Identify all risks to ensure recoverability in an outage

A failed recovery means discontinued business. Having systems inoperable and people unavailable for a matter of hours or even days of lost revenue, customer dissatisfaction, and negative press. It is therefore critical to understand the root-causes behind why recoveries fail in the first place:

Failure to See the Big Picture.
To avoid the specter of a failed recovery, BC/DR plans must be comprehensive, detailed, and consolidated.

Failure to Manage Change.
Change management is required to ensure that daily business operations, the BC/DR plan, and the recovery solution are all kept in sync.

Failure to Validate.
The combination of tests (does it work) and exercises (can we do it) provide the final stamp of approval that a business has done their due diligence to protect themselves against a failed recovery.

Each and every one of the root causes behind failed recoveries can be overcome, providing businesses with the resiliency they need to move forward with confidence.

Failure isn't a pleasant topic for discussion, but is necessary to prevent future failures from occurring.

When considering business continuity and disaster recovery (BC/DR), a failed recovery means discontinued business. Having systems inoperable and people unavailable for a matter of hours or even days can be disastrous in terms of lost revenue, customer dissatisfaction, and negative press. It is therefore critical to understand the root-causes behind why recoveries fail in the first place.

Failure to See the Big Picture
Planning is foundational to BC/DR. Consequently, a failure to plan — and plan well — destroys all opportunity for successful recovery.

There are many reasons why enterprises may neglect to create a BC/DR strategy at all. Many owners and managers have simply never felt the need to develop a formal plan, believing that insurance companies, the government, and their own business skills will help them pick up the pieces in the event a disaster strikes. Others would like to develop a BC/DR game plan, but believe that the process is either too time-consuming or too complex to tackle. Then there are the procrastinators: the owners and managers who fully understand the

Each and every one of the root causes behind failed recoveries can be overcome, providing businesses with the resiliency they need to move forward with confidence.

SUNGARD® AVAILABILITY SERVICES™

WHITE PAPER

Thought Leadership

42%

"Companies have plans in place but don't always keep them up-to-date … In 2007, 58% of companies were updating their plans at least twice a year, but in 2010 that number shrank to 42%. The best practice in plan maintenance is to ensure that you update DR plans continuously as part of configuration management and change management."

need for a BC/DR blueprint, but who never get around to creating the plan, repeatedly postponing the task to another day — a time that never seems to arrive. Finally, many companies feel that in today's difficult economic environment, creating a BC/DR strategy is simply too expensive.

Fortunately, with recent disasters very much in the forefront of people's minds, BC/DR planning is taking place more regularly, from local concerns to global enterprises. But just "having a plan" is not enough. To avoid the specter of a failed recovery, BC/DR plans must be comprehensive, detailed, and consolidated.

Comprehensive

A BC/DR strategy that will truly protect mission-critical operations must cover every aspect of continuity analysis and planning, and be flexible enough to adapt to a business' unique preferences and requirements. It should:

- **Assess vulnerability and risk regularly** to identify the exact people, property, and processes at risk of injury or damage from any sort of destructive event.
- **Ensure vendor viability** by evaluating vendors' resiliency, their level of preparedness, and their ability to meet the business needs in the event of a disruption.
- **Manage emergency communications,** providing two-way communication and the ability to track recovery efforts remotely, escalate incidents as needed, and make instant decisions to ensure the safety of the business's employees and critical processes.

Detailed

Considering the effort put into plan development, it's surprising how many companies do not have sufficient detail in their procedures to truly recover from an event. Four aspects must be taken into account at all times when determining the level of detail to include.

First, detail should include **what** needs to be recovered, i.e., applications, databases, networks, servers and processes.

Second, **how** the various items are recovered should be delineated. For many organizations, in-house recovery expertise is limited, which makes restoring applications and returning to normal business processes difficult. Procedures should therefore be documented in step-by-step fashion: an individual's expert knowledge should not be relied upon, since that individual may not be available during a crisis.

Third, **when** items should be recovered must be prioritized. One of the most common problems in recovery is an inadequate understanding of the interdependencies among the systems and applications being recovered. This can result in a failure to properly sequence the restart of applications. Additionally, prioritization is crucial to ensure that critical applications are brought up first, without wasting time on areas that are not essential to immediate operations.

Finally, **who** is involved cannot be overlooked or minimized. BC/DR plans must include the people responsible for each aspect of recovery and how they will address recovery — especially if people are directly affected by the disaster, making them unable or unwilling to travel. Will people need to travel to a data center? Will a mobile recovery unit come to the area? Will virtual workplaces be an option?

Consolidated

IT organizations often have data relevant to recovery in a number of places — such as in their Configuration Management Data Base (CMDB), ticketing system, and shared file space — and there is often a reluctance to consolidate that information and align it with the overall BC/DR plan. Organizations need to find the balance between duplicating information or creating two potential sources of record to ensure that there is one cohesive, coherent view of the documentation/information needed to support a recovery (and access to that information immediately at time of need).

By taking the time and effort to create a comprehensive, detailed, consolidated BC/DR plan, businesses can be confident that they have laid the foundation for recovery and resiliency after a crisis.

Failure to Manage Change

Lack of planning, however, is not the only root cause of failed recoveries. A failure to manage change effectively is a common culprit. Forrester observes, "Companies have plans in place but don't always keep them up-to-date … In 2007, 58% of companies were updating their plans at least twice a year, but in 2010 that number shrank to 42%. The best practice in plan maintenance is to ensure that you update DR plans continuously as part of configuration management and change management." [1]

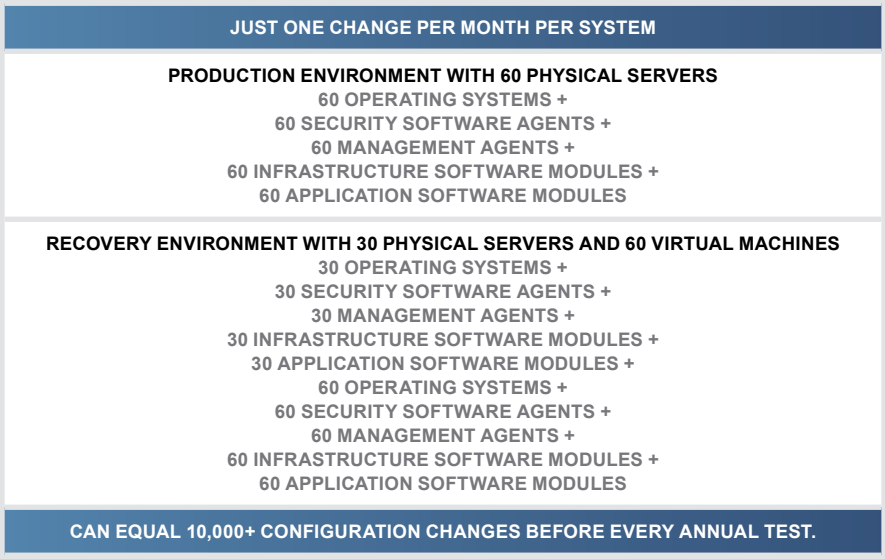
For example, changes happen constantly in the production environment, spanning hardware and software updates, the addition or removal of systems, and configuration changes. Consider a typical environment with just 60 servers (see Fig. 1). A single change per month per system can result in more than 10,000 changes before each annual test.

Keeping the recovery environment current with the production environment can become a monumental task for resource-strapped IT organizations. Yet if the production environment and the recovery configurations are not kept in lock-step with one another, a business risks a critical breakdown in the event of a crisis.

The production environment is only one place where changes occur in business. Process changes, personnel changes, vendor changes, and more all affect the BC/DR plan and therefore a company's overall resiliency. Change management is required to ensure that daily business operations, the BC/DR plan, and the recovery solution are all kept in sync.

1
"Wake-Up Call: You Aren't Ready For A Disaster," Rachel A. Dines, Forrester Research, Inc., February 2011.

Figure 1



The frequency and complexity of change means keeping your recovery plans and processes up-to-date is a huge task.

Continual validation, testing, and exercises are essential to verify that the recovery solution is aligned with production, documentation is up to date, and people are at an enhanced state of readiness to respond to an incident.

Failure to Validate

A business creates a well-documented, detailed BC/DR plan and manages changes on a systematic basis. Can recovery still fail?

Absolutely. Continual validation, testing, and exercises are essential to verify that the recovery solution is aligned with production, documentation is up to date, and people are at an enhanced state of readiness to respond to an incident. This includes not only regular testing of systems, applications, networks, and failover capabilities, but also validation of the wider spectrum of business concerns. Stephanie Balaouras of Forrester Research, Inc., addressed this point when she stated that IT DR teams, "very rarely include BC considerations, such as communication, as part of their test. They are simply testing their ability to recover IT systems. There is very little realism in these plans; they assume that all IT employees are available or that power, transportation, and telecommunication are available. IT DR tests should also include business users; recovering the systems is not the same as validating that users can do their jobs."[2]

2 "Stop The Insanity: If You Don't Exercise Your Business Continuity Plans, You Aren't Prepared," Stephanie Balaouras, Forrester Research, Inc., December 2011.

Tests and exercises fall into three main categories:

- **Communication validation:** Can information be transmitted to and received from company personnel?
- **Plan content validation:** Are all the components of an effective plan present? i.e., Is the necessary equipment available? Are roles and responsibilities defined? Are all procedures documented?
- **Recovery strategy validation:** Does the established plan actually work smoothly and effectively?

Within these categories, there are multiple types of tests and exercises that can be executed:

Function Test Types (Examples)

FUNCTION TEST NAME	FUNCTION TEST DESCRIPTION
Notification	Notification/Call tree test to validate contact capabilities
Work-From-Home	Functional test to validate capabilities
Alternate Workplace	Validation of alternate workplace/site capabilities
Workload Transfer (remote)	Validation of work volume/skills/capabilities to alternate site
Workload Transfer (local)	Validation of workload transfer locally (skills/volume/etc.)
Laptop Procurement	Validate the ability to request and provision laptops
Alternate Procedures	Validate alternate procedures due to event (i.e. loss app.)
Mobile Recovery Unit	Validate capabilities of utilizing alternate work site/facility

Exercise Types (Examples)

EXERCISE NAME	EXERCISE DESCRIPTION
Plan Walkthrough	Walk through BC Plan with Plan owners/team members to identify concerns and provide overall Plan content and format awareness training (BC Plan page turn exercise)
Tabletop (simulation)	Simulates an event in an informal and stress-free environment; designed to elicit constructive scenario-based discussions. Used for training and awareness purposes of BC Plan actions/activities
General Walkthrough	Various types of general walkthrough exercises to review the scenario with relevant personnel and make key personnel aware of expectations and identify potential issues/areas of concern
Full-Scale	Simulates an actual emergency, intended to evaluate Business Continuity procedures and capabilities under simulated and somewhat stressful conditions

It is the combination of tests (does it work) and exercises (can we do it) that provide the final stamp of approval that a business has done their due diligence to protect themselves against a failed recovery.

Identify all risks to ensure recoverability in an outage

Conclusion

Failure Is Not An Option

For businesses who want to compete, grow, and succeed, a failed recovery is not an option. Fortunately, organizations can decide how to proceed with planning, managing, and testing their recovery solutions. They can elect to perform all these tasks in-house, or they can seek the services of an expert service provider who would then be responsible for:

- Providing lifecycle BC/DR guidance, direction, and management.
- Managing and maintaining the recovery infrastructure, whether cloud, dedicated physical, or a hybrid of the two.
- Overseeing data movement to and from the recovery site using technologies selected to meet the recovery requirements of the specific applications.
- Planning validation, test, and exercise scope, type, and frequency.
- Performing a fully-managed restart of simple and complex applications.
- Meeting the recovery time and recovery point objectives of the business.
- Connecting users seamlessly, whether remotely, with mobile recovery units, or with specialized workforce recovery facilities.

The bottom line — and the encouraging news — is that each and every one of the root causes behind failed recoveries can be overcome, providing businesses with the resiliency they need to move forward with confidence.

Additional reading

IT Disaster Recovery Best Practices

10 Things Your Team is Afraid to Tell You About Your DR Plan

For more information

Call us to schedule a customized workshop or learn how your organization can benefit from Sungard AS customized cloud solutions and services.

About Sungard Availability Services

Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us