VIRTUALIZATION
CLOUD
APPLICATION DEVELOPMENT
NETWORKING
STORAGE ARCHITECTURE
DATA CENTER MANAGEMENT
BI APPLICATIONS
DISASTER RECOVERY/COMPLIANCE
SECURITY

Essential Guide

Developing Effective DR/BC Plans

Putting together an effective disaster recovery/business continuity plan can be a challenge. Learn about the importance of enterprise risk management and tailoring your DR plan to your organization's needs.

1
EDITOR'S NOTE

2
TEN ESSENTIAL DR TIPS

3
ENTERPRISE RISK MANAGEMENT AND BUSINESS CONTINUITY PRIMER

4
TAILORING A DISASTER RECOVERY PROGRAM TO YOUR ORGANIZATION'S NEEDS

TechTarget

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

Make DR Planning a Priority

I'VE BEEN COVERING disaster recovery for about eight years now, and year after year, our surveys show that organizations are not confident in their ability to recover data after an outage. And the reasons they cite remain largely the same. Some lack confidence in the backup/DR technologies they rely on. Others say that DR planning is too expensive and they can't get management support for an initiative that isn't directly tied to revenue.

If it's a technology issue: Why? Is it really a tech issue, or does your organization lack the necessary skills? Have you taken an inventory of your backup data recently? If restores are slow, perhaps you are backing up information that you don't need? If you are relying on outdated technology, maybe it is time to make an investment in something new. I'm not going to argue that good backup and DR is cheap, but there are a variety of options available today at many price points, depending on your organization's needs.

Traditionally, disaster recovery is an exercise in risk mitigation. Many have likened DR planning to purchasing insurance, because it is an investment in something that you may never need to use. All of that is true, and that can be a tough sell—but maybe you don't have to sell that exactly. Is there a way that you can

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

integrate DR with other essential processes? Can you take technology you already own and put it to use for DR? Maybe it's a matter of showing management just how much downtime can cost an organization. In other words, convince them it's not an insurance policy, but rather a way to increase productivity.

This Essential Guide offers a primer on business continuity and risk management, information on tailoring a DR plan to your organization's needs, and 10 things every IT professional should know about disaster recovery. Make DR planning a priority before you regret it. ■

Andrew Burton

Senior Site Editor, SearchDataBackup.com

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

Ten Essential DR Tips

THE TRUTH ABOUT disaster recovery (DR) planning is that it's a complex and typically underfunded undertaking focused on building a continuity capability that's best organized, not by disaster scenario, but by business process. It's also a task best pursued by an enthusiastic, optimistic and tenacious practitioner well-versed in project management techniques (and Middle East peace negotiations) who will work with business stakeholders. One final truth: DR planning must have senior management backing or it won't succeed.

Here are 10 essential DR planning tips that you ignore at your own risk.

1. **Make a backup.** This may seem obvious, especially given that approximately 75% of the world's data is currently protected by copying it to tape and then removing the tape to secure off-site storage. But if you read the stuff that I read or lurk around the back doors of storage analyst conferences and vendor seminars, you've certainly heard many declarations that tape is a deceased technology.

   The simple fact is that tape isn't dead, and it's a linchpin of a successful recovery following just about any disaster. Its price/performance metrics are great and getting better: There's no faster way to write data, no higher data

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

density per raised floor tile, no other media with the reliability of tape and it's dirt cheap. Even if you're mirroring disk-to-disk locally or replicating asynchronously between two stands of disks, send a backup of the data to tape just to be sure. If you're wondering why, just ask Google, Amazon, the Commonwealth of Virginia or any of the other organizations that have recently brought their systems back to life via tape data restore, despite their investments in lots of disk mirroring gear.

2. **Break a mirror.** If you're using synchronous disk mirroring (or async replication), break the mirror and check for data deltas. Nobody tests their mirrors because it's a huge hassle. You must quiesce applications using the storage, flush the cache to write data to disk A, replicate it to disk B and then turn everything off. Next, you need to do a file-by-file compare between the primary and secondary disk, and if you like what you find, you can cross your fingers and restart the mirroring or replication process hoping that everything synchronizes again.

   Why should you bother with breaking the mirror? Simple. Data's physical location on disk has a tendency to be moved by storage administrators (or these days, server administrators) who may not appreciate the importance of updating the keeper of the DR plan. Thus, you might be mirroring the wrong data or even blank space between disks. At a minimum, you need to know how

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

latency and jitter affect your replication process; these can lead to significant deltas (differences between original and copied data) that can make your recovery data useless.

3. **Get real about data archiving.** It may seem like moving older data off your primary spindles to an archival repository is outside the scope of DR planning, but you should understand how a little data archiving and grooming can reduce the workload demand on data protection services, making them more efficient. Based on our analysis of more than 3,000 companies, approximately 40% of the data stored on every hard drive in a typical shop is archival quality data. It needs to be retained, but it isn't accessed and could be moved off your spinning rust and onto an energy-efficient platform like tape augmented with the Linear Tape File System (LTFS). Set up an effective archiving system and purge the 30% of data on your disk that's junk, duplicate data or contraband, and you could recover up to 70% of the capacity of every spindle you own. That just might bend the storage cost curve at your company, and management will love you.

4. **Consider storage virtualization.** Forget what you heard back in the late 1990s when storage hardware vendors spilled so much ink condemning software-based storage virtualization as an ineffective technology that would burn up

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

budget bucks with little benefit. Since then, several array makers have transitioned their own products into stands of disk trays topped by 1U rack servers running RAID software and centralized value-add applications under a Windows or Linux OS. For the money, a software-only offering beats a hardware-centric play.

What does it have to do with disaster recovery? Storage virtualization engines—or storage hypervisors, as they're more fashionably referred to these days—provide a convenient software layer for consolidating the assortment of data protection functions that are applied in various ways to different data to deliver "defense in depth." That, in turn, simplifies the management of data protection services and enables them to be selectively applied to different data workloads based on requirements.

5. **Try a restore.** The biggest problem in DR is when you recover all your backup data only to discover that you don't have everything you need to bring your application back to life.

It isn't enough to have your mailbox data to recover Microsoft Exchange; you also need the mail software, the right .NET version, the ESE or CRCL files, and the software for your hub transport, client access server, unified message server and Active Directory roles. Are you capturing all this data? Try a restore and find out.

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

6. Set up a virtual tape library (VTL). A VTL is just some disk on which you can store 30 days' or so worth of data that has also been copied to physical tape and moved off site. The benefit of a local disk repository is the ability it provides to quickly restore individual files that have become corrupted without having to restore an entire file set from tape. You can also use post-processing deduplication to squeeze the data on your disk and reduce the capacity requirements. Post-process dedupe is usually free with your backup software.

7. Test your plan. Do an "ad hoc" tabletop exercise. Put some sticky notes on various pieces of hardware in your data center or on the monitors of your personnel indicating software or hardware failures. Then call your DR team into a meeting room and walk through the procedures to address the mock disaster scenario. This is a lot cheaper than scheduling a formal DR test event and it allows you to test procedures in a linear, sequential way that provides a great rehearsal for recovery team participants.

8. Be proactive. Maintain logs of server downtime and the root causes for downtime incidents. This data is better than generic data for ensuring that you continue to retain management support for the continuity capability. Over time, you may be able to show how your disaster prevention measures have improved uptime or mitigated what was previously protracted downtime.

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

9. **Check in with DR plan stakeholders.** Regularly contact the stakeholders in your DR plan to see what changes are coming in the next quarter. Many potential disasters can be avoided if you know about new business initiatives and new equipment deployments or other technology rollouts such as a new virtualization scheme. These types of events can upset a DR plan. Contingency plans should be created to cope with disruptive changes; plans should be retested and updated after any significant application or infrastructure changes.

10. **Polish your rhetorical skills, especially euphemisms.** With lean economic times there's usually a reduction in the management interest in funding business continuity strategies. It isn't that the business is less important, or that dependency on automation has dropped off in a tough economy. In fact, the opposite is true: Do more with less means fewer staff are even more dependent on the proper operation of the machine. DR plans are an insurance policy that in the best of circumstances will never need to be used. So, if management is losing interest in DR, call it something else. Call it software quality assurance, your new technology test lab or your cloud strategy pilot—whatever will get you the funding you need to continue operations.

These 10 DR tips will help you to keep your continuity capability on track and in line with business requirements in 2013 and beyond. —*Jon Toigo*

Enterprise Risk Management and Business Continuity Primer

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

ANY DISCUSSION OF risk management and business continuity should begin with a definition of risk. Risk has many different definitions, but it usually comes back to the fact that in virtually any activity there is the potential for something to go wrong.

The probability or likelihood of something happening becomes the risk associated with that activity. If an activity was always successful and never had any problems or issues, the probability of failure (the risk) could be considered zero. But when we think realistically, the probability or likelihood of something, no matter how insignificant, happening with an event or process is somewhere between zero and one or 100%.

For example, if a specific disruptive incident (such as a power outage lasting less than one hour) has a one in five chance of occurring (based on insurance or actuarial statistics), the risk likelihood (or probability) would be 0.2 or 20%; a one in three chance of occurrence gives a probability of 0.33 or 33%. By contrast, the probability of a wayward asteroid hitting the Earth is probably closer to zero, whereas the probability of someone being sick from work due to a cold will probably be closer to one.

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

When we examine risks, we analyze the likelihood of an event occurring, the potential severity of the event (e.g., damage to the desired process), and also the vulnerability of the situation (e.g., a weakness that helps the event occur). From this we analyze risks as a product of the likelihood of the event occurring times the potential severity times the vulnerability.

In other words, the formula for risks in business continuity works as follows:

Risk = Likelihood x Severity x Vulnerability

We can map this formula with **TABLE 1** (the data listed in Table 1 are examples):

TABLE 1. *Formula for risks in business continuity*

SITUATION	LIKELIHOOD	SEVERITY	VULNERABILITY	CALCUALTED RISK
Fire	0.3	0.7	0.2	0.042
Hurricane	0.7	0.9	0.4	0.25
Theft	0.5	0.3	0.6	0.09
Virus attack	0.6	0.8	0.4	0.19
Hostage	0.2	0.7	0.3	0.042

Likelihood: 0 = Not likely to 1 = 100% likely to occur; Severity: 0 = No impact to 1 = Total destruction
Vulnerability: 0 = None to 1 = Totally vulnerable

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

What the calculated risk figure means in the "fire" example is that there's a four in 10 chance of a fire occurring that causes significant damage, based on the existing vulnerability to fire. From the completed table you can identify and prioritize risks for further action. While we have assigned arbitrary figures to each category in this example, many of these figures can be obtained from risk tables, which themselves are based on historical data and analyses of specific events and their outcomes.

As a business continuity professional, be sure to perform a risk assessment, as we have done above, to identify situations that could occur to your organization. Once you have an agreed-upon set of risks, you can begin a business impact analysis (BIA) to determine the financial and operational effects of the identified risks to your organization.

■ ***Risk Treatment***. In enterprise risk management, once you have identified risks, you then need to decide how to address them. There are four basic approaches:

1. **Avoidance**: Deciding to not perform an activity that carries risk

2. **Reduction**: Using various approaches to reduce or mitigate the severity of the risk; you are not eliminating the risk; rather you are reducing its potential impact

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

3. **Sharing**: Identifying and engaging another entity to absorb a portion of the risk; using insurance is often considered a risk sharing option

4. **Retention**: Willingness to accept the risk and its potential outcomes

These options can be factored into your business continuity/disaster recovery planning strategies.

■ ***Risk management in the business continuity process***. Where would we place risk management in a process flow for business continuity? Risk management activities occur very early in the process. We can't begin to develop strategies, plans or anything else until we know where the organization is at risk.

■ ***Risk Management Standards and Professional Associations.*** The global risk management standard is ISO 31000, Risk Management—Principles and Guidelines on Implementation, which was released in November 2009 by the International Organization for Standardization (ISO). Another useful standard is ISO 31010:2009, Risk Management—Risk Assessment Techniques, which provides guidance on how to organize and conduct a risk assessment. In the U.S., an excellent risk management standard is SP 800-30, developed by National Institute for Standards and Technology (NIST). When working on a risk management project,

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

be sure to have these standards available for reference and advice.

Perhaps the most prominent risk organization in the U.S. is RIMS (The Risk Management Society), which addresses the entire risk management spectrum through educational programs, professional accreditations, conferences, publications, risk-related information and networking among fellow risk professionals.

Enterprise risk management is a key part of the business continuity process. Examine any of the current business continuity/disaster recovery standards, such as BS 25999 Part 2 or NFPA 1600:2010, and you'll see references to risk management.

Enterprise risk management is a key part of the business continuity process.

If your organization is large enough, it may have a risk management department or function. Be sure to contact the group and engage them early on in your business continuity/disaster recovery initiatives. Include the risk team with all your business continuity/disaster recovery efforts to share ideas and experience and reduce potential confusion during business continuity/disaster recovery plan development. —*Paul Kirvan*

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

Tailoring a Disaster Recovery Program to Your Organization's Needs

Protecting your firm's investment in its technology infrastructure and its ability to conduct business are good reasons to implement a business continuity and disaster recovery program. To be sure your plan is synchronized with your business; consider using our BC/DR checklist below.

1. **Begin** by obtaining management approval and funding for a BC/DR activity.

2. **Learn** all you can about your organization by researching the firm, interviewing company leaders, and reading annual reports and other relevant documentation.

3. **Find out** about any previous experience the organization had with disasters and other disruptive incidents, how they responded, lessons learned, etc.

4. **Review** any previous BC/DR work done by the organization. For example, did the firm have a previous BC/DR plan? If so, how well did it work and what happened to it?

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

5. **Review** results from previous analytical activities, such as a business impact analysis and/or risk assessment. It may be appropriate to update these documents to determine what changes are needed in a new or updated BC/DR activity.

6. **Meet** with essential department leaders and stakeholders to identify the important issues that should be addressed in a business continuity and disaster recovery activity.

7. **Talk** with other organizations about how they addressed similar BC/DR issues and what ultimately worked for them.

8. **Use** a request for information or request for quotation if you need to obtain specific information.

9. **Discuss** your findings and observations with colleagues such as IT leadership, company risk managers, company facilities and security staff, business unit leaders and company strategic planners.

10. **Identify** and prioritize operational, financial, human resources and other issues that will better tailor plans to the organization's needs.

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

11. **Create** a table or spreadsheet that summarizes the findings and results of your discovery. This will help you tailor BC/DR solutions to the needs of the business.

Follow these steps, and if the organization already has BC/DR plans, use your findings to update existing plans to better fit the organization's requirements. If your organization does not have a business continuity or disaster recovery program, meet with management to discuss steps for a new BC/DR program that aligns with management's perceived needs and satisfies business objectives. Results of such a meeting may not initially be a plan, but it should help you focus your efforts.

Consider using BC/DR standards as part of your development efforts.

Once you create a framework for a BC/DR activity conduct a tabletop walkthrough to see if it meets management's needs as defined in your previous meetings. If management wants a more detailed plan, the next step is to drill down to the details, e.g., procedures to recover a server, perform a server failover to a backup unit, or organize a relocation of staff to an alternate site.

Consider using BC/DR standards as part of your development efforts. Existing standards such as BS 25999:2007, NFPA 1600:2010, NIST SP 800-34, ASIS

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

SPC.1-2009, ISO 27031, and ISO 24762 can be obtained for little or no cost and can provide an effective starting point and structure to your program and plans.

Let's briefly examine some examples of tailoring a business continuity/disaster recovery program to your business' needs:

As the result of a recent merger, a firm discovers its data protection requirements have expanded significantly, especially because the new company was backing up its data on-site. The outcome was to change the data backup strategy from one in which tapes were shipped once a week to an off-site storage facility to a data mirroring application where data was replicated in real-time to an off-site data storage facility. Outcomes: More reliable and timely data backups; lower recovery point objective (RPO)

Investments in business continuity and disaster recovery can range from nothing to millions of dollars in annual spending.

In an effort to stabilize data storage costs and reduce physical space, a school district signs up for a cloud-based data storage service. Outcome: Secure data storage, fast data recovery assured when needed, additional storage space.

An IT department discovers it can leverage its other field offices as backup data storage sites by installing NAS devices in each field office and sending backup files after hours to each office via the Internet. Outcome: Diversified data storage solution.

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

Investments in business continuity and disaster recovery can range from nothing (e.g., take your chances) to millions of dollars in annual spending for hot sites, backup data centers, redundant servers, meshed data network infrastructures, storage area networks, and many other solutions. The time you spend researching the business and then tailoring a business continuity/disaster recovery program to business and operational needs will help you achieve better value for money from BC/DR investments.

Finally, once the investments have been made, and you have implemented BC/DR solutions that support your business needs, be sure to regularly exercise those solutions and keep all pertinent documentation up to date. —*Paul Kirvan*

Home

Editor's Letter

Ten Essential DR Tips

Enterprise Risk Management and Business Continuity Primer

Tailoring a Disaster Recovery Program to Your Organization's Needs

JON WILLIAM TOIGO *is a 30-year IT veteran, CEO and managing principal of Toigo Partners International, and chairman of the Data Management Institute.*

PAUL KIRVAN, *CISA, FBCI, works as an independent business continuity consultant/auditor and is secretary of the Business Continuity Institute USA chapter and member of the BCI Global Membership Council. He can be reached at pkirvan@msn.com.*

TechTarget

Developing Effective DR/BC Plans
is a SearchDataBackup.com e-publication.

Rich Castagna | *Editorial Director*

Andrew Burton | *Senior Site Editor*

Ed Hannan | *Managing Editor*

John Hilliard | *Associate Site Editor*

Sonia Lelii | *Senior News Writer*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Jillian Abbott | *Publisher*
jabbott@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com