Managing the information that drives the enterprise

STORAGE

ESSENTIAL GUIDE TO

Getting started with disaster recovery planning

Whether you're new to IT disaster recovery planning or want to brush up on best practices, we have the answers for you in this essential guide.

INSIDE

TechTarget

Disaster Recovery's
Speedway

No more excuses

Sure, disaster recovery planning can be complicated and time consuming—but consider the alternative. This Essential Guide will get you started with simple step-by-step instructions and free planning templates.

IT SEEMS LIKE every month a new survey surfaces that reveals how many companies are still unprepared to cope with any kind of service disruption, much less an out-and-out disaster. And the numbers are often staggering, with half or more of the represented companies hoping to get by on a wing and a prayer.

Equally staggering are the industry statistics that show how hard a company can be hit by the loss of their IT resources for even a relatively short period time. For some, a day or two without systems can be a fatal blow.

No company chooses to be vulnerable, but many feel that disaster recovery (DR) planning is too complex, consumes too many resources and is far too expensive. There's no denying that in some cases, putting together a DR plan can be a complicated and time-consuming process, but for most organizations, doing a little homework and making judicious purchases can effectively protect key computing assets that are core to your business.

Understanding potential risks is one of the initial steps in preparing for business continuity. During the risk assessment process, you're likely to find that the scope of your efforts doesn't have to be as wide as anticipated and you can concentrate on only the likeliest of possible interruptions.

With a good understanding of potential risks in place, you can then assess the impact of events associated with those risks. In effect, you can determine just how much preventive medicine is required and what will be needed to get the patient—your company—back on its feet.

This, of course, is an oversimplification of DR planning, but the point is planning for business continuity is not only within the reach of most companies, it may also be imperative for the survival of a business.

This guide will serve as an easy on-ramp to DR planning. Each article describes critical points and considerations, and guides you through each planning phase. And to make the planning process even less painful, we've provided links so you can download DR planning templates from our extensive SearchDisasterRecovery.com template library. These templates make creating a DR plan nearly as easy as filling in the blanks, so you can get started on your company's DR plan right now. ⊙

Rich Castagna is the editorial director of TechTarget's Storage Media Group.

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

10 THINGS THAT MUST BE INCLUDED IN DR PLANS

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

Use this helpful checklist to ensure you don't miss any key points in the DR plan process.

By Harvey Betan

THERE ARE MANY items that are required in IT disaster recovery (DR) plans—some are location-specific but some are more generic. This article will discuss the top 10 items critical for the success of your IT DR plan. Organizations may differ on the priority or of these items, but they must exist somewhere within the DR plan.

1. **DR plans must have an accurate communication or call list.** Communicating with other employees is essential during a disaster. Some organizations use third-party products from companies

such as Everbridge Inc. or MIR3 Inc. for this. Regardless of how you generate your call list, the list must be current. The list should have designated backups for each key individual and contact information for them (home phone, cell phone, email). If you are using a call tree, make sure that you have a loop back so that the last person on the list will confirm that the call was made. Also, someone should be designated as the communication list manager to monitor responses and contact backup staff as necessary.

2. **Work off of a detailed script during a disaster.** When you are in recovery mode, many things can occur at the same time, and confusion is a given. In order to make the DR process easier, have a detailed script or step-by-step instructions in your DR plan. The script should be formally reviewed by several different members of the DR team. And since there is no guarantee the script will be followed by the same person who wrote it, it's best to use a simple bulleted list with easy-to-follow steps. Also, a disaster can occur at any time, so if the plan is executed late at night, confusion is likely to be high. Whatever can be done in the plan to make the steps easier to follow will go a long way. If at all possible, try to anticipate errors and include remediation steps. An example bulleted point can be as follows: "Connect network cable to PC. If network not found, first check if PC Ethernet connection shows signal." Straightforward instructions go a long way when you are under extreme stress and fatigue. Avoid using terms that may not be understood when extreme fatigue hits. If you must use technical terms or acronyms that may not be understood, add a glossary of terms.

In order to make the disaster recovery process easier, have a detailed script or step-by-step instructions in your DR plan.

3. **Test and retest the detailed DR plan**. It's possible to test separate portions of the DR plan on their own, but make sure the whole plan is tested at least once a year, or if a major change takes place. If you exercise or test the DR plan at least once a quarter, then the staff will become more familiar with the plan. And to make it more effective, try to exercise the plan with different staff members if you can. When testing the DR plan, don't assume that everything will go according to plan—this is why it's important to test. Always anticipate unusual conditions. You must come up with solutions for unexpected events, e.g., what would the team do if a drive or a technical component fails?

4. **Each member of the team should be familiar with their defined role.** Additionally, the backup members must be familiar with their roles. If a team member whose primary role is applications has a backup role as a telecommunications resource, make sure they know what that role entails.

5. **Include an application list in the DR plan.** An application list is any software package or system that will be part of the recovery, and it should always appear in a master list. Each entry in the list should have the application name as the technical staff identifies it, the name the business side recognizes and any technical details such as server name, etc. Along with the technical items, include the application owner, their full contact information and backup contacts.

Along with the technical items, include the application owner, their full contact information and backup contacts.

6. **Include a current network diagram of the entire network and recovery site in the DR plan.** Each node on the switch and panels should have some means of identification. In a recovery, you do not want to start following cables and wires through switches, etc.

7. **The DR plan should contain an easy-to-follow map and directions of how to reach the recovery site.** Don't assume everyone knows how to get to the recovery site. Secondary directions should be provided, too, in case the main route is congested or impassable. You should also include available parking facilities.

8. **Have a list of 24-hour supply delivery resources and restaurants at the recovery site.** This item may sound odd as a "must have," but it's of utmost importance sometimes. You will likely spend many hours at a recovery site and will need to replenish supplies. You do not want to start searching for places when every minute and resource counts. You may very well need to be at the recovery site for longer than 24 hours at a time. Also, be sure you know where the nearest hardware and office-supply stores are at your recovery site.

9. Include additional documentation such as a list of vendor contacts and insurance documentation such as policy numbers. These items as well as a list of all the hardware and software licenses you may have are helpful to have in a DR plan.

10. The DR plan must be current. The most critical issue regarding a DR plan is that it must be current and a backup copy exists at the recovery site. You do not want to go through a recovery process with an outdated plan. In order to avoid this, update the plan at least once a year, or whenever modifications are made that require a change in the DR plan. These changes can be in hardware, software upgrades virtualized servers, or any change that would modify the current DR environment.

BEST PRACTICES FOR IT DR PLANS

It's important to be sure the plan is clearly laid out and easy to follow. Keep in mind that there's no need to make it too lengthy or complex. The DR plan should be concise with easy-to-follow bullet points. Also, there may be circumstances that do not allow the plan's author to be present during the recovery period. DR plans should be written so that someone with a similar skill level can accurately follow all steps in the plan. Knowing this, the author should omit any shorthand or technical jargon from the instructions. It is important to realize that DR plans will probably be exercised under extreme conditions of stress and timing. When reviewing and editing the plan, ask yourself if the plan is simple and concise enough to follow under stressful and tiring situations. ⊙

Harvey Betan is a certified business continuity planning consultant with experience in disaster recovery in both technology and business functions.

Disaster recovery budget checklist and template

Learn how to put together a DR budget with our free template designed to help you organize your DR budget planning process.

By Paul Kirvan

WHEN DEVELOPING a disaster recovery (DR) budget, the following assumptions and considerations need to be addressed:

1. No DR and business continuity activities exist.
2. DR plans are in place for IT functions only.
3. DR plans are in place for business functions only.
4. Some departments/divisions have business continuity plans.
5. Management support for business continuity (BC)/DR activities does/doesn't exist.
6. The department is currently conducting business impact analyses (BIAs) and/or risk assessments.
7. The department is currently developing and implementing BC/DR plans that meet the needs of the organization.
8. An emergency operations center does/doesn't exist.
9. BC/DR policies and procedures are in place and approved by senior management.
10. A crisis management process and plan does/doesn't exist.
11. An enterprise risk assessment for the board and/or senior management has been/has not been completed.

Continued on p. 12

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

SAMPLE DISASTER RECOVERY BUDGET TEMPLATE

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
STAFFING													
Department manager/director													
Senior analyst													
Analyst													
Administrator													
Contractors													
Total staffing													
INTERNAL WEBSITE													
Website development (one-time cost)													
Hosting													
Support and maintenance													
Total website													
PROGRAM OFFICE													
Office space													
Furniture													
Electric													
Phone													
Internet													
Supplies													
Postage													
Emergency disaster funds													
Emergency operations center													
Other													
Total program office													
DR/BC MANAGEMENT SYSTEMS													
Risk analyses													
Business impact analyses													
Policies and procedures													
Plan development/updating													
Documentation													
Plan exercising													
Maintenance													
Training and awareness/company culture													
Incident/emergency management													
Records management													
Auditing/compliance													
Other BCMS projects													
Total BC management system													
SPECIAL SYSTEMS AND TECHNOLOGY													
Hot site													
Cold site													
Alternate office space													
Data backup and recovery													
Notification/alerting systems													
Mobile recovery systems													
Disaster recovery technology													
BC/DR software													
System/software maintenance													
Emergency communications													
Other													
Total special systems													
EDUCATION AND TRAINING													
Webinars/podcasts													
Attendance at conferences													
Subscriptions													
Professional memberships													
Professional accreditations													
Other													
Total education and training													
OTHER EXPENSES													
Travel (other than for conferences)													
Miscellaneous													
Other expenses total:													
Total budget													

DR TEMPLATE FOR YOUR BUDGET

Our DR budget template (see p. 9) provides a selection of typical DR and business continuity budget line items. Clearly some of the items on the table won't apply to every organization. Smaller organizations may not have the same types of budget line items in their organization as a larger enterprise.

Remember that the DR budget process, as well as the entire DR and BC organization in your firm, exists to accomplish several key activities:

- Develop and implement DR/BC plans that facilitate the timely recovery of critical business functions and IT facilities following a major disruption.
- Develop policies, procedures and compliance activities to address all BC/DR and security requirements.
- Develop, document and maintain plans to ensure survival of the business and minimize the impact of business and technology disruptions.
- Identify and assess potential risks to the enterprise and its operations, technology infrastructure, business processes and people.
- Identify and assess potential vulnerabilities to the enterprise and its operations, technology infrastructure, business processes and people.
- Design and deploy cost-effective emergency mechanisms that can quickly recover business and technology operations.
- Develop and deploy training and awareness programs so that all employees are fully aware of their responsibilities and commitments.
- Establish and maintain liaison with external parties such as customers, vendors, insurers, emergency first responders, regulators, financial institutions, etc.
- If external recovery facilities (e.g., hot sites) are used, ensure they are secure and that systems are prepared for emergency activation.
- Develop a capability to optimize media relations so as to minimize adverse publicity and negative business implications.

Putting together a DR and BC budget can be time-consuming and complicated if you haven't done it before. To help make your budgeting process easier, download SearchDisasterRecovery.com's disaster recovery budget template that will help you get started with your budget planning process.

Paul Kirvan, CISA, CSSP, FBCI, CBCP, has more than 20 years experience in business continuity management as a consultant, author and educator. He has been directly involved with dozens of IT/telecom consulting and audit engagements ranging from governance program development, program exercising, execution and maintenance, and RFP preparation and response. Kirvan currently works as an independent business continuity consultant/auditor, and is the secretary of the Business Continuity Institute USA chapter.

Business risk assessments in IT disaster recovery planning

Learn why a risk assessment is an important part of your DR plan and how to put one together.

By Harvey Betan

THERE ARE MANY things to consider when discussing business risk assessments in disaster recovery (DR) planning. In simple terms, a risk assessment is a list of possible threats against an organization. It also estimates the probability of these threats occurring and the impact of these threats to the operation of an organization. Duration also plays a part in the risk assessment as well. For example, the impact of shutting down for a day due to weather is not the same as having the building destroyed by weather. In every organization, risk assessments should be taken into consideration when making a DR plan. They help identify and reduce potential threats to ensure business continuity (BC). This article explores the purpose of risk assessments, the steps needed to put one together and how to review business risk assessments in your organization.

WHAT IS THE PURPOSE OF A RISK ASSESSMENT?

The Disaster Recovery Institute International (DRII) states that the purpose of a risk assessment is “to determine events, probabilities and environmental surroundings that can adversely affect the organization and its facilities with disruption and disaster and the controls needed to prevent or minimize the effects of potential loss.”

One thing to keep in mind is that there is a great deal of subjective analysis that is part of the impact or risk assessment. In other words, risk assessments should be reviewed by a team possessing knowledge about both the organization and the business continuity plan.

Steps should be taken to avoid risks once they have been identified in the impact assessment. For example, once the probability of occurrence and the level of impact have been determined, you can directly address the risk posed and try to eliminate the risk. If the risk is somewhat unpredictable, such as a natural disaster, it’s advised to at least try and reduce the impact of the risk. And although it’s not advised, you can also ignore the risk and accept the consequences. But addressing risks is often not complicated. A sufficient response to a risk or threat may be as simple as purchasing uninterruptible power supply (UPS) units and generators on standby to address electrical power issues found during a risk assessment.

Top 10 musts for a DR plan
DR budgets
Business risk assessments
BIAs and DR planning
Free DR templates
Sponsor resources

STEPS FOR PUTTING TOGETHER A RISK ASSESSMENT

Putting together a risk assessment is simple. Most organizations use a spreadsheet to compile and present the risks in their organization, and these can be found from vendors or internet sites.

The first step for putting together a risk assessment is to identify as many threats as are applicable to your organization. For example, natural threats in the Midwest may include tornados, while organizations along the East Coast are more concerned about hurricanes. Once threats are identified, the next step is to estimate the probability of occurrence for each threat (this will most likely be subjective), followed by the business impact on the organization. The impact threshold is labeled low, medium, or high according to the effect it could have on the organization.

Below is an example of identifying a risk:

SAMPLE WORKSHEET SHOWING HOW TO IDENTIFY A RISK TO YOUR BUSINESS

Threat	Probability	Impact	Measures to be taken
Power outage	0.1	High	Obtain UPS or generator for essential areas

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

In this example, the threat of a power outage has a 10% likelihood of occurring, however, if it does occur the impact to the organization is high. To reduce this risk, one can obtain UPS units or a generator. The probability of this threat occurring would still be 10%, but the impact would be reduced to low. The next step is to sort your list from low, medium and high impacts to your organization. Then you can begin to address some mitigation process for threats as appropriate.

The risk assessments can be completed by an individual, but there are many subjective values involved, so it may be advantageous to have a small group involved to eliminate bias. The team should consist of representatives from IT, operations and finance at the very least. IT should be included for obvious reasons, operations and finance to ensure the impacts of the outages are viable. The team leader must be someone who can ensure the rest of the team takes this task and schedule seriously. The team should start by looking at natural threats, then progress to other possible threats such as safety and access in the facility. To do this, walk through the facility and look for safety related issues, blocked walkways, hot plates, storage facilities, or anything that could create issues of safety, entry and egress. Above all, to perform adequate risk assessment, you must be honest and objective when reviewing these issues, especially those relating to workplace violence, disgruntled employees, or data access.

The team should start by looking at natural threats, then progress to other possible threats such as safety and access in the facility.

RISK ASSESSMENTS AND DISASTER RECOVERY SITES

One issue that does not get the attention it deserves is the fact that the DR site itself should go through its own business risk assessment because it's an additional facility that not only is a place to back up your technologies, but also, the activity that goes on there can affect your organization if an incident occurs. If you are using a third-party vendor, such as IBM Corp., SunGard Data Systems Inc. or some other facility, look at who is assigned space close to you. Some sites will review the nearby tenants and discuss location with you.

Risk assessments at DR sites should be similar to the original site. Some issues to look for include: What is the policy for vendors and visitors? Are there sufficient restrooms for all staff and dining facilities? Is there a further need for credentialing? Most disaster recovery sites are in more remote areas, but is the site as accessible as the main site? Are the roads passable in bad weather? All the threats associated with the main DR site should be reviewed and applied to the DR site. You must realize that the DR plan and DR site may be expected to be the operations site for a period of time. That duration is uncertain and could be for an extended period of time, depending on the incident.

REVIEW YOUR RISK ASSESSMENT REGULARLY

A business risk assessment should be reviewed as often as the DR plan itself. Even if there are no changes to be made, you should review your risk assessment at least once a year. The team leader should ensure not only that the plan is reviewed but that the plan is presented and accepted by the executive level. A vigorous risk assessment is not expensive to execute, but you do need an objective view and knowledge of what to look for. Both the DRII and Business Continuity Institute agree that the risk assessment should come before the business impact assessment. This seems logical when you consider that before you look at operating functions, you must look at the overall risks to the organization in general. ⊙

Harvey Betan is a certified business continuity planning consultant with experience in disaster recovery in both technology and business functions.

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

Getting started with a business impact analysis: 10 easy steps

Learn why a business impact analysis is an important part of your DR plan and how to put one together.

By George Wrenn

A **BUSINESS IMPACT ANALYSIS** (BIA) is the cornerstone of a disaster recovery (DR) strategy and plan. A BIA will identify the processes, systems and functions that are critical to the survival of your company. Understanding these elements allows you to allocate resources wisely to ensure continuing operations even with unexpected events disrupting normal business operations.

A BIA is an analytic process that aims to reveal the business impacts that would result when a critical process exceeds its maximum allowable outage.

To start, you need to understand the business operations of your company in detail. Here is a simple step-by-step approach that will put you on your way to conducting a successful BIA:

1. Get support from senior management for the exercise. You will then be able to meet with the operations-level managers that know enough detail about the processes to be helpful to the program. It's hard to get people's time and even harder to get follow up for a business continuity plan (BCP) without this support.

2. Hold a kickoff meeting with the managers responsible for the core business processes and introduce the program goals, timelines and deliverables.

3. Collect data. Create a BIA questionnaire, which you will distribute at the meeting to all managers. Instruct each manager on how to com-

WHAT YOUR BIA MUST INCLUDE

The business impact analysis questionnaire should gather the following data:

1. The "functional parent" of the process, this may be a department or location.
2. The process name and a detailed description of the process.
3. List of all inputs and outputs from the process.
4. Define maximum allowable outage time before impact occurs.
5. Descriptions of the financial and operational impact experienced during an outage.
6. Human and technology resources needed to support the process including computers, networks, offices, people, etc.
7. A description of the customer impact of external facing or inward facing processes, and a list of departments that depend on the process outputs.
8. Explanation of any legal or regulatory impacts that may be created in an outage.
9. Description of past outages and the impacts associated with each.
10. Description of workaround procedures or work shifting options to other departments or remote workers as applicable.

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

plete the document. Make it clear that you will be following up with each manager on an individual basis to review the document. See "What your BIA must include" on p. 16 for more information about creating a BIA questionnaire.

4. Document the gross revenue and net profit your organization generates per year. This can be done at the appropriate business unit levels as well. The data sets the upper limit for business losses related to the business operation. Include this on your presentations to drive home the importance of the program.

5. Meet with each manager and review the data collected. If needed, block off a couple of hours to help complete and refine the document with the manager.

6. Merge all the data into a spreadsheet or database for easy data analysis and reporting capability.

7. Schedule and conduct a "BIA review and prioritization meeting" with all managers participating in the program. Look for gaps not mentioned by the departments, especially between departments. Prioritize each process based on impact to the business, both direct and indirect as the process may be critical dependency for another process. High, medium and low can be used as measures.

8. During the prioritization discussion you will need to document a recovery time objective (RTO) for each process. The RTO defines the time to return the process to normal operation before impact results to the business and is generally measured in hours.

9. Create groups or bands of process RTOs. Start with the shortest allowable RTO first and then define the upper limits not to exceed 24 hours. These items constitute the Tier 0 RTOs. The next band of RTOs is the Tier 1 group. This group generally extends from 24 to 48 hours. Recovery point objectives (RPOs) are different as they deal more with data recovery and are used more in a "data protection strategy" context. They are also usually measured in minutes to hours as in the case of a production database. It may have an RPO of 20 minutes between scheduled replications.

10. Lastly, convene a summary meeting to present the results of the program to senior management, managers and others core to the processes at topic. You will want to present the business processes in order of RTO and importance, along with the other process details collected during the program. Issue a final report to meeting attendees to reinforce the learning and memory of the participants. Make the report available in hard copy to use in the event of an actual outage to help prioritize actions to resume operations.

The BIA report ideally provides a foundation for the BCP that should follow this exercise. It can also provide an important input to risk management programs that may follow, now that you have insights into where business risk lives. ⊙

George Wrenn, CISSP, ISSEP, is frequent contributor to SearchSecurity.com and *Information Security* magazine. He served as a Director of Security in the financial services industry and is now a consulting security expert.

TOP FIVE FREE DISASTER RECOVERY PLAN TEMPLATES

***Download** our top five free disaster recovery plan templates.*

By SearchDisasterRecovery Editorial Staff

An information technology disaster recovery (DR) plan gives organizations a formal approach for responding to unplanned disasters that threaten an IT infrastructure. Parts of your organization that can be affected by disasters are hardware, software, networks, processes and, most importantly, people. Protecting your company's investment in its technology infrastructure, and protecting your firm's ability to conduct business are the key reasons for implementing an IT DR plan.

If you've never put together a DR plan, it can be a daunting task. To help you make your job easier, we've collected the top five DR plan templates.

IT DR plan template: A free download and sample plan

According to National Institute for Standards and Technology (NIST) Special Publication 800-34, Contingency Planning for Information Technology Systems, the following summarizes the ideal structure for an IT disaster recovery plan:

- **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
- **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components.
- **Identify preventive controls.** These are measures that reduce the effects of system disruptions and can increase system availability and reduce contingency life cycle costs.
- **Develop recovery strategies.** Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption.
- **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
- **Plan testing, training and exercising.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
- **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.

To get started with your IT DR plan, download SearchDisasterRecovery's IT DR template.

A pandemic recovery plan template

Pandemic plans differ slightly from traditional DR and business continuity (BC) plans because they focus more on people and less on technology. When you think about the potential health threat to employees from a pandemic, a carefully designed pandemic recovery plan can help your organization remain viable, even if you have less staff members working in the office. This pandemic planning guide and SearchDisasterRecovery.com's free downloadable pandemic planning template provide an excellent starting point for pandemic planning.

Business impact analysis template and methodology guide

A business impact analysis is an essential component of the BC process that analyzes mission-critical business functions, and identifies and quantifies the impact a loss of those functions may have on the organization. SearchDisasterRecovery.com has created a free downloadable BIA template

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

to help with your business continuity planning. Download and print out our template, and then read the step-by-step business impact analysis guide for disaster recovery professionals to create a successful BIA.

BC plan template

For many IT professionals, the BC and DR planning processes are very challenging. The BC planning process contains several steps. These include project initiation, risk assessment, business impact analysis, strategy development, plan development, plan exercising and maintenance, emergency communications, awareness and training and coordination with public authorities. SearchDisasterRecovery.com has created a free downloadable business continuity template to assist you in your business continuity planning. Download and print out our template, and then read the step-by-step guide on business continuity planning.

IBM's free disaster recovery plan template

A disaster recovery plan will help you respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. IBM Corp. has provided a free downloadable DR template on its website.

For even more information on disaster recovery templates, bookmark our special page on free disaster recovery plan templates.

Top 10 musts for a DR plan

DR budgets

Business risk assessments

BIAs and DR planning

Free DR templates

Sponsor resources

RESOURCES FROM OUR SPONSOR

riverbed®

Think fast.®

See ad page 2

- **Best Practices in Business Continuity and Disaster Recovery**
- **ESG - Practical Advice for Streamlining Business Continuity/Disaster Recovery Solutions**
- **Chalk Talk: Disaster Recovery**

About Riverbed Technology, Inc.:
Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization.