

## Four Pillars of Emergency Management

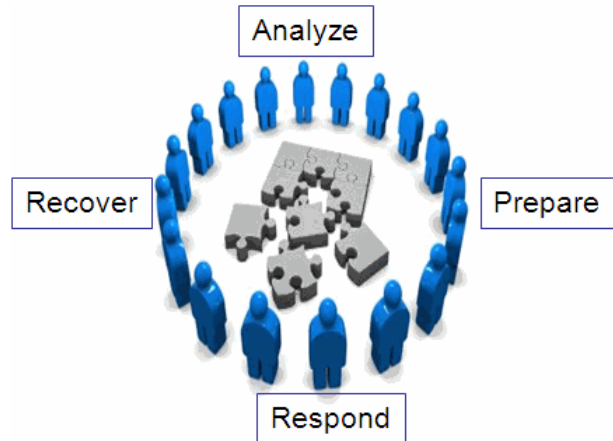
By Rex Bullard

When developing a Disaster Recovery Plan, you are really working in the area of Emergency Management. Corporations implement disaster recovery plans just as cities have emergency management plans to deal with major events such as hurricanes, snow storms, civil unrest, etc.

As teams develop Emergency Management Plans, they work with four basic tenets of plan development.

They are:

1. **Mitigation/Analyze**
2. **Preparation**
3. **Response**
4. **Recovery**



In the Mitigation phase of disaster recovery planning, we look for ways to reduce the potential for disaster within your organization. We review certain standards and policies that may or may not already be in place and improve the way business is transacted on a day-to-day basis.

The success of the plan will depend on how much effort is put into it during the development stage. In other words, your mother was right – “you’ll get out of it exactly what you put into it.” Whether you call her and tell her is up to you.

Of the four areas of emergency management, the one most often overlooked is Response. Specific actions call for specific response. We don’t automatically summon the fire department when the smoke alarm goes off. We evaluate the problem, and respond appropriately. Likewise, recovery response should be linked to what aspects of the disaster recovery plan need to be implemented. If a fire wipes out your entire building it’s a different response than if a hard drive crashes on the main server. So the disaster recovery plan is based on levels of response, depending on the emergency.

Finally, the Recovery stage details the exact events that are required to restore operation and get the data center fully functional. Once again, these events differ based on the type of emergency that has occurred. This is the stage that you are preparing for, and one that you hope you never need.

One major point to be consider - having a backup strategy, doing backups everyday and running anti-virus software **does not mean** that you have a Disaster Recovery Plan. While these things are necessary, they are only small pieces of what should be a much more comprehensive planning process.

Extracted from “Designing a Disaster Recovery Strategy” – Info-tech Research Group  
OCT09

LANtech Limited, 191 Thorndon Quay, Wellington  
PH: +61 4 499 4661  
[www.lantech.co.nz](http://www.lantech.co.nz)

# The Third and Fourth Pillar of a Disaster Recovery Plan

## Plan Review & Testing

**According to the American Red Cross, 40% of small businesses that suffer a disaster will never re-open for business.**

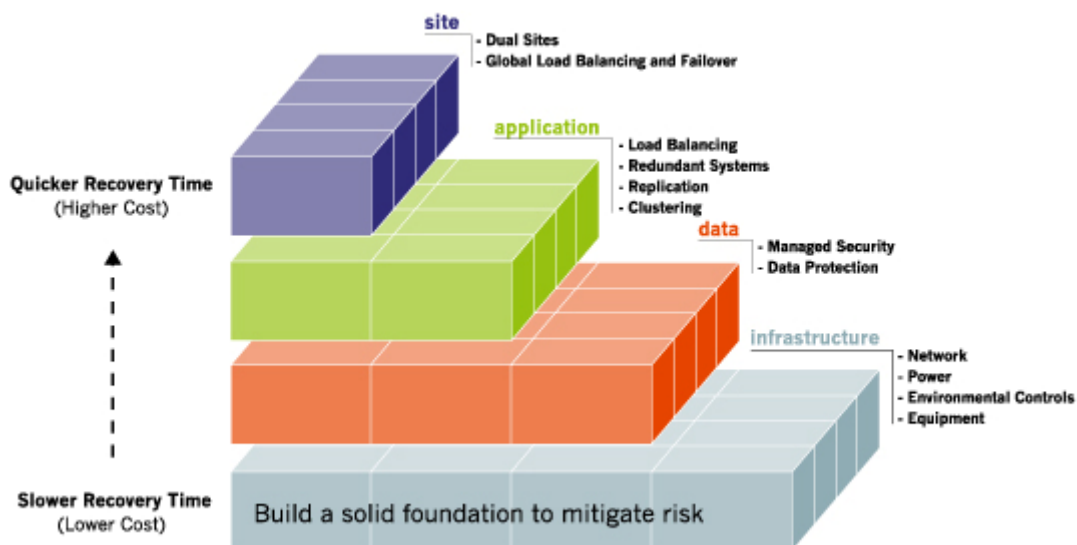
Once the team assignments and roles have been defined, the report is basically ready for the last two steps. These are Plan Review and Plan Testing. Software developers would never implement a new application without testing, and we're not going to put the plan to save the world on the shelf without giving it a thorough review.

First, each member of the Disaster Recovery Team should review the plan. They are looking for basic flaws in the approach taken to recover the systems. Have the team review the prioritization, team alignment, recovery instructions and so on. Don't be afraid of discussion and even some criticism, if it means a smoother recovery later. If changes are required, make them and have the team review the document again.

Once the team has agreed with the plan in principle, it must be tested.

Do you think your organisation is prepared for a full system recovery? It is important to test critical parts of the plan and eliminate as many assumptions as possible. Often, the plans cover the big picture and miss critical details. Remember that recovery is more than getting tapes from offsite storage and restoring the applications.

Check the details. Make no assumptions. Make sure any database can be restored as you think it can. Set benchmarks to estimate performance and make notes about the test in the documentation. Make sure the instructions are clear and easy to follow.



Extracted from “Designing a Disaster Recovery Strategy” – Info-tech Research Group  
OCT09

LANtech Limited, 191 Thorndon Quay, Wellington  
PH: +61 4 499 4661  
www.lantech.co.nz

## You may think you have covered everything in your plan.

### *You haven't!*

When you come to test it you will realise that you have missed something. Maybe it's the after hours phone number of your IT Support company. Maybe its license information or authentication codes. Something is likely to be missed.

### *Better to find out during a controlled test rather than in the midst of chaos and rubble.*

If possible, put in place the ability to have redundant servers and to be able to test the restore process. Your IT Support Partner should be able to assist you with this. Use a replacement server that is as close as possible to your current production system. Have your Hardware and Software Support team install the replacement environment using instructions from the Disaster Recovery Plan. Be sure to make corrections or enhancement to the plan as a result of the test.

Grade your tests. Have meetings after the test and evaluate your performance. Discuss what went well and what needs to be improved. Learn from the test and make as many notes as possible. If you feel the test went well, find another part of the plan and test it too. Keep growing and evolving the plan to keep it sharp.



## Maintenance

Once the plan is developed, accepted and tested, you may feel like your team's work is done. Sorry - It has just begun. For the plan to remain effective, it must be kept up to date. Companies who do it right actually go as far as to change their entire culture around the concept of disaster recovery. When a new server is installed, disaster recovery is considered. When a new application is written, recovery is evaluated. Virtually everything in IT goes through the "DRP filter" once the plan has been developed. This may be as simple as updating the Disaster Recovery Plan. Or, it may be more complex and actually impact the deployment of certain equipment in order to be effective with regard to recovery.

## Conclusion

Pilots say that any landing you walk away from is a good landing.

The best Disaster Recovery Plan you will ever develop is the one you never have to use. The secret to success is to plan for the absolute worst and be ready for anything. Be thorough in the development of the plan.

Test it. Keep it up to date. Think about recovery during your development projects.

Extracted from "Designing a Disaster Recovery Strategy" – Info-tech Research Group  
OCT09

LANtech Limited, 191 Thorndon Quay, Wellington  
PH: +61 4 499 4661  
[www.lantech.co.nz](http://www.lantech.co.nz)