the entire corporation's continuity plan, you ensure that these copies can be retrieved in case all other copies of a particular continuity plan are destroyed. Copies should be maintained on site in data safes and at the company's off-site data storage vaults.

Exercising the plan

Continuity plans should not be tested—they should be *exercised*. Tests are passed or failed, whereas exercises are conducted for practice. Exercise the plans thoroughly to ensure that they work. During the exercise, note any problems that occur and encourage feedback from participants. The purpose of the exercises is to reveal any defective or missing components in the plans. It is counterproductive to reprimand someone for pointing out errors or omissions. Some companies spend hundreds of hours testing and refining specific parts of their plans until they are satisfied with the time or accuracy of execution.

It is best to exercise and update the plans at least annually, or when major changes occur. Update call lists quarterly. It is better to have no plan at all than to have an out-of-date plan—such a plan lends a false sense of security and wastes time during an actual disaster.

Pitfalls of a continuity planning program

The primary pitfall of a continuity planning program is that often its expenditures are charged directly against profits and appear to provide no immediate benefit. Other pitfalls include

- > The program is viewed as negative or depressing.
- > Continuity planners usually work with employees who lack awareness of the problem.
- > Employees often are expected to work on the plan in addition to their other tasks, possibly overburdening them.
- > Many companies do not have adequate documentation of their daily activities or information flows to begin plan development, so those must be developed first.

Tips for successful continuity planning

Here are some practical tips.

Contact an amateur (ham) radio organization

If your company has an amateur radio club, that is a great start to help with your recovery efforts. Contact the American Radio Relay League (www.arrl.org) to locate a local group if you are in the United States, or your national ham radio association if you are in another country. While you use your security radios to recover the business, amateur radio volunteers can be called on to assist with human safety issues. Their license restricts the use of ham radio to life safety and non-business-related communications. They cannot have forms delivered but can handle almost anything relating to people, including location, medical needs, and safety. Regional authorities can curtail the use of cellular phones and some or all business radio bands as well as commandeer phone and radio equipment during an emergency.

Assess application availability requirements

Five nines or 99.999 percent uptime is usually calculated based on unplanned downtime. This number isn't always relevant, especially since scheduled maintenance is usually excluded from the measurements. According to *Interactive Week*, 30 percent of all application downtime

is attributable to scheduled maintenance. Some vendors advertise 99.999 percent hardware uptime, but this does not necessarily mean *application* uptime. If your application is down, so is your company.

If the risk analysis shows that your computer application cannot be down even for routine maintenance, you need to select systems that allow for online upgrade and maintenance, for example, to add processors or disks, introduce new application code, and reorganize database files. Compaq *NonStop™ Himalaya™* servers provide that continuous availability.

Refine your backup/restore process

As noted previously, many companies spend hundreds of hours refining their backup and restoration procedures. Some methods of decreasing your recovery time are as follows:

- > Pull and ship files from your off-site storage in “waves” so that the most critical files arrive sooner. While the next set of tapes is being pulled, the first set can be on its way to the recovery site. If you have duplicate tapes, ship them separately so that a transportation mishap doesn't derail your recovery.
- > Determine how many tape drives are required at the backup site to meet your RTO. One company uses 64 drives in parallel.
- > Tape is inexpensive. Filling tapes to save money could prevent you from recovering in the allotted time because multiple restore threads need the same tape. One company cut their file restoration time by 50 percent by optimizing tape use.
- > If at all possible, automate your recovery tasks so that mistakes are minimized. One company has 800 batch jobs that restore the application and database from tape, roll the database forward with the logs, and check consistency.
- > Separate and back up files in the order that they need to be restored. One such partitioning could be operating system, application, database files, and transaction logs.

Enhance your plan with everyday procedures

Ensure that your change control process has links to your continuity plan. If processes, procedures, or infrastructure change, the plan may need to be altered.

Instead of storing special forms or other supplies in a warehouse or ordering them “just in time,” rotate them from the vendor to your backup site or off-site storage and then to production. In this way, your supplies are always fresh, and if you declare a disaster, they are on hand. When on-site gear becomes obsolete, rotate it to the backup site or off-site storage for use during recovery.

Work with local authorities

It is helpful to contact other companies and regional civil disaster management authorities during development of your plan. Schedule facility walkthroughs with local police, fire, and toxic spill personnel so that they become familiar with your facility *before* you need to call on them in a disaster situation. They need to know where your computer rooms, data closets, flammable or toxic chemicals, and power supplies are located.

By working with local authorities before a disaster, not only can you gain insight and expertise, you can also find out if elements of your plan conflict with those of other companies or with rules in effect during a regional disaster declaration.

When it is time to exercise the continuity plan, consider inviting the authorities to participate. That will ensure a more realistic exercise, and you can find out if there are any coordination issues while there is still time to make corrections.

Conclusion

A continuity plan should not and cannot be written by the IT department alone, nor should it be written solely for a given computer or data center. Developing such a plan is a long-term process that requires substantial human and monetary resources throughout the company. Without a long-term commitment to continuity planning from the highest executive levels, efforts to develop such a plan are bound to fail.

The planning process cannot even begin without documentation for everyday processing already in place, including change control procedures, standard operating procedures, run books, data flow diagrams, problem isolation procedures, and a tape backup or rotation schedule. As a by-product, continuity planning forces more formalized standard documentation across the entire company, resulting in faster isolation of application bugs, fewer operational mistakes, reduced support requirements, faster training of new personnel, and easier maintenance and enhancement of current applications.

Not only is a continuity plan required by many regulatory agencies, it could also mean the survival of your company.

For further information

DRI International (DRII) was founded in 1988 to provide a base of common knowledge in continuity planning, a rapidly growing industry. DRII also administers the industry's only global certification program for qualified business continuity or disaster recovery planners. The organization's Professional Practices for Business Continuity Planners, a common base of knowledge, serves as the industry's best practices standard. Refer to the website at www.dr.org.

The *Disaster Recovery Journal* was the first publication dedicated to the field of disaster recovery and business continuity and now has over 50,000 subscribers. The *Disaster Recovery Journal* also sponsors two annual conferences, one on each coast of the United States. More than 2,500 continuity planning professionals from all over the world attend these two conferences combined, making them the largest in the entire industry. The journal's website is www.drj.com.

Some helpful books on continuity planning are

- > *Designing Controls into Computerized Systems*. Fitzgerald, Jerry, and Fitzgerald, Ardra F., Jerry Fitzgerald and Associates, ISBN 0-932410-40-5 (out of print)
- > *Disaster Recovery Planning*. Toigo, Jon William. 1999, Prentice-Hall, ISBN 0-13-084506-X
- > *Data Replication—Tools and Techniques for Managing Distributed Information*. Buretta, Marie. 1997, John Wiley & Sons, ISBN 0-471-15754-6

For more information from Compaq on continuity planning, contact Ron LaPedis at ron.lapedis@compaq.com.

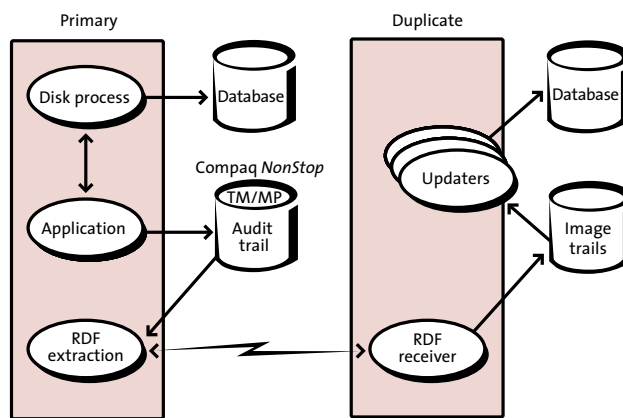
Appendix A: Compaq Remote Database Facility software

For more than a decade, major companies relying on the world's most fault-tolerant computing platform, Compaq *NonStop Himalaya* servers, have also turned to Remote Database Facility (RDF) software to replicate critical data and ensure uninterrupted service in the face of natural disasters. Recently, with the addition of two new versions, the RDF product family has been extended to provide increased throughput, faster takeover, and even more flexibility when implementing a business continuity plan in real time.

RDF software enables you to maintain multiple "live" copies of your critical databases on designated backup systems. Regardless of whether a backup database is located across town or on the other side of the world, changes to your primary database are mirrored at your backup sites in a fraction of a second. As a result, should your primary database become inaccessible for any reason, you can quickly pick up processing at a backup site with minimal service disruption or data loss.

With RDF software, you can implement a wide variety of backup configurations—including multiple backup systems for each primary system, or a single backup for multiple primary systems (see figure). You can also enhance the overall performance of your applications by employing backup systems for query and batch activities until the exact moment they are needed to support a recovery operation.

In the face of power failures, fires, floods, earthquakes, and other disasters, RDF software puts you in full control of your business-critical resources. With dot-com downtime measured in millions of dollars per hour, no company can afford to be without the kind of protection that RDF software provides.



Remote Database Facility software enables high-performance, real-time updates to duplicate sites.

Appendix B: Compaq Reliable Transaction Router software

In addition to a wide variety of clustered continuous computing solutions, Compaq offers the industry's most robust solution for ensuring transactional integrity across wide-area, heterogeneous environments.

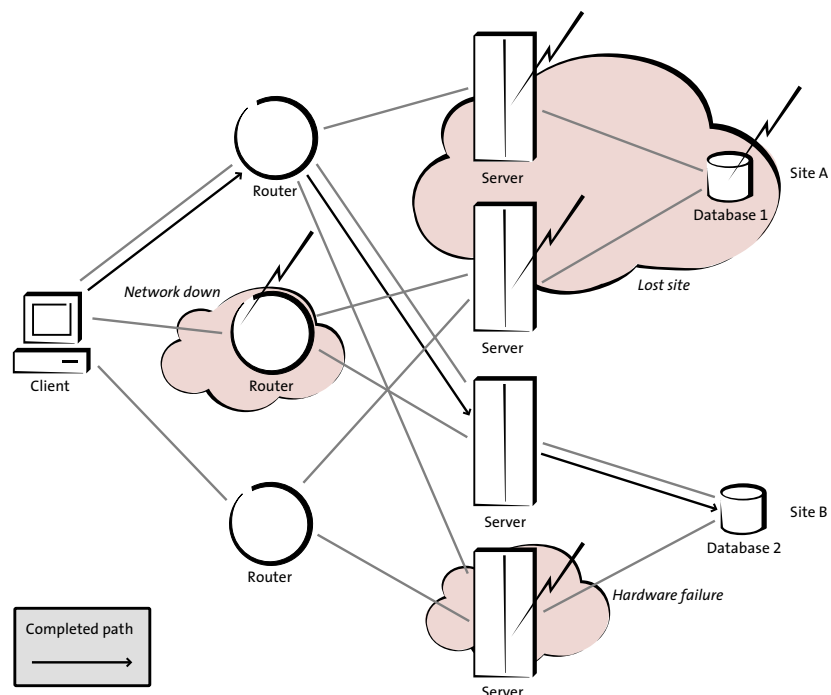
Reliable Transaction Router (RTR) software supports widely distributed client/server applications that require continuous processing, ensuring the ability to execute transactions dependably, in real time, without interruption of service. By replicating transactions and processing them on redundant systems located up to thousands of kilometers apart, RTR software extends disaster tolerance across multivendor client/server environments and delivers continuous, reliable transaction processing across global networks.

RTR software uses a combination of buffering, journaling, and monitoring techniques to insulate applications from software, network, and site failures and to maintain information on transactions in process. If a failure occurs,

RTR software provides automatic and transparent failover, including router failover. RTR software supports two-phase commit, transactional message integrity across distributed systems, and broadcast messaging, such as informational messages from servers to subscribing clients.

Applications using RTR software can operate in heterogeneous environments. For example, one system can be from IBM, another can be from Hewlett-Packard, and a third can be a Compaq *AlphaServer*™ system running the *OpenVMS*™ operating system. RTR is supported

on Windows 95, 98, 2000, Me, and Windows NT systems; the *AlphaServer* system running the *Tru64*™ UNIX and *OpenVMS* operating systems; and Sun Solaris, IBM AIX, HP-UX, and SCO UNIX systems. RTR software has a simple application program interface (API), with built-in semantics for transaction and data integrity, that simplifies application development and maintenance.



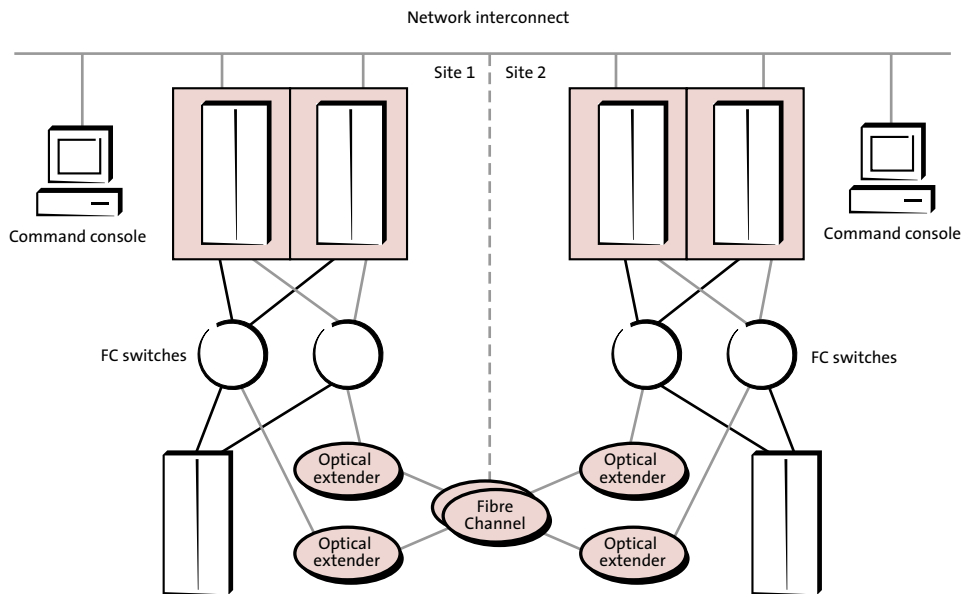
Reliable Transaction Router software guarantees delivery of transactions despite node, database, site, or network failures.

Appendix C: Compaq StorageWorks Data Replication Manager software

StorageWorks™ Data Replication Manager (DRM) software, implemented by using HSG80 Array Controller System V8.5P software, provides controller-to-controller based mirroring of data via duplicated input/output (I/O). The controllers may be separated by an arbitrary distance that is dependent on inter-site link communications technology. The replicated data is useful for fulfilling business requirements, such as data center moves or data recovery, as specified in business continuity and disaster recovery plans.

For the purpose of this discussion, consider that data is kept in two separate locations. These two locations may be as close together as a couple of meters, or as far apart as several thousands of kilometers. The copy of the data that is closest to the server initiating the I/O is considered to be at the local, or initiator, site. Similarly, a mirror of the data that is located the furthest from the server initiating the I/O is at the backup, remote, or target site.

DRM software works via cooperation between a unique pair of storage controllers. The storage controller continues to process data requests from the initiator server to the storage media (either RAID or JBOD). The DRM function operates parallel to the storage function and attempts to maintain copies of the data in the remote storage subsystem. This one-way duplication of write I/O continues as long as the link between the two storage systems is intact.



StorageWorks Data Replication Manager software architecture.

By design, DRM software is fault tolerant, so that when a failure occurs in the storage area network, the correct recovery action is taken. For example, on a link failure, the recovery actions are first to attempt to fail over to the standby link and then to try to temporarily log data for later merging into the remote copy. Finally, a full copy to the remote storage subsystem is performed.

DRM software provides disaster tolerance for systems based on Microsoft Windows NT Server and the *AlphaServer* system running *Tru64* UNIX and *OpenVMS* operating systems. The systems can be clustered at both locations, at one location, or at neither location, depending on the desired level of availability to complement the disaster tolerance.

Appendix D: Compaq Disaster Tolerant Cluster Services

Disaster Tolerant Cluster Services (DTCS) is an industry-leading disaster-tolerant computing architecture that ensures recovery of essential applications in minutes or seconds—even if an entire data center or site is disabled. Most fault-tolerant architectures safeguard only against single-component failure.

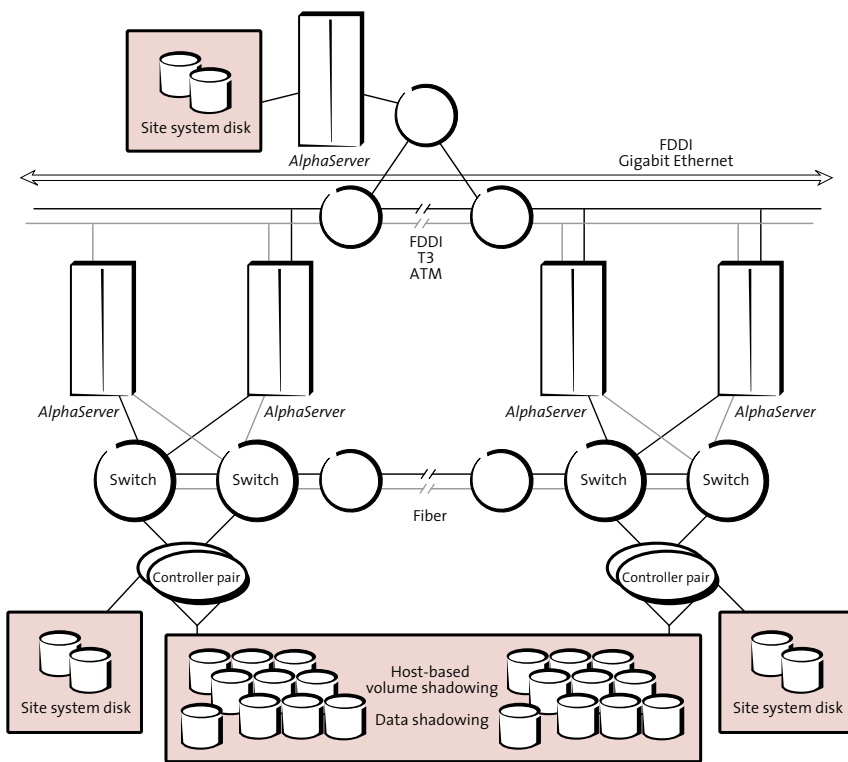
Using high-speed networks and *OpenVMS* clustering technology, the *AlphaServer* system's disaster-tolerant solutions link two data centers up to 500 miles (800 km) apart. During normal operations, the two sites communicate and share resources. If a disaster disables one facility, the critical applications fail over, transferring control to the surviving data center.

Recovery is accomplished so quickly that failures are virtually transparent to users.

As part of DTCS, Compaq Global Services can

- > Review your current and planned IT environment and recovery procedures
- > Define the cluster configuration to meet your redundancy needs and desired performance levels
- > Implement your configuration, then customize and install the software environment
- > Test and verify your solution
- > Provide orientation training for your staff

Depending on your current situation, Compaq can create a totally new solution, extend an existing single-site environment to a two-site cluster, or, if you choose, implement one site at your location and the other at a Compaq facility.



Disaster Tolerant Cluster Services architecture.

compaq.com

COMPAQ
Inspiration Technology

June 2001. Compaq, AlphaServer, Himalaya, NonStop, StorageWorks, and the Compaq logo, registered U.S. Patent and Trademark Office. Inspiration Technology, OpenVMS, and Tru64 are trademarks of Compaq Information Technologies Group, L.P. Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the U.S. and other countries. All other product names mentioned herein may be trademarks or registered trademarks of their respective companies. Compaq Computer Corporation shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

Printed in the U.S.A. 01-0028 Order number 147T-0301A-WWEN

©2001 Compaq Computer Corporation