Waters' Software Disaster Recovery Plan for Business Continuity

Julien Chardon and Gilles Bassard
Waters Corporation, Saint-Quentin-en-Yvelines, France

ABSTRACT

Are you really prepared and ready for disasters?

Do the business expectations match the IT solutions?

Data volume continues to increase in the laboratory environment. As a result, Laboratory Informatics solutions such as Waters™ Empower™ Chromatography Data System, UNIFI™ Scientific Information System, NuGenesis™ LMS, NuGenesis SDMS, and NuGenesis ELN products are becoming more business critical given the large number of instruments and staff that they serve.

Treating these products as business critical applications, therefore, would seem to make good sense for science-driven organizations.

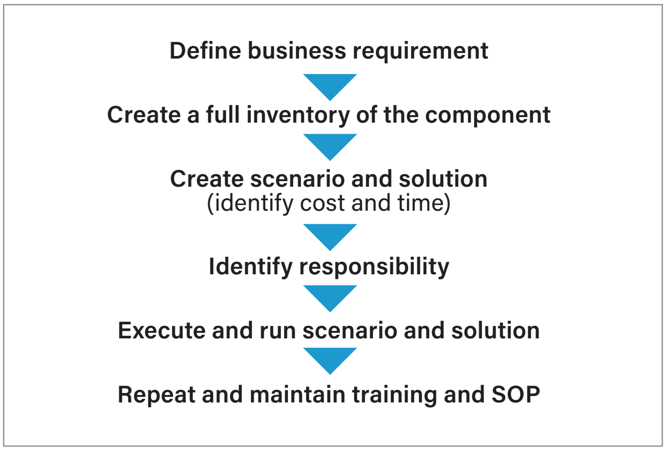
In this white paper we will explore application infrastructure architecture, backup strategies, recovery time objectives (RTO), recovery point objectives (RPO), failure analysis, and how to deploy and challenge a disaster recovery protocol.

INTRODUCTION

An Information Technology (IT) Disaster Recovery Plan (DRP) provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes, and people. Protecting your firm's investment in its technology infrastructure, and protecting your firm's ability to conduct business are the key reasons for implementing an IT DRP.

The intent of a system DRP is to provide a step-by-step procedure for recovering disrupted systems and networks, and help resume normal operations. The goal of these processes is to minimize any negative impacts to your company's operations. The disaster recovery process identifies critical IT systems and networks; prioritizes their recovery time objective; and delineates the steps needed to restart, reconfigure, and recover them. This plan also includes all the relevant supplier contacts, sources of expertise for recovering disrupted systems and a logical sequence of action steps to take for a smooth recovery.

The success of disaster recovery may require multiple resource and knowledge to cover all aspects (network, application, compliance, and business people). Waters can help, review, and participate but cannot develop a full DRP for customers.



Define business requirement

Create a full inventory of the component

Create scenario and solution
(identify cost and time)

Identify responsibility

Execute and run scenario and solution

Repeat and maintain training and SOP

Figure 1. Global process.

RISK ASSESSMENT AND/OR BUSINESS IMPACT ANALYSIS

Before you can generate a detailed recovery plan, you'll need to perform a Risk Assessment (RA) and/or Business Impact Analysis (BIA) to identify the system services that support the critical business activities. Then, you'll need to establish recovery time objectives (RTOs) and recovery point objectives (RPOs).

RA and BIA are crucial steps in the development of a DRP. But, before we look at them in detail, we need to locate disaster recovery RA and BIA in the overall planning process.

The overall goal for a DRP is to provide strategies and procedures that can help return to an acceptable level of performance as quickly as possible following a disruptive event. The speed at which system assets can be returned to normal or near-normal performance will impact how quickly the organization can return to business as usual or an acceptable interim state of operations.

A disaster recovery project has a fairly consistent structure, which makes it easy to organize and conduct plan development activity.

As (figure 2) illustrates, the disaster recovery process has a standard process flow. In this, the BIA is typically conducted before risk assessment.

The BIA identifies the most important business functions and the systems and assets that support them.

- Which business processes are of strategic importance?
- What disasters could occur?
- What impact would they have on the organization financially? Legally? On human life? On reputation? On productivity?
- What is the required recovery time period?

Answers obtained via questionnaire, interviews, or meeting with key users of IT.

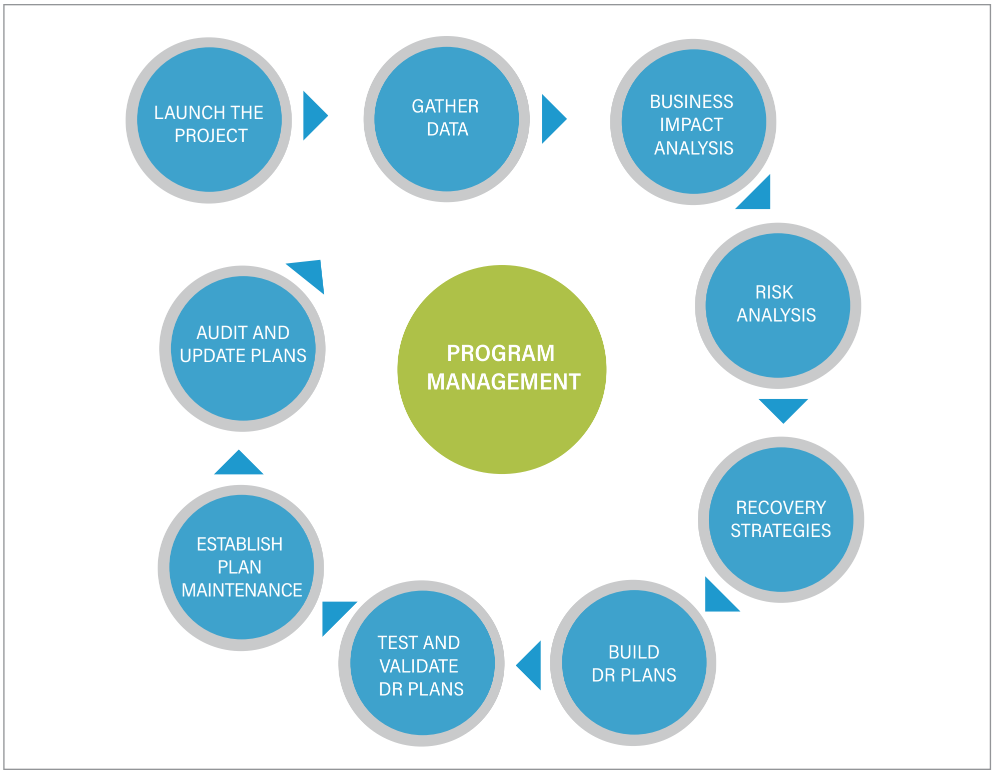


Figure 2. Lifecycle.

Next, the risk assessment examines the internal and external threats and vulnerabilities that could negatively impact system assets.

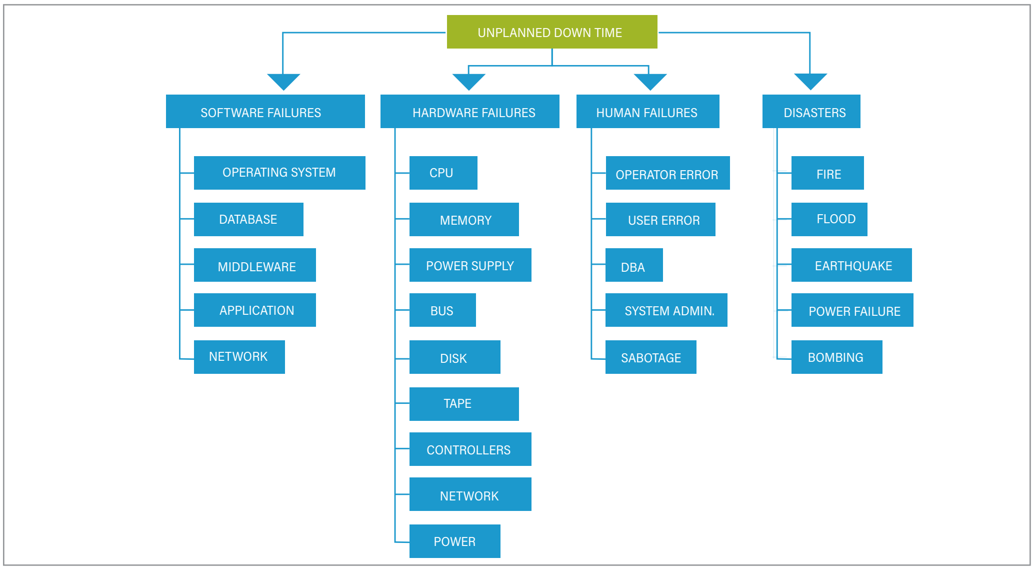


Figure 3. Possible vulnerabilities caused by unplanned downtime.

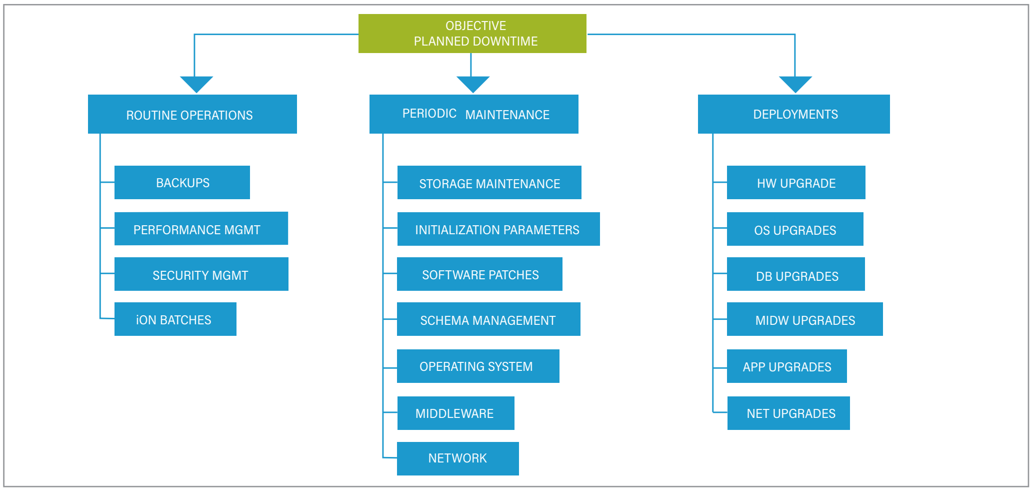


Figure 4. Possible vulnerabilities caused by planned downtime.

EVENT DAMAGE CLASSIFICATION

- Negligible: No significant cost or damage
- Minor: A non-negligible event with no material or financial impact on the business
- Major: Impacts one or more departments and may impact outside customers
- Crisis: Has a major material or financial impact on the business

Minor, Major, and Crisis events should be documented and tracked to repair.

HOW MANY 9'S DO YOU NEED?

Hours/day X 7 days/week X 52 weeks/year – 8,736 hrs/year

- If the system requires 99.9% up time then the system can be unavailable for 8.74 hours/year 0.4 days/year (1 shift)
- If the system requires 99.99% up time then the system can be unavailable for 0.9 hours/year 52 min/year
- If the system requires 99.999% up time then the system can be unavailable for .09 hours/year 5 min/year

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the disaster. These factors in turn depend on the affected equipment and application(s). An RTO is measured in seconds, minutes, hours, or days and is an important consideration in disaster recovery planning.

Once the RTO for an application has been defined, administrators can decide which disaster recovery technologies are best suited to the situation. For example, if the RTO for a given application is one hour, redundant data backup on external hard drives may be the best solution. If the RTO is five days, then tape, recordable compact disk (CD-R), or offsite storage on a remote web server may be more practical.

The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs, and can be specified in seconds, minutes, hours, or days. This is an important consideration in disaster recovery planning.

Once the RPO for a given computer, system, or network has been defined, it determines the minimum frequency with which a backup must be made. This, along with the recovery time objective (RTO), helps administrators choose optimal disaster recovery technologies and procedures. For example, if the RPO is one hour, backups must be made at least once per hour. In this case, external, redundant hard drives may prove to be the best disaster recovery solution. If the RPO is five days (120 hours), the backup must be made at intervals of 120 hours or less. In this situation, tape or CD-R may be adequate.

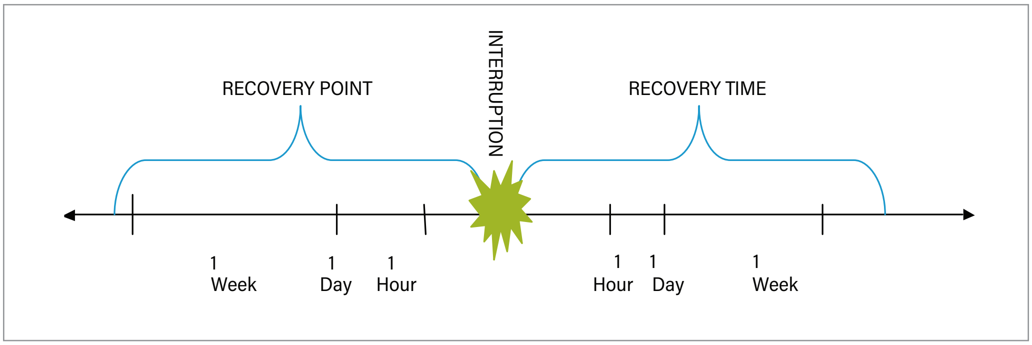


Figure 5. Recovery Point/Recovery Time.

STRUCTURE FOR A DISASTER RECOVERY PLAN

Assuming you have completed a RA and have identified potential threats to your infrastructure, the next step is to determine which infrastructure elements are most important to the performance of your company's business. Also assuming that all others IT/scientific systems and networks are performing normally, your firm ought to be fully viable, competitive and financially solid. When an incident – internal or external – negatively affects the system, the business could be compromised.

Once this work is out of the way, you are ready to move on to developing disaster recovery strategies, followed by the actual plans.

DEVELOPING DISASTER RECOVERY STRATEGIES

According to the Global Standard for IT Disaster Recovery (ISO/IEC 27031), "Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery, and restoration are put in place." Strategies define what you plan to do when responding to an incident, while plans describe how you will do it.

Once you have identified your critical systems, RTOs, RPOs, etc., create a table to help you formulate the disaster recovery strategies you will use to protect them.

You'll want to consider issues such as budgets, management's position with regard to risks, the availability of resources, costs versus benefits, human constraints, technological constraints, and regulatory obligations.

TRANSLATING DISASTER RECOVERY STRATEGIES INTO DISASTER RECOVERY PLANS

Once your disaster recovery strategies have been developed, you're ready to translate them into DRPs. Here we can see the critical system and associated threat, the response strategy and (new) response action steps, as well as the recovery strategy and (new) recovery action steps. This approach can help you quickly drill down and define high-level action steps.

DEVELOPING DISASTER RECOVERY PLANS

DRPs provide a step-by-step process for responding to a disruptive event. Procedures should ensure an easy-to-use and repeatable process for recovering damaged assets and returning them to normal operation as quickly as possible. If staff relocation to a third-party hot site or other alternate space is necessary, procedures must be developed for those activities.

The success of disaster recovery may require multiple resource and knowledge to cover all aspects.

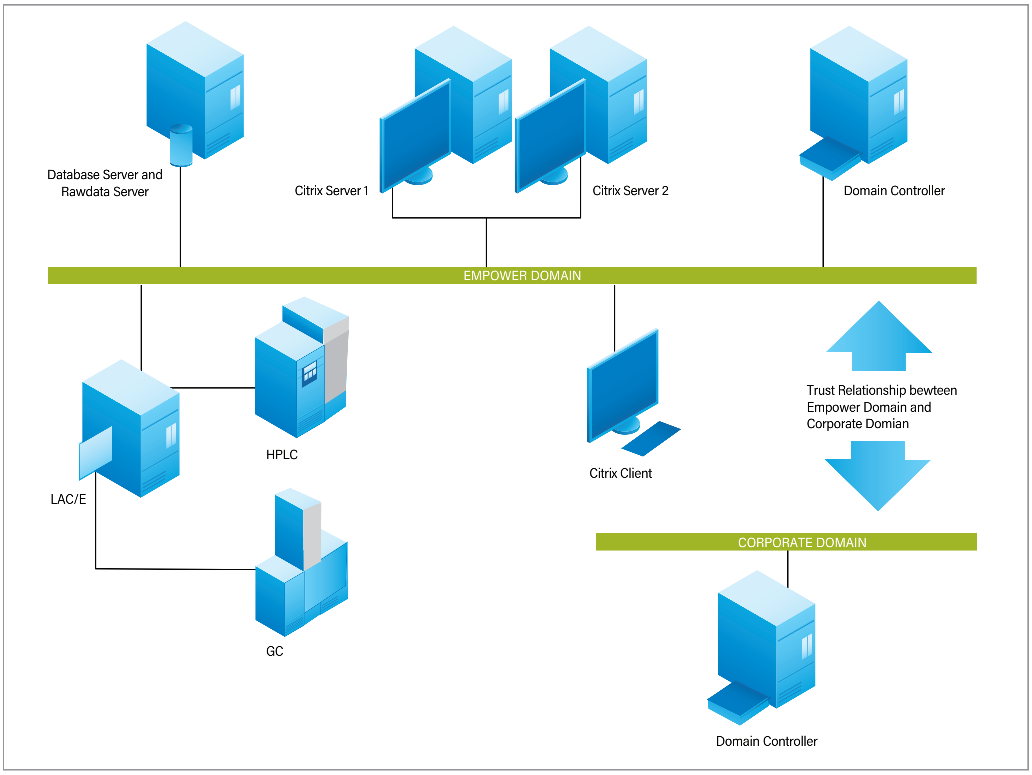


Figure 6. Empower system example.

BASIC DISASTER RECOVERY PLAN SCENARIOS TO CONSIDER

- The full loss of any device (Domain Controller (DC), DataBase (DB), RawData, LAC/E,™ Switch, etc.)
- Restore of backup (Test all types: hot backup, cold backup, OS backup)
- Hardware component lost for any device identified

At server level the following have to be done as a minimum:

Example: for Empower an SOP or Internal Procedure for:

- Full server lost must be defined
- OS disk lost must be defined
- Program disk lost must be defined
- Database disk lost must be defined
- Raw data disk lost must be defined

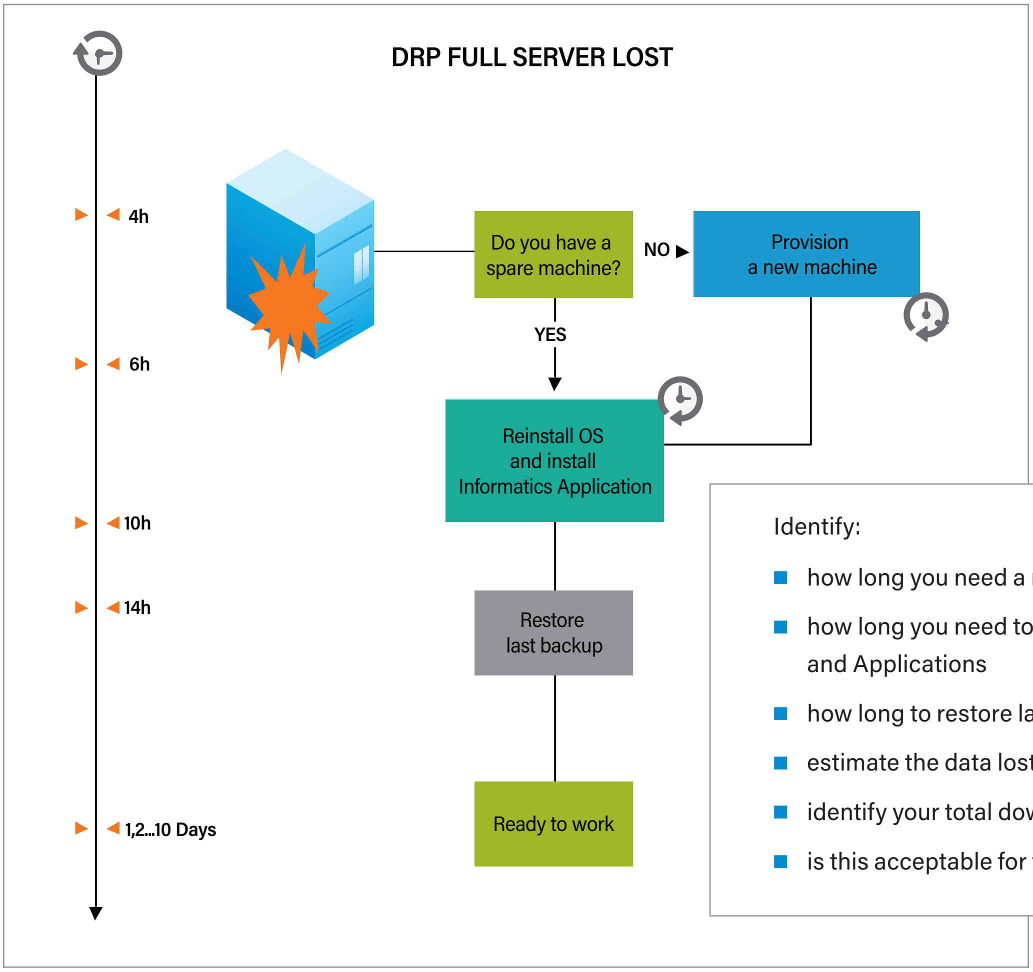


Figure 7. DRP Full server lost example.

Identify:

- how long you need a new machine
- how long you need to setup Windows and Applications
- how long to restore last backup
- estimate the data lost and cost
- identify your total downtime and estimate the cost
- is this acceptable for the labs

THE DISASTER RECOVERY PLAN STRUCTURE

The following section details the elements in a DRP plan in the sequence defined by ISO 27031 and ISO 24762.

Important: Best-in-class DRPs should begin with a few pages summarizing key action steps and lists of key contacts and their contact information for ease of authorizing and launching the plan.

- **Introduction.** Following the initial emergency pages, DRPs have an introduction that includes the purpose and scope of the plan. This section should specify who has approved the plan, who is authorized to activate it, and a list of links to other relevant plans and documents.
- **Roles and responsibilities.** The next section should define roles and responsibilities of disaster recovery team members, their contact details, spending limits (for example, if equipment has to be purchased), and the limits of their authority in a disaster situation.
- **Incident response.** During the incident response process, awareness of abnormal situations (such as being alerted by various system-level alarms) becomes evident. Quickly assess the situation (and any damage) to make an early determination of its severity. Attempt to contain and control the incident, and notify management and other key stakeholders.
- **Plan activation.** Based on the findings from incident response activities, the next step is to determine if DRPs should be launched, and which ones in particular should be invoked. If DRPs are to be invoked, incident response activities can be scaled back or terminated, depending on the incident, allowing for launch of the DRPs. This section defines the criteria for launching the plan, what data is needed and who makes the determination. Included within this part of the plan should be assembly areas for staff (primary and alternates), procedures for notifying and activating disaster recovery team members, and procedures for standing down the plan if management determines the DRP response is not needed.
- **Document history.** A section on plan document dates and revisions is essential, and should include dates of revisions, what was revised and who approved the revisions. This can be located at the front of the plan document.
- **Procedures.** Once the plan has been launched, disaster recovery teams take the materials assigned to them and proceed with response and recovery activities as specified in the plans. The more detailed the plan is, the more likely the affected IT asset will be recovered and returned to normal operation. Technology DRPs can be enhanced with relevant recovery information and procedures obtained from system vendors. Check with your vendors while developing your DRPs to see what they have in terms of emergency recovery documentation.
- **Appendixes.** Located at the end of the plan, these can include systems inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data, and any additional documentation that will facilitate recovery.

FURTHER ACTIVITIES

Once your DRPs have been completed, they are ready to be exercised. This process will determine whether they will recover and restore IT assets as planned.

Always tested in this order:

- Desk-based Evaluation/Paper Test: A group steps through a paper procedure and mentally performs each step
- Preparedness Test: Part of the full test is performed, different parts are tested regularly
- Full Operational Test: Simulation of a full disaster

Test types:

- Checklist Review: Reviews coverage of plan – are all important concerns covered?
- Structured Walkthrough: Reviews all aspects of plan, often walking through different scenarios
- Simulation Test: Execute plan based upon a specific scenario, without alternate site

- Parallel Test: Bring up alternate off-site facility, without bringing down regular site
- Full-Interruption: Move processing from regular site to alternate site

Existing plans will result in successful recovery of infrastructure and business processes also can:

- Identify gaps or errors
- Verify assumptions
- Test time lines
- Train and coordinate staff

Testing incident response can start with easier operations and proceed to more complex. Often part of the problem is the long time it takes or the errors made, which can be optimized by practice.

At the end, compare current level with desired level:

- Which processes need to be improved?
- Where is staff or equipment lacking?
- Where does additional coordination need to occur?

The key here is not whether you have a backup, but if the backup is good. Has it been tested? Were there any errors during that last backup that you're relying on so heavily? Did you check the event logs? When disaster strikes, it's too late to find out that your backup isn't reliable.

You want redundancy built into your production servers, but are both of these power supplies plugged into the same circuit? Are they plugged into the same power strip? Could someone accidentally turn off both supplies with an accidental flip of a switch? This has happened before. You need to proactively identify single points of failure in your system. It doesn't matter how many power supplies you have if someone can accidentally flip a switch and turn off the whole system, possibly introducing database corruption that could take hours to repair.

Having a spare system is one of the best ways to ensure that you'll be able to get back up and running without relying on some third party to provide you with hardware. However, do not fool yourself into believing that you will be able to merely power up this spare system and go back to bed when your system crashes in the middle of the night. You still have potentially lots of work to do before you are done. Only through careful analysis and rehearsal will you be able to minimize your downtime.

Having an on-call system is wonderful, but there are still many things to consider. Does every on-call team member know how to perform disaster recovery on their own? Have they been involved in drills? Do they have access to the disaster kit? Has knowledge been shared amongst the team or reside with one person?

Use your imagination. Be creative when thinking of ways the system can fail. Remember that part of disaster preparedness is to expect the unexpected. For example, you may deploy Uninterruptible Power Supplies (UPS) everywhere. However, if the UPS get hit by lightning or some other disaster happens, the UPS will fail. Be creative when considering what can go wrong. Remember "Murphy's Law": Anything that can go wrong will, and at the most inopportune moment.

Improving security and availability is a good idea, many solutions exist from software or hardware, but both have limitations and must be selected according to needs and knowledge. Do not implement a solution without expertise.

In parallel to these activities are three additional ones: creating employee awareness, training, and records management. These are essential in that they ensure employees are fully aware of DRPs and their responsibilities in a disaster, and disaster recovery team members have been trained in their roles and responsibilities as defined in the plans. And since disaster recovery planning generates a significant amount of documentation, records management (and change management) activities should also be initiated. If your organization already has records management and change management programs, use them in your disaster recovery planning.

HOW WATERS PROFESSIONAL SERVICES CAN HELP YOU

Today's laboratory-based organizations face increasing pressure to reduce cost, speed product to market, and increase resource utilization. Waters strives to be a partner that is involved in our customer's success. This partnership is even more important with the increasing number of customer requests for process help in their business workflow. The improvements in process and workflow provided by these professional and consultative services can easily be integrated into an organization's efforts to reduce waste and variability.

Our corporate mission is to ensure our customers are successful at leveraging all aspects of the innovative technologies in the marketplace. We strongly believe that we have the responsibility to not only provide the tools for scientists to make profound discoveries, but also assist our customers to achieve maximum utilization from their investment and minimize the timelines for the return on investment.

During the initial visit, the Waters consultant and personnel associated with your site meets with appropriate stakeholders to gain a thorough understanding of your business goals and to determine the areas of focus and the scope of the project.

At this occasion your company will provide to Waters personnel an overview of their IT system in place. Based on Waters recommendation, your company will provide a RA and/or BIA.

From this activity, a Statement of Work (SOW) is created and delivered to you for agreement and approval. The second step is the organization of an on-site workshop to discuss the DRP proposal which has been developed based on the scope and information that you had provided to Waters.

The DRP proposal comes with a discussion, recommendations, and knowledge to cover all aspects. The information below is an example layout of information provided:

- Basic DRP scenario to consider
- Backup strategies
- Improve security and availability
- Training

With the specifics, the Waters consultant and personnel associated with your site will work with you to determine how and where the recommendations can have a positive business impact on your organization. If required, the consultant works with a team of specialists, service engineers, account managers, and trainers to ensure that all appropriate resources required to execute the action plan are involved in the process.

Although the knowledge of your specific system is mandatory, for the purposes of this white paper we will focus on the generic process to build a DRP.

If you would like to discuss this with a Waters Professional Services Consultant, contact Waters.

References

1. Paul Kirvan, Independant IT consultant/auditor. How to Write a Disaster Recovery Plan and Define Disaster Recovery Strategies, www.computerweekly.com
2. Disaster Recovery Plan Templates & Sample Documents, 2013. www.everyday-tech.com
3. Backup and Recovery Glossary. http://whatis.techtarget.com/glossary/Backup-and-Recovery
4. Gilles Bassard, Informatics Consultant Manager, Waters. Business Continuity and Disaster Recovery Planning, 2015.

Waters

THE SCIENCE OF WHAT'S POSSIBLE.™

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
www.waters.com